Federal Office
for Information Security

IT-Grundschutz-Compendium

Final Draft, 1 February 2022

Foreword

Attacks with ransomware currently represent the greatest threat to companies and public authorities. Time and again, criminals successfully compromise and blackmail those affected, including critical infrastructures such as hospitals or entire supply chains of manufacturing companies.

Unfortunately, alongside recurring software vulnerabilities, employees also represent another gateway for attacks of this kind; they fall victim to increasingly sophisticated digital traps - otherwise known as social engineering.

At the BSI we aim to support companies, public authorities and critical infrastructure facilities to properly secure themselves against risk. This is what our BSI IT-Grundschutz stands for. As well as technical and staffing recommendations, the latest edition of the IT-Grundschutz Compendium provides users with useful tips for securing their organisation and infrastructure.

It is important to us is that IT-Grundschutz is sustainable in practice. Only a holistic approach works: thinking about people, structures and technology as a single entity. Examples of these are the security considerations for building automation and control systems (BACS) or remote maintenance in industry that are included in this new edition.

At the BSI, we aim to support you with this revision work. Feel free to contact my colleagues if you have questions or suggestions for improvement.

We can only make Germany digitally secure by working together. This is what the BSI stands for.

Arne Schönbohm

President of the Federal Office for Information Security

Acknowledgements

Due to the rapid developments in the field of information technology and increasingly shorter production cycles, the contents of the IT-Grundschutz Compendium are subject to constant change. Alongside the BSI itself, IT-Grundschutz users make a valuable contribution by providing texts (or even entire modules), commenting on modules, or suggesting new subjects.

The following organisations and individuals have contributed their specialist knowledge to the development and revision of the IT-Grundschutz Compendium modules.

IT-Grundschutz users

We would like to take this opportunity to thank numerous IT-Grundschutz users for their contribution to Edition 2022 of the IT-Grundschutz Compendium. Many users have commented on individual IT-Grundschutz modules and contributed their expertise to the new edition.

Special thanks are due to the following users, who have commented extensively on several IT-Grundschutz modules and thus contributed to the revision of the 2021 compendium:

- Claus Irion (Cyber and Information Domain Service)
- Dr. Tatjana Loewe (secunet Security Networks AG)

IT-Grundschutz continues to be developed not only by or on behalf of the BSI; users also regularly take on new module subjects. They develop new modules or revise existing texts without compensation. Special thanks goes to the following users, who have developed or significantly updated the above modules:

- Christoph Puppe (SVA System Vertrieb Alexander GmbH) for APP.4.4 *Kubernetes* and SYS.1.6 *Containerisation*

Employees of the Federal Office for Information Security

The current revision of the IT-Grundschutz Compendium also incorporates the expertise of numerous BSI employees. The following individuals deserve special thanks:

Stefan Ahlers, Julian Backhaus, Dr. Klaus Biß, Markus de Brün, Thorsten Dietrich, Klaus Hunsänger, Jens Kluge, Vera Lange, Jens Mehrfeld, Marc Meyer, Andreas Neth, Dr. Harald Niggemann, Detlef Nuß, Martin Reuter, Rudolf Schick, Frank Weber, Jens Wiesner, Dr. Melanie Winkler, Dr. Dietmar Wippig

We wish to express our particular gratitude to Ms Isabel Münch, who, as former head of the IT-Grundschutz unit, has left a lasting mark on IT-Grundschutz.

Updating and further development of previous editions

Along with the BSI itself, numerous organisations and individuals from the realms of public administration, industry, and science have also contributed to the updating and further development of previous editions of the IT-Grundschutz Compendium. Our thanks go out to these people, as well.

Legal Notice

Publisher
Federal Office for Information Security (BSI), Bonn, Germany

Overall responsibility and chief editorship
Holger Schildt

Editors
Katrin Alberts, Stefanie Förster, Brigitte Hoffmann, Fabian Nißing und Jessika Welticke

Preparation and update of IT-Grundschutz modules
Alex Didier Essoh, Stefanie Förster, Daniel Gilles, Florian Göhler, Florian Hillebrand, Brigitte Hoffmann, Cäcilia Jung, Birger Klein, Alexander Nöhles, Johannes Oppelt, and Christoph Wiemers

Version
February 2022

Table of Contents

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violations of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.34 Assault

G 0.35 Coercion, Blackmail or Corruption

G 0.36 Identity theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.40 Denial of Service

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

G 0.47 Harmful Side Effects of IT-Supported Attacks

ISMS.1 Security Management

ORP.1 Organisation

ORP.2 Personnel

ORP.3 Awareness and Training in Information Security

ORP.4 Identity and Access Management

ORP.5 Compliance Management

CON.1 Crypto Concept

CON.2 Data Protection

CON.3 Backup Concept
CON.6 Deleting and Destroying Data and Devices
CON.7 Information Security on Trips Abroad
CON.8 Software Development
CON.9 Information Exchange
CON.10 Development of Web Applications
OPS.1.1.2 Proper IT Administration
OPS.1.1.3 Patch and Change Management
OPS.1.1.4 Protection Against Malware
OPS.1.1.5 Logging
OPS.1.1.6 Software Tests and Approvals
OPS.1.1.7 System Management
OPS.1.2.2 Archiving
OPS.1.2.4 Teleworking
OPS.1.2.5 Remote Maintenance
OPS.1.2.6 NTP Time Synchronisation
OPS.2.1 Outsourcing for Customers
OPS.2.2 Cloud Usage
OPS.3.1 Outsourcing for Service Providers
DER.1 Detecting Security-Relevant Events
DER.2.1 Security Incident Handling
DER.2.2 Provisions for IT Forensics
DER.2.3 Clean-Up of Extensive Security Incidents
DER.3.1 Audits and Revisions
DER.3.2 Audits Based on the BSI “Guideline for IS Audits”
DER.4 Business Continuity Management
APP.1.1 Office Products
APP.1.2 Web Browsers
APP.1.4 Mobile Applications (Apps)
APP.2.1 General Directory Service
APP.2.2 Active Directory
APP.2.3 OpenLDAP
APP.3.1 Web Applications and Web Services
APP.3.2 Web Servers
APP.3.3 File Servers

APP.3.4 Samba

APP.3.6 DNS Servers

APP.4.2 SAP ERP Systems

APP.4.3 Relational Database Systems

APP.4.4 Kubernetes

APP.4.6 SAP ABAP Programming

APP.5.2 Microsoft Exchange and Outlook

APP.5.3 General E-Mail Clients and Servers

APP.6 General Software

APP.7 Development of Individual Software

SYS.1.1 General Server

SYS.1.2.2 Windows Server 2012

SYS.1.3 Linux and Unix Servers

SYS.1.5 Virtualisation

SYS.1.6 Containerisation

SYS.1.7 IBM Z

SYS.1.8 Storage Solutions

SYS.2.1 General Client

SYS.2.2.2 Windows 8.1 Clients

SYS.2.2.3 Windows 10 Clients

SYS.2.3 Linux and Unix Clients

SYS.2.4 macOS Clients

SYS.3.1 Laptops

SYS.3.2.1 General Smartphones and Tablets

SYS.3.2.2 Mobile Device Management (MDM)

SYS.3.2.3 iOS (for Enterprise)

SYS.3.2.4 Android

SYS.3.3 Mobile Telephones

SYS.4.1 Printers, Copiers, and All-in-One Devices

SYS.4.3 Embedded Systems

SYS.4.4 General IoT Devices

SYS.4.5 Removable Media

IND.1 Process Control and Automation Technology

IND.2.1 General ICS Components

IND.2.2 Programmable Logic Controller (PLC)

IND.2.3 Sensors and Actuators

IND.2.4 Machine

IND.2.7 Safety Instrumented Systems

IND.3.2 Remote Maintenance in Industry

NET.1.1 Network Architecture and Design

NET.1.2 Network Management

NET.2.1 WLAN Operation

NET.2.2 WLAN Usage

NET.3.1 Routers and Switches

NET.3.2 Firewall

NET.3.3 VPN

NET.4.1 Telecommunications Systems

NET.4.2 VoIP

NET.4.3 Fax Machines and Fax Servers

INF.1 Generic Building

INF.2 Data Centre and Server Room

INF.5 Room or Cabinet for Technical Infrastructure

INF.6 Storage Media Archives

INF.7 Office Workplace

INF.8 Working from Home

INF.9 Mobile Workplace

INF.10 Meeting, Event, and Training Rooms

INF.11 General Vehicle

INF.12 Cabling

INF.13 Technical Building Management (TBM)

INF.14 Building Automation and Control Systems (BACS)

What's New in the IT-Grundschutz Compendium

The 2022 edition of the IT-Grundschutz Compendium contains a total of 104 IT-Grundschutz modules. These include 7 new IT-Grundschutz modules and the 97 modules from the 2021 edition. Of these, 16 modules were revised for the 2022 edition.

New Modules

The following 7 new IT-Grundschutz modules have been added in five different layers:

- OPS.1.1.7 System Management
- OPS.1.2.6 NTP Time Synchronisation
- APP.4.4 Kubernetes
- SYS.1.6 Containerisation
- IND.3.2 Remote Maintenance in Industry
- INF.13 Technical Building Management (TBM)
- INF.14 Building Automation and Control Systems (BACS)

Revised Modules

After the publication of the last edition of the IT-Grundschutz Compendium in February 2021, the IT-Grundschutz team received a considerable amount of valuable feedback from IT-Grundschutz users. Advice on individual aspects and feedback from the professional practices of chief information security officers and other experienced users help to make the contents even more up to date and practical. The individual module texts were then reviewed and revised so that 16 IT-Grundschutz modules were updated in the 2022 edition.

The IT-Grundschutz modules were revised to varying extents. The changes are classified as follows:

- **Extensive changes** that can impact certification processes or existing security policies can be found in separate change logs. Such changes are found in 14 modules from the 2021 edition. The "Change Logs (2022 Edition)" are contained in the following section and published on the BSI website under the heading IT-Grundschutz Compendium.
- **Minor linguistic and editorial changes** and revisions that aim to provide for better comprehensibility are not listed in a separate change log. In cases where there have only been minor revisions of this kind to IT-Grundschutz modules, this has only been indicated by changing the date in the footer to the current edition. Such changes are found in 2 modules from the 2021 edition.

IT-Grundschutz modules from the 2021 edition that have been revised and for which a change log is available:

- CON.3 Backup Concept

- CON.8 Software Development
- CON.10 Development of Web Applications
- OPS.1.1.5 Logging
- OPS.1.1.6 Software Tests and Approvals
- OPS.1.2.5 Remote Maintenance
- APP.3.1 Web Applications and Web Services
- APP.4.3 Relational Database Systems
- APP.6 General Software
- SYS.1.1 General Server
- SYS.1.5 Virtualisation
- SYS.1.7 IBM Z
- SYS.2.1 General Client
- SYS.2.2.3 Windows 10 Clients

IT-Grundschutz modules from the 2021 edition with minor revisions:

- APP.1.2 Web Browsers
- INF.2 Data Centre and Server Room

Errata and revised modules

In spite of careful, multi-stage quality assurance, errors and inaccuracies cannot always be avoided in a work as extensive as the IT-Grundschutz Compendium. Due to the rapid development cycles in information technology, concepts and requirements from IT-Grundschutz may also no longer be fully applicable as of the publication date of each edition.

Users who notice errors or other problems are invited to report them to *grundschutz@bsi.bund.de*. All comments from users will be reviewed by the IT-Grundschutz team and incorporated as appropriate into the next edition of the IT-Grundschutz Compendium.

In the course of the year, drafts of revised modules may also appear that have already been updated accordingly.

Necessary corrections that occur after the editorial deadline for the current edition will be published in “Errata zur Edition 2022” [Errata for the 2022 Edition] on the IT-Grundschutz website at https://bsi.bund.de/grundschutz under the heading “IT-Grundschutz Compendium”. They will replace the corresponding erroneous statements in the IT-Grundschutz Compendium.

IT-Grundschutz – The Basis for Information Security

Why is Information Security Important?

Information is an essential asset for companies and public authorities, which is why it requires adequate protection. Today, most business processes and specialised tasks in the economy and public administration are no longer imaginable without IT support. Reliable information processing and the technology it involves are indispensable in maintaining operations. In many cases, however, inadequately protected information is an underestimated risk factor that can even pose an existential threat. At the same time, basic IT protection and a reasonable level of information security can be achieved with relatively modest resources. In IT-Grundschutz, the BSI offers organisations practicable methods for appropriately protecting their information. The combination of the IT-Grundschutz methodologies for basic, core and standard safeguards and the IT-Grundschutz Compendium outlines security requirements for establishing an information security management system (ISMS) in different operational environments, which ultimately facilitates the secure handling of information. IT-Grundschutz can be used by small and medium-sized companies (SME) as well as large organisations to establish a management system for information security. However, successful implementation of the IT-Grundschutz Compendium requires that an organisational unit (IT operations) is established to set up, operate, monitor and maintain internal IT.

Due to their dependency on IT systems, organisations that are affected by security incidents face a greater risk of suffering damage to their image. They need to adequately protect the information they process and to plan, implement and monitor their security safeguards with the requisite care. Here, it is important not to focus solely on the security of IT systems; information security must be viewed holistically. It also depends greatly on the framework conditions at hand in terms of infrastructure, organisation and personnel. It is vital not to neglect operating environment security, adequate employee training, service reliability, proper handling of sensitive information and many other important aspects.

Deficiencies in information security can, after all, lead to significant problems. The types of potential damage can be assigned to different categories:

- **Loss of Availability**
  If basic information is not available, this is usually noticed quickly, especially when it means tasks cannot be continued. If an IT system is down, it may be impossible to execute financial transactions, place online orders or carry out production processes, for example. Even if the availability of certain information is only restricted in some way, the business processes or specialised tasks within an organisation can still be affected.
- **Loss of Confidentiality of Information**
  Every citizen and customer wants their personal data to be handled confidentially. Every company knows that the competition is interested in confidential internal data about turnover, marketing, research and development. The accidental disclosure of information can result in serious damage in many areas.

- **Loss of Integrity (Correctness of Information)**
  Falsified or manipulated data may cause erroneous bookings, incorrect deliveries or faulty products, for example. The loss of authenticity (that is, genuineness and verifiability as a subarea of integrity) is also of great importance. Data can be assigned to the wrong person, for example. Payment instructions or orders could thus be charged to the account of a third party, inadequately secured digital declarations of intent could be associated with the wrong persons or an individual's digital identity could be forged.

Information and communication technology plays an important role in almost all areas of daily life, and the pace of innovation has remained consistently high for years. The following developments are particularly worth mentioning:

- **Increasing Level of Networking**
  People and IT systems no longer operate in isolation; indeed, they are becoming increasingly connected. This makes it possible to access shared databases and engage in in-depth forms of collaboration across geographic, political and organisational boundaries. As a result, our world is dependent not only on individual IT systems, but to a large extent on data networks, as well. This in turn means that security deficiencies can quickly have global consequences.
- **IT Distribution and Penetration**
  More and more areas are being supported by information technology, often without the user's awareness. As it becomes increasingly compact and inexpensive, the necessary IT hardware is finding its way into all aspects of daily life. Examples include clothes with integrated health sensors, light bulbs connected to the Internet, IT-supported sensor systems in cars that can react automatically to changing surroundings and even self-driving vehicles. More and more often, these different IT components communicate with one other wirelessly. This makes it possible to locate and control everyday objects via the Internet.
- **Disappearance of Network Borders**
  Until recently, it was possible to clearly associate business processes and applications with specific IT systems and communication routes. It was also possible to determine where the systems were located and the organisations to which they belonged. The rising popularity of cloud services and communication via the Internet is increasingly blurring the lines among these systems.
- **Shorter Attack Cycles**
  The best way to prevent malware or other attacks on IT systems, application programs and protocols is to obtain the most recent information on vulnerabilities and how to eliminate them (such as by installing patches or updates). These days, the announcement of a vulnerability is followed almost immediately by the first large-scale attacks, which means it is becoming more and more important to have a well-staffed information security management team and a corresponding warning system.
- **Greater Application Interactivity**
  Existing technologies are increasingly being combined to create new usage models. This includes various fields of application such as social communication platforms; portals for the shared use of information, photos and videos; and interactive web applications. However, this is also leading to increasingly intertwined business processes and higher complexity, which makes it generally more difficult to safeguard the underlying IT systems.

- **User Responsibility**
  The best technology and solid security safeguards cannot ensure a sufficient level of information security if the human factor is not adequately taken into account. This mainly concerns responsible behaviour on the part of the individual. To that end, current information on security risks and the code of conduct regarding the handling of IT need to be taken into account.

IT-Grundschutz: Objectives, Concept and Design

In the IT-Grundschutz Compendium, standardised security requirements for typical business processes, applications, IT systems, communication links and rooms are described in the individual IT-Grundschutz modules. The objective of IT-Grundschutz is to enable organisations to attain an adequate level of protection for all their information. The IT-Grundschutz Methodology is characterised by a holistic approach. By implementing a suitable combination of standard organisational, personnel-related, infrastructural, and technical security requirements, it is possible to attain a security level that is adequate for the relevant protection needs and appropriate for protecting information relevant to the organisation. Furthermore, the requirements of the IT-Grundschutz Compendium not only form a security basis for business processes, applications, IT systems, communication links and rooms that are highly sensitive; in many instances they also explain how a higher security level can be reached.

IT-Grundschutz follows a modular approach to enable improved structuring and planning in an area as heterogeneous as information technology, including with regard to operational environments. The individual modules address typical business process workflows and areas of IT use – for example, emergency management, client/server networks, buildings, and communication and application components.

The modules of the IT-Grundschutz Compendium reflect the state of the art based on the latest knowledge at the time of their publication. The requirements formulated in the modules describe what generally should be implemented in order to achieve the state of the art by means of appropriate security safeguards. The requirements and safeguards that reflect the state of the art correspond both to what is technologically advanced at the time of publication and what has proven successful in practice.

Reducing Analytical Effort

The IT-Grundschutz Methodology is designed to make drawing up IT security concepts a simple and efficient process. Within the context of traditional risk analysis, threats and vulnerabilities are initially determined and assigned a likelihood of occurrence so that suitable security safeguards can then be selected and residual risks assessed. These steps have already been completed for each IT-Grundschutz module. Appropriate security requirements have been selected for typical application scenarios so that users can translate them into appropriate security safeguards according to their individual framework conditions. The analysis involved in applying the IT-Grundschutz Methodology is limited to determining what gaps exist between the security requirements recommended in the IT-Grundschutz Compendium and those that have already been met. Any unfulfilled requirements constitute security deficits that need to be rectified. Only when the protection needs are significantly higher is it necessary to perform an individual risk analysis that takes into consideration aspects of cost and effectiveness in addition to the requirements from the IT-Grundschutz

modules. In this case, though, it is generally sufficient to supplement the safeguards selected based on the IT-Grundschutz Compendium with corresponding individual, higher-quality safeguards. A procedure for this is described in BSI Standard 200-3, *Risk Analysis Based on IT-Grundschutz*.

The IT-Grundschutz Compendium provides valuable guidance that also extends to special components or operational environments it does not specifically handle. If an individual risk analysis is required, the focus can be placed on the specific threats and security safeguards in question.

Requirements for Any Security Need

The requirements listed in the IT-Grundschutz Compendium should be fulfilled in order to achieve an adequate security level. They are divided into Basic Requirements, Standard Requirements and Requirements in Case of Increased Protection Needs. The Basic Requirements represent the minimum security safeguards that should be implemented. As a starting point, users can keep to the Basic Requirements in order to fulfil the most effective requirements in short order. However, adequate state-of-the-art security is only achieved by implementing the Standard Requirements. The exemplary Requirements in Case of Increased Protection Needs have also proven successful in practice by specifying additional safeguards an organisation can implement to meet elevated protection requirements. In addition, the supplementary Implementation Guidance published for most modules contains best practices and further information on how the requirements can be fulfilled. For certification according to ISO 27001 based on IT-Grundschutz, the Basic Requirements and Standard Requirements must be fulfilled for the selected scope of application. Since the Basic Requirements are absolute essentials that must be fulfilled as a matter of priority, certification according to ISO 27001 on the basis of IT-Grundschutz is only possible once all these requirements have been fulfilled.

Like most of the information relating to IT-Grundschutz, the IT-Grundschutz modules and the associated Implementation Guidance are also available in electronic form. The IT-Grundschutz texts can thus also be used as a basis for drawing up security concepts. In addition, users are provided with auxiliary resources and sample solutions that can help them meet the requirements.

Since IT-Grundschutz has also proven popular on an international scale, the IT-Grundschutz Compendium and other publications are also available online in English.

Continued Development of the IT-Grundschutz Compendium

Due to the rapid developments in the field of information technology and increasingly shorter production cycles, the contents of the IT-Grundschutz Compendium are subject to constant change. The structure and content of the IT-Grundschutz Compendium are therefore designed to facilitate prompt updates and the inclusion of new subjects in its modules and other individual publications. Alongside the BSI, IT-Grundschutz users can also contribute by drawing up texts (or even entire modules) for IT-Grundschutz, commenting on modules or suggesting new subjects. The aim is to keep the IT-Grundschutz Compendium up to date.

Current information on IT-Grundschutz is also provided by the IT-Grundschutz Newsletter, which can be subscribed to free of charge on the BSI website. The newsletter also regularly

informs users about ways they can get involved, such as through surveys on specific current subjects. The feedback received from users provides valuable ideas and inspiration for the continued development of IT-Grundschutz. Their everyday practical experiences are of great importance in reviewing the requirements and recommendations and adapting them to current needs.

Structure of the IT-Grundschutz Compendium

The IT-Grundschutz Compendium can be divided into different areas, each of which is explained below:

Introduction

This section briefly explains the ideas, aims and structure of the IT-Grundschutz Compendium. A detailed description of the IT-Grundschutz Methodology can be found in BSI Standard 200-2.

Information on the Layer Model and Modelling in General

In order to model a complex information domain according to IT-Grundschutz, the corresponding modules of the IT-Grundschutz Compendium have to be selected and implemented. To make the selection easier, the modules in the IT-Grundschutz Compendium are initially divided into process and system modules. Process modules are equally applicable to all or major parts of the information domain, whereas system modules are generally applicable to individual objects or groups of objects. The process and system modules in turn consist of further sublayers.

The information on the layer model and modelling in general describes when it is appropriate to use an individual module and the target objects to which it should be applied. In addition, the modules are marked according to the priority of their implementation.

Description of Roles

In the requirements of the modules, the roles that are responsible for their implementation are specified. Based on this information, the appropriate contact persons for the relevant subject matter at a given organisation can be identified. Since the titles of the people or roles named as responsible persons in the IT-Grundschutz Compendium are not the same in every organisation, a short description of the most important roles is provided in section 3, *Roles*, to make assignment easier.

Glossary

The glossary of the IT-Grundschutz Compendium explains the most important terms in the field of information security and IT-Grundschutz. An additional glossary on cyber security can be found on the BSI website.

Elementary Threats

From the large number of specific individual threats within the modules of the previous IT-Grundschutz Catalogues, the BSI has identified the general aspects and translated them into 47 Elementary Threats. These are listed in the IT-Grundschutz Compendium. The overview of the Elementary Threats was created to achieve the objectives described below. Elementary Threats are:

- optimised for use in risk analysis
- product-neutral (always) and technology-neutral (if possible; certain technologies influence the market to such an extent that they also influence the abstracted threats)
- compatible with comparable international catalogues and standards
- seamlessly integrated into IT-Grundschutz

IT-Grundschutz Modules

Each of the modules of the IT-Grundschutz Compendium contains a description of the component, approaches and IT systems under consideration, followed by a short overview of the specific threats and the requirements to be met in safeguarding the component.

Structure of the Modules

The most important part of the IT-Grundschutz Compendium is the modules, which all have the same structure. First, the relevant target object under consideration is described. The subsequent objective formulates the security to be gained by implementing the IT-Grundschutz module. This is followed by the section *Scoping and Modelling*. This details the aspects not included in the scope of the module and references to other modules where these are addressed. In addition to specifying the aspects not included in the scope, this section provides modelling notes for the specific module.

Specific threats are then listed. The list is by no means exhaustive, but it does convey an understanding of the security problems which may arise when using the component, approach or IT system under consideration without countermeasures. The explanation of the potential risks can raise the user's awareness of the subject. In the risk analysis which forms the basis of each module, the specific threats have been derived from the Elementary Threats. Requirements that counteract these threats are generally included in the same module; in some cases, however, additional requirements from other modules need to be considered.

In each module's structure, the specific threats are followed by the requirements. These are divided into three categories: Basic Requirements, Standard Requirements and Requirements in Case of Increased Protection Needs. The implementation of Basic Requirements has priority, as they make it possible to achieve the maximum benefit with minimal effort. Together with the Basic Requirements, the Standard Requirements reflect the state of the art and address normal protection needs. In addition, the modules of the IT-Grundschutz Compendium offer suggestions for Requirements in Case of Increased Protection Needs. For reference purposes, the requirements are clearly numbered across all modules, e.g. SYS.3.4.A2. According to this schema, the layer is specified first ("SYS" in the example), followed by the numbers of the respective sublayer and module ("3.4") and finally the requirement itself ("A2"). If matching Implementation Guidance is available, the safeguard mentioned in the recommendations for requirement "A" will have the same number with a preceding letter "M" – "SYS.3.4.M2" in this example case.

Each module describes who is responsible for its implementation. The role that is generally responsible is always specified. There can be additional roles with further responsibilities in implementing requirements. These are indicated in the title of the requirement in square brackets. The Chief Information Security Officer (CISO) must always be involved in strategic

decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

In the headings of the requirements, the requirement titles are supplemented by an abbreviation in addition to the roles to be involved in order to make it directly apparent (even outside the context of the respective module) whether the requirement is a "Basic Requirement" (B), a "Standard Requirement" (S), or a "Requirement in Case of Increased Protection Needs" (H).

At the end of the module, additional information and cross-references are listed. In addition, an appendix to the modules contains a cross-reference table where the relevant Elementary Threats are linked to the requirements. These associations can be used for risk analysis.

Modal Verbs

In the modules of the IT-Grundschutz Compendium, the evaluation aspects of the requirements are formulated using the modal verbs MUST and SHOULD (along with the associated negations) in capital letters in order to make the guidance as clear as possible. The modal verbs are conjugated in line with the relevant grammatical rules. When negations are used, the two words may be separated.

The definition used here is based on RFC 2119 (Key Words for Use in RFCs to Indicate Requirement Levels, version 1997) and DIN 820-2:2012, appendix H.

MUST / MUST ONLY / MAY ONLY:

This term means it is imperative that the requirement be fulfilled (absolute requirement).

MUST NOT:

This term means that something must not be done under any circumstances (absolute prohibition).

SHOULD:

This term means that the requirement must be fulfilled under normal circumstances, but there may be reasons to the contrary. These must be carefully assessed and well founded, however.

SHOULD NOT:

This term means that something should not be done under normal circumstances, but there may be reasons to do it. These must be carefully assessed and well founded, however.

Basic Requirements are formulated as follows:

xyz MUST be done. xyz MUST NOT be done.

Standard Requirements and Requirements in Case of Increased Protection Needs are expressed in the following form:

xyz SHOULD be done. xyz SHOULD NOT be done.

Individual statements in the Basic Requirements can be expressed with “SHOULD”. These partial requirements in the Basic Requirements do not necessarily have to be fulfilled, but do

occur in connection with binding MUST requirements and complement them with additional aspects. An excerpt from module OPS.1.2.2 *Archiving* is shown below as an example:

OPS.1.2.2.A8 Logging Archival Access [IT Operation Department] (B)

All attempts to access electronic archives MUST be logged. To this end, dates, times, users, client systems, the actions performed, and any error messages SHOULD be recorded. [...]

It is imperative that all attempts to access an electronic archive be logged. The first requirement is therefore a partial MUST requirement. Whether or not all the data mentioned, such as the user or client, can be recorded in detail can depend on technical or legal framework conditions (among other things). As a result, the second requirement is a partial SHOULD requirement.

Partial requirements can be expressed with "MUST" in Standard Requirements, as well. These are aspects that must be fully met when the requirement is implemented. An excerpt from Standard Requirement ISMS.1.A10 *Drawing Up a Security Concept* (from module ISMS.1 *Security Management*) is shown below as an example:

ISMS.1.A10 Drawing Up a Security Concept (S)

For the specified scope (the information domain), an adequate security concept SHOULD be drawn up as the central document in the security process. [...] In the security concept, specific security safeguards appropriate for the information domain under consideration MUST be derived from the security objectives of the organisation, the protection needs identified and the risk evaluation conducted. [...]

The creation of a security concept is important. Since this usually involves a great deal of effort, it often cannot be completed as a matter of priority in practice. Drawing up a security concept is therefore a partial SHOULD requirement. However, certain activities are mandatory when creating a security concept, which makes them partial MUST requirements. This includes the fact that appropriate security safeguards must be derived from the security objectives of the organisation and the protection needs identified.

In addition, there may be individual partial MUST requirements for Standard Requirements which only need to be met under certain conditions. If, for example, communication links SHOULD be encrypted, the encryption method used MUST also be suitable for this purpose.

In the case of Requirements in Case of Increased Protection Needs, the modal verb SHOULD is mainly used. These requirements result from best practices and should be evaluated within the scope of risk analysis.

Cross-Reference Tables

Each module includes an appendix with an overview of the relevant Elementary Threats. The relationship between the Elementary Threats of IT-Grundschutz and the requirements of the module can be obtained from the cross-reference tables. They can also be found in the appendix to the module.

All cross-reference tables have the same layout. The column headers contain the numbers of the Elementary Threats listed in the corresponding module. The first column contains the numbers of the requirements.

The remaining columns describe the specific relationships between the requirements of the module and the Elementary Threats. If an "X" is entered in a field, this means that the requirement is effective in counteracting the corresponding threat. This can avoid or minimise damage.

It should be noted that a requirement is not automatically superfluous if none of the threats associated with it in a table are relevant to a certain application case. Whether or not a requirement is necessary must always be checked and documented on a case-by-case basis according to the overall security concept in question and not solely based on the cross-reference table.

Revision of IT-Grundschutz Modules

IT-Grundschutz undergoes continuous further development. In this respect, the IT-Grundschutz Compendium is not only supplemented by modules on new topics; the existing modules are also regularly revised so that the contents correspond to the current state of the art.

If individual requirements of a module change, it may be necessary for IT-Grundschutz users who have already implemented the module to adapt their existing security concepts. In order to facilitate this, the BSI provides change logs with respect to the previous year's edition of the IT-Grundschutz Compendium. These list all the changes made to modules that go beyond minor linguistic or editorial issues. All the changes are documented in the section “What’s New in the IT-Grundschutz Compendium”.

Note: The initial numbering of the individual requirements will remain the same following revisions to modules in future editions. This ensures, for example, that security concepts or IT-Grundschutz profiles that refer to specific requirements will still contain the correct references even after the respective module has been updated. This means that when requirements are added, removed or moved within a module, they may no longer be numbered in ascending or continuous order. If, for example, a module that has previously comprised five Basic Requirements (“A1” to “A5”) and 10 Standard Requirements (“A6” to “A15”) is supplemented by a new Basic Requirement, this new requirement is assigned the number “A16” and placed between “A5” and “A6” at the end of section 3.1, "Basic Requirements”.

Implementation Recommendations

Detailed Implementation Guidance is available for many modules in the IT-Grundschutz Compendium. It describes how the requirements of the modules can be implemented and explains suitable security safeguards in detail. The safeguards can be used as a basis for security concepts, but should be adapted to the framework conditions of the relevant organisation.

Implementation Guidance addresses the groups of persons that are responsible for the implementation of the module requirements – for example, the IT Operation Department or Building Services. It is not part of the IT-Grundschutz Compendium; it is published as auxiliary resources for the modules.

Since many security requirements are usually covered by higher-level modules, Implementation Guidance can include safeguards for several modules. For example, module SYS.3.2.1 *General Smartphones and Tablets* includes a requirement regarding the use of access protection. This applies to all smartphones and tables, regardless of the operating system. The

Implementation Guidance for SYS.3.2.3 *iOS (for Enterprise)* then describes safeguards specific to iOS to meet this general requirement from SYS.3.2.1.

The safeguards found in Implementation Guidance are numbered in ascending order, with a clear association between the safeguards (marked M) and the requirements (marked A). Implementation Guidance does not distinguish between requirement categories.

Ways to Apply the IT-Grundschutz Compendium

To successfully establish an ISMS, BSI Standard 200-2, *IT-Grundschutz Methodology* (together with the IT-Grundschutz Compendium) provides a multitude of information on the methodologies for Basic, Core and Standard Protection, as well as practical implementation resources. In addition to this, there are potential solutions for various tasks relating to information security – for example, security design, auditing and certification. Depending on the task at hand, different ways of using IT-Grundschutz may be appropriate.

Layer Model and Modelling

When implementing IT-Grundschutz, the information domain under consideration must be modelled with the help of the existing modules. This means that the relevant security requirements must be compiled from the IT-Grundschutz Compendium. To this end, all processes, applications and IT systems must be recorded or a structure analysis (and usually a determination of the protection needs at hand) must be available. Building upon these documents, an IT-Grundschutz model of the information domain is developed that consists of the various IT-Grundschutz modules—some of which may be used several times—and a mapping of these modules to the security-relevant aspects of the information domain.

Whether the information domain consists of IT systems already in use or is still in the planning stages does not matter for the IT-Grundschutz model developed. The model can thus be used in different ways:

- The IT-Grundschutz model of an information system *already implemented* identifies the relevant security requirements based on the modules used. It can be used in the form of a Gap Analysis Plan to compare current circumstances to the target situation.
- The IT-Grundschutz model of a *planned* information system, on the other hand, constitutes a development concept. Using the selected modules, it describes the security requirements that need to be met during the implementation of the information domain.

Typically, an information domain currently in use comprises both implemented components and others that are still being planned. The resulting IT-Grundschutz model then contains both a Gap Analysis Plan and some elements of a development concept. Together, all the security requirements envisaged in the Gap Analysis Plan and development concept form the basis on which an IT security concept can be produced.

In general, the corresponding modules of the IT-Grundschutz Compendium must be selected and implemented in order to model a complex information domain in line with IT-Grundschutz. In this IT-Grundschutz Compendium, the modules are separated into process and system modules and further divided into individual layers to facilitate selection:

Process Modules:

The process modules, which in general are equally applicable to all or major parts of an information system, are divided into the following layers, which again can consist of further sublayers.

- The ISMS layer includes the *Security Management* module as a basis for all further activities in the security process.
- The ORP layer addresses organisational and personnel security aspects. This layer includes, for example, the modules *Organisation* and *Personnel*.
- The CON layer includes modules that deal with concepts and methodologies. Typical modules of the CON layer include *Crypto Concept* and *Data Protection*.
- The OPS layer comprises all security aspects of an operational nature. This particularly includes the security aspects of IT operations in both in-house environments and those

that are run partially or completely by third parties. Furthermore, it includes the security aspects that are to be considered when running IT operations for third parties. Examples of modules in the OPS layer include *Protection Against Malware* and *Outsourcing for Customers*.

- The DER layer contains all the modules which are relevant for reviewing the implemented security safeguards, detecting security incidents and taking suitable action in response. Typical components of the DER layer are *Security Incident Handling* and *Provisions for IT Forensics*.

In addition to the process modules, the IT-Grundschutz Compendium also includes system modules. In general, these are applied to individual target objects or groups of target objects. The system modules are divided into the layers below. Like the process modules, system modules can also contain further sublayers.

System Modules:

- The APP layer deals with the protection of applications and services in communications, directory services, network-based services and business and client applications, amongst other areas. Typical modules within the APP layer include *General E-Mail Clients and Servers*, *Office Products*, *Web Servers* and *Relational Database Systems*.
- The SYS layer addresses the individual IT systems of a given information domain that may have been combined into groups. The security aspects of servers, desktop systems, mobile devices and other IT systems such as printers and telecommunication systems are addressed here. The SYS layer includes, for example, modules for specific operating systems, as well as *General Smartphones and Tablets* and *Printers, Copiers, and All-in-One Devices*.
- The IND layer deals with the security aspects of industrial IT. This layer includes modules such as *Process Control and Automation Technology*, *General ICS Components* and *Programmable Logic Controller (PLC)*.
- The NET layer examines the networking aspects not primarily related to specific IT systems, but to network connections and communication. It includes, for example, the modules *Network Management*, *Firewall* and *WLAN Operation*.
- The INF layer brings together different aspects of infrastructural security by addressing architectural and technical factors. It includes the modules *Generic Building* and *Data Centre and Server Room*.

Modelling

IT-Grundschutz modelling entails determining whether and how the modules of each layer can be used to map a given information domain. Depending on the module at hand, this can involve different target objects, such as applications, IT systems, groups of components, rooms and buildings.

In the individual modules, section 1.3, "Scoping and Modelling", describes in detail when a module should be used and the target objects to which it should be applied.

When modelling an information domain according to IT-Grundschutz, there may be target objects that cannot be mapped adequately using the existing IT-Grundschutz modules. In this case, a risk analysis must be performed as described in the IT-Grundschutz Methodology.

Many sublayers include general modules that describe fundamental aspects that also apply generally to the specific modules in question. For instance, SYS.2.1 *General Client* includes requirements for *all* client operating systems, which are then specified and expanded for macOS, Windows, and Unix/Linux clients in the corresponding modules. For additional examples, consider APP.2.1 *General Directory Service* or SYS.3.2.1 *General Smartphones and Tablets*. Specific modules should always be use alongside the general modules. Furthermore, general modules provide a good basis for modelling and risk analysis if no specific module exists for a particular target object.

The following table provides an initial overview of the target objects to which the modules are to be applied in each case and the order in which the modules can be implemented (for an explanation of R1, R2 and R3, please see section 2.2, *Processing Order of the Modules*).

There are modules that can be clearly associated with target object types such as IT systems, applications, or information domains/generic aspects—that is, they deal *exclusively* or *predominately* with these aspects. Some modules, such as OPS.1.2.4 *Teleworking* or INF.9 *Mobile Workplace*, *cannot* be clearly associated with target object types because they address different aspects. Teleworking, for example, deals with aspects of IT systems, communication links, information flow, backups and so on. These modules therefore have an impact on the entire information domain and are therefore associated with the target object "Information domain/generic aspects".

The assignment to the target objects is given as an example and serves for better classification and easier understanding. In the individual implementation of IT-Grundschutz, for example, an assignment of a module to "information domains/generic aspects" does not mean that this target object type must be created. Rather, it means that the module can have an impact on the entire information network and thus, if necessary, on several target objects.

Module	**Order**	**To be applied to Target Object Type**
ISMS.1 Security Management	R1	Information domain/generic aspects
ORP.1 Organisation	R1	Information domain/generic aspects
ORP.2 Personnel	R1	Information domain/generic aspects
ORP.3 Awareness and Training in Information Security	R1	Information domain/generic aspects
ORP.4 Identity and Access Management	R1	Information domain/generic aspects
ORP.5 Compliance Management	R3	Information domain/generic aspects
CON.1 Crypto Concept	R3	Information domain/generic aspects
CON.2 Data Protection	R2	Information domain/generic aspects
CON.3 Backup Concept	R1	Information domain/generic aspects
CON.6 Deleting and Destroying Data and Devices	R1	Information domain/generic aspects

CON.7 Information Security on Trips Abroad	R3	Information domain/generic aspects
CON.8 Software Development	R3	Information domain/generic aspects
CON.9 Information Exchange	R3	Information domain/generic aspects
CON.10 Development of Web Applications	R2	Information domain/generic aspects
OPS.1.1.2 Proper IT Administration	R1	Information domain/generic aspects
OPS.1.1.3 Patch and Change Management	R1	Information domain/generic aspects
OPS.1.1.4 Protection Against Malware	R1	Information domain/generic aspects
OPS.1.1.5 Logging	R1	Information domain/generic aspects
OPS.1.1.6 Software Tests and Approvals	R1	Information domain/generic aspects
OPS.1.1.7 System Management	R2	Information domain/generic aspects
OPS.1.2.2 Archiving	R3	Information domain/generic aspects
OPS.1.2.4 Teleworking	R2	Information domain/generic aspects
OPS.1.2.5 Remote Maintenance	R3	Information domain/generic aspects
OPS.1.2.6 NTP Time Synchronisation	R2	Application
OPS.2.1 Outsourcing for Customers	R2	Information domain/generic aspects
OPS.2.2 Cloud Usage	R2	Information domain/generic aspects
OPS.3.1 Outsourcing for Service Providers	R3	Information domain/generic aspects
DER.1 Detecting Security-Relevant Events	R1	Information domain/generic aspects
DER.2.1 Security Incident Handling	R1	Information domain/generic aspects
DER.2.2 Provisions for IT Forensics	R3	Information domain/generic aspects
DER.2.3 Clean-Up of Extensive Security Incidents	R3	Information domain/generic aspects
DER.3.1 Audits and Revisions	R3	Information domain/generic aspects
DER.3.2 Audits Based on the BSI “Guideline for IS Audits”	R3	Information domain/generic aspects
DER.4 Business Continuity Management	R3	Information domain/generic aspects
APP.1.1 Office Products	R2	Application
APP.1.2 Web Browsers	R2	Application

APP.1.4 Mobile Applications (Apps)	R2	Application
APP.2.1 General Directory Service	R2	Application
APP.2.2 Active Directory	R2	Application
APP.2.3 OpenLDAP	R2	Application
APP.3.1 Web Applications and Web Services	R2	Application
APP.3.2 Web Servers	R2	Application
APP.3.3 File Servers	R2	Application
APP.3.4 Samba	R2	Application
APP.3.6 DNS Servers	R2	Application
APP.4.2 SAP ERP Systems	R2	Application
APP.4.3 Relational Database Systems	R2	Application
APP.4.4 Kubernetes	R2	Application
APP.4.6 SAP ABAP Programming	R2	Application
APP.5.2 Microsoft Exchange and Outlook	R2	Application
APP.5.3 General E-Mail Clients and Servers	R2	Application
APP.6 General Software	R2	Application
APP.7 Development of Individual Software	R3	Information domain/generic aspects
SYS.1.1 General Server	R2	IT system
SYS.1.2.2 Windows Server 2012	R2	IT system
SYS.1.3 Linux and Unix Servers	R2	IT system
SYS.1.5 Virtualisation	R2	IT system
SYS.1.6 Containerisation	R2	IT system
SYS.1.7 IBM Z	R2	IT system
SYS.1.8 Storage Solutions	R2	IT system
SYS.2.1 General Client	R2	IT system
SYS.2.2.2 Windows 8.1 Clients	R2	IT system
SYS.2.2.3 Windows 10 Clients	R2	IT system
SYS.2.3 Linux and Unix Clients	R2	IT system
SYS.2.4 macOS Clients	R2	IT system
SYS.3.1 Laptops	R2	IT system
SYS.3.2.1 General Smartphones and Tablets	R2	IT system
SYS.3.2.2 Mobile Device Management (MDM)	R2	Information domain/generic aspects
SYS.3.2.3 iOS (for Enterprise)	R2	IT system
SYS.3.2.4 Android	R2	IT system
SYS.3.3 Mobile Telephones	R2	IT system
SYS.4.1 Printers, Copiers, and All-in-One Devices	R2	IT system
SYS.4.3 Embedded Systems	R2	IT system
SYS.4.4 General IoT Devices	R2	IT system
SYS.4.5 Removable Media	R2	IT system
NET.1.1 Network Architecture and Design	R2	Network
NET.1.2 Network Management	R2	IT system
NET.2.1 WLAN Operation	R2	Network
NET.2.2 WLAN Usage	R2	IT system
NET.3.1 Routers and Switches	R2	IT system
NET.3.2 Firewall	R2	IT system
NET.3.3 VPN	R2	IT system

NET.4.1 Telecommunications Systems	R2	IT system
NET.4.2 VoIP	R2	Network
NET.4.3 Fax Machines and Fax Servers	R2	IT system
IND.1 Process Control and Automation Technology	R2	Information domain/generic aspects
IND.2.1 General ICS Components	R2	IT system
IND.2.2 Programmable Logic Controller (PLC)	R2	IT system
IND.2.3 Sensors and Actuators	R2	IT system
IND.2.4 Machine	R2	IT system
IND.2.7 Safety Instrumented Systems	R2	IT system
IND.3.2 Remote Maintenance in Industry	R2	IT system
INF.1 Generic Building	R2	Building/room
INF.2 Data Centre and Server Room	R2	Building/room
INF.5 Room or Cabinet for Technical Infrastructure	R2	Building/room
INF.6: Storage Media Archives	R2	Building/room
INF.7 Office Workplace	R2	Building/room
INF.8 Working from Home	R2	Building/room
INF.9 Mobile Workplace	R2	Information domain/generic aspects
INF.10 Meeting, Event, and Training Rooms	R2	Building/room
INF.11 General Vehicle	R3	Building/room
INF.12 Cabling	R2	Building/room
INF.13 Technical Building Management (TBM)	R2	Building/room
INF.14 Building Automation and Control Systems (BACS)	R2	Building/room

Processing Order of the Modules

The essential security requirements must be fulfilled early, and corresponding security safeguards must be implemented to cover basic risks and establish holistic information security. This is why IT-Grundschutz proposes an order in which modules should be implemented (see section 2.1, *Modelling*).

- R1: These modules should be implemented with priority because they are the basis for an effective security process.
- R2: These modules should be implemented next because they are required to achieve sustainable security in essential parts of an information domain.
- R3: These modules are also needed to achieve the desired security level and must be implemented. The BSI recommends considering these after the other modules.

These designations serve to describe a sensible order in which the requirements of a given module can be implemented; it is not meant to indicate that any module has any more weight than another. In principle, all the modules of the IT-Grundschutz Compendium that are relevant to the information domain under consideration must be implemented.

Roles

Compliance Manager

A Compliance Manager is responsible for identifying the statutory, contractual, and other specifications relevant to their organisation and checking them for compliance.

Audit Team

An Audit Team is composed of auditors and professional experts who support the Audit Team leader with technical advice during audits.

Construction Manager

A Construction Manager is responsible for the execution of construction projects.

User

A User is an employee in an organisation who uses information technology to perform their tasks. IT Users and Users are considered synonymous in this case because today, almost every employee of a given organisation uses information technology to perform their tasks.

Area Security Officer

An Area Security Officer is responsible for all security issues relating to business processes, applications, and IT systems in their area (e.g. a department or remote office). Depending on the size of the business unit at hand, the responsibilities of an Area Security Officer can be assumed by someone who is already entrusted with similar tasks.

Procurement Department

A Procurement Department initiates and monitors acquisitions. Government organisations follow defined procedures for procurement. The Procurement Department role includes the responsible organisational unit head.

Fire Safety Officer

A Fire Safety Officer is responsible for all issues relating to fire safety and serves as a contact person in this regard. Amongst other things, this person is responsible for drawing up fire risk analyses, training and education programmes for employees, and sometimes even for maintaining and servicing fire safety equipment.

Data Protection Officer

A Data Protection Officer is a person appointed by an organisation's Top Management who is responsible for ensuring that personal data is handled correctly and in a legally compliant manner within the organisation.

Developer

In the context of IT-Grundschutz, a Developer is a person involved in the development of software, hardware, or entire systems. Within the framework of IT-Grundschutz, the Developer role summarises many different roles, e.g. Software Architect, Software Designer,

Software Developer, Computer Programmer, and Tester. The Developer role includes the responsible organisational unit head.

Construction Company

A Construction Company is a company that installs a certain type of equipment, but can also include those that construct buildings.

Department

A Department is a part of an organisation that is responsible for performing certain specialised tasks. In state and federal administrations in Germany, a Department is an organisational unit consisting of several sub-departments with related tasks.

Process Owner

A Process Owner is responsible for the content of one or more business processes or specialised procedures. In IT-Grundschutz, various other roles are grouped together under the role of Process Owner. These include the roles of change manager and archive administrator.

Building Services

Building Services is the organisational unit responsible for the infrastructure in a building or on a property. Examples of this infrastructure include electrical engineering, signalling and control technology, security technology, IT networks (in the physical sense), heating and sanitary engineering, and lifts and escalators. The Building Services role includes the responsible organisational unit head.

ICS Information Security Officer

An ICS Information Security Officer (often also known as an Industrial Security Officer) is a person appointed by an organisation's Top Management to ensure that special requirements in the area of industrial control are covered and that the ICS security organisation is integrated into the overall scope of the ISMS in place.

Chief Information Security Officer (CISO)

A CISO is a person appointed by an organisation's Top Management to coordinate and advance tasks pertaining to information security.

Organisation

In this context, the term “organisation” refers to companies, public authorities, and other public and private organisations.

Top Management

This term refers to the executive management level of the organisation or organisational unit under consideration.

IS Audit Team

An IS Audit Team is composed of IS auditors and professional experts who support the person in charge of an IS audit, particularly from a technical perspective.

IT Operation Department

An IT Operation Department is an organisational unit that configures, operates, monitors, and maintains internal IT. The IT Operation Department role includes the responsible organisational unit head.

Employee

An employee is part of an organisation.

BCM Officer

A BCM Officer controls all activities in the field of business continuity management. They responsible for drawing up, implementing, maintaining, and supporting the organisation-wide emergency management process and of the corresponding documents, regulations, and safeguards. They analyse the overall BCM procedure that is to be followed should an event of damage occur.

OT Operations (Operational Technology, OT)

OT Operations is responsible for configuring, operating, monitoring, and maintaining ICS systems.

Head of OT

A Head of OT (also known as the Head of Production and Manufacturing) directs production and manufacturing and/or bears responsibility for the industrial control systems (ICS) used by their organisation.

A Head of OT is also responsible for assessing information security risks to the integrity of safety instrumented systems (SIS) and taking appropriate state-of-the-art safeguards. In particular, they are responsible for training their organisation's workforce on information security issues.

Human Resources Department

A Human Resources Department is responsible for the following tasks, among others:

- Basic issues relating to human resources
- Planning staff requirements
- Managing employees' HR-related matters
- Support for employees in social issues
- General co-operation with the personnel representatives

The Human Resources Department role includes the responsible organisational unit head.

Planner

The general term "planner" includes roles such as a "network planner" and "construction planner". This term refers to persons responsible for planning and designing specific tasks.

Tester

Testers are people who test new or changed software and/or hardware and compare the results against the corresponding expectations according to procedures and criteria previously specified in a test plan.

Supervisor

A Supervisor is an employee of an organisation who is authorised to assign jobs to the employees in their area.

Maintenance Personnel

Maintenance Personnel are employees of external service providers who have been commissioned with the maintenance of technical systems (e.g. ICS or IT systems) in a given information domain. It is usually necessary for Maintenance Personnel to have access to the systems in question.

Central Administration

This organisational unit regulates and supervises general operations and plans, organises, and carries out all administrative services. The Central Administration role includes the responsible organisational unit head.

Glossary

This glossary explains the most important terms related to information security and IT-Grundschutz. An additional glossary (in German) on cyber security can be found on the BSI website at https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html.

Requirement in case of increased protection needs

See “Security requirement”.

Attack

An attack is a deliberate form of threat, namely an undesired or unauthorised action executed with the goal of gaining advantages and/or causing damage to third parties. Attackers may also act on behalf of third parties who wish to gain an advantage through the attack.

Assets

Assets refer to inventories of objects which are required for a specific purpose, in particular to meet business objectives. As a synonym for “asset”, the German term “*Wert*” (English: value) is often used. However, the term “value” has a wide range of meanings, from the social relevance of something to the intrinsic quality of an object. In IT-Grundschutz, the term “assets” should be understood as “valuable target objects”.

Authentication

Authentication refers to the process of proving or verifying authenticity. An identity can be authenticated, amongst other means, by a password, chip card, or biometry; data, meanwhile, can be authenticated using cryptographic signatures (for example).

Authenticity

In the context of IT-Grundschutz, authenticity is a characteristic ascribed to a communication partner who actually is who they claim to be. Authentic information is information guaranteed to have been created by the source specified. This term is used not only when checking the identity of persons, but with regard to IT components and applications, as well.

Authorisation

An authorisation process checks whether a person, an IT component, or an application has permission to perform a specific action.

Basic Protection

Basic Protection enables organisations to implement broad and fundamental initial safeguards across all their business processes and/or specialist procedures as a first step in applying IT-Grundschutz.

Basic Requirement

See “Security requirement”.

Modules

The IT-Grundschutz Compendium contains explanations regarding threat landscapes, security requirements, and additional information that are summarised in modules on specific processes, components, and IT systems. Based on this modular structure, the IT-Grundschutz Compendium focuses on presenting the key security requirements in each topic area. The basic structure the IT-Grundschutz Compendium is divided into process-oriented and system-oriented modules, which are also categorised by subject in a layer model.

IT Security Officer

A person with technical competence in IT security who is in charge of aspects related to IT security in a large organisation and cooperates closely with the IT Operations Department. The Chief Information Security Officer (CISO) designs information security management and establishes general security objectives and provisions; an IT Security Officer ensures that these are implemented on the technical side. An IT Security Officer thus usually operates in the field of IT, whilst a CISO reports directly to the management level.

Basic threat

In general terms, a threat is an event or condition which involves the risk of damage. The possible damage in this case relates to actual value - in terms of financial assets, knowledge, objects, or people's health, for example. In IT terms, a basic threat is a condition or event which can negatively affect the availability, integrity, or confidentiality of information, which in turn may result in damage to the owner and/or user of the information. Examples of basic threats include force majeure, human error, technical failure, and deliberate acts. If a basic threat encounters a vulnerability (technical or organisational shortcomings in particular), an applied threat arises.

BIA (business impact analysis)

A Business Impact Analysis (consequential damage analysis) is an analysis designed to determine potential direct and indirect consequential damage for an organisation caused by the occurrence of an emergency or a crisis and the failure of one or several business processes. It is a procedure designed to identify critical resources and recovery requirements, as well as the effects of unscheduled interruptions in business operations.

Business continuity management

Business continuity management (BCM) refers to all organisational, technical, and personnel safeguards that serve to ensure the continuity of the core business of a public authority or company when an emergency and/or a security incident occurs. Furthermore, BCM also supports the successive continuation of business processes during long-term failures or malfunctions.

Cyber security

Cyber security addresses all aspects of security in the fields of information and communications technology. The key tasks of information security are thus extended to all of cyberspace. Cyberspace includes all the information technology connected to the Internet and comparable networks, as well as communications, applications, processes, and processed

information based thereon. Considerations of the subject of cyber security often include a specific focus on attacks from cyberspace.

Privacy Policy

Data protection seeks to safeguard individuals' right to privacy from being violated through improper handling of their personal data. Data protection is therefore used to refer to the protection of personal data against eventual misuse by third parties (not to be confused with the term data security).

In English, “data protection” refers to data protection as a legal term. The term “privacy”, on the other hand, is more directly related to the lives of people (i.e. the protection of their privacy) and is used primarily in the United States, although its use is becoming more common in the European Union.

Data protection management

Data protection management refers to the processes necessary to ensure the implementation of the legal requirements of data protection law when planning, configuring, and operating procedures used to process information, as well as after these procedures are taken out of operation.

Data security

Data security refers to the protection of data in connection with stipulated requirements regarding confidentiality, availability and integrity. A modern term for this is “information security”.

Specialised task

Specialised tasks are those that relate to an organisation’s specific purpose or mission. In IT-Grundschutz, the term “specialised tasks” refers to the business processes of public authorities.

Danger

"Danger" is often regarded as a generic term, whereas "threat" is understood as a danger described in more detail (with regard to type, scope, and direction, as well as in spatial and temporal terms). For example, the potential loss of data is a danger. Loss of data may occur due to a defective hard disk or as the result of a hard disk being stolen by a thief, among other things. The threats in this case thus include "defective storage media" and "theft of storage media". However, since this differentiation is not made consistently in the related literature and its significance is more academic in nature, "danger" and "threat" can be deemed synonymous.

Applied threat

An applied threat is a basic threat that has a direct effect on an object as the result of a vulnerability. A basic threat therefore only becomes an applied threat to an object when it is combined with a vulnerability.

For example, is malware a basic or an applied threat to a user who is surfing the Internet? According to the above definition, all users are exposed in principle to the basic threat of malware on the Internet. A user who downloads a file infected with malware is then exposed

to an applied threat if their IT system is vulnerable to this type of malware. Users with effective anti-virus protection, a configuration that will prevent the malware from working, or an operating system incapable of executing the malware code, however, will not be exposed to an applied threat if they download this harmful software.

Business process

A business process is a set of logically linked individual activities (tasks, workflows) that are carried out to meet commercial or operational objectives.

Key security objectives

IT-Grundschutz defines three key security objectives: confidentiality, availability, and integrity.

Each IT-Grundschutz user is, of course, free to include additional key security objectives when assessing protection requirements if this is helpful in individual cases. Further generic umbrella terms in the field of information security include authenticity, liability, reliability, and non-repudiation.

Industrial control system (ICS)

ICS is a generic term for automation solutions that are used to control technical processes.

An industrial control system (ICS, IACS) is an integrated hardware and software solution for automation that includes sensors, actuators, and their networking, as well as procedures for evaluating and controlling primarily industrial processes. Processes for the operation of machines are automated through continuous measurement and control.

Information security

The aim of information security is to protect information. This information might be stored on paper, in IT systems, or inside people's heads. The primary objectives (or "core values") of information security are confidentiality, integrity, and availability. Many users include additional core values in their considerations.

Chief Information Security Officer (CISO)

A Chief Information Security Officer (CISO) is responsible for achieving and maintaining information security from a operative standpoint. A CISO may also be referred to as an information security manager (ISM). The role of CISO should be assumed by a person in the administrative executive department of a company or public authority who has expertise in information security.

Information security management

The planning, management, and control activities that are essential in establishing and continuously implementing a thoroughly thought through and effective process for ensuring information security are referred to as information security management. This is a continuous process that involves monitoring strategies and concepts on an ongoing basis in terms of their performance and effectiveness and updating them as required.

Information security management team

In larger organisations, it makes sense to establish an IS management team (often also referred to as an IT security management team) to support the CISO—for example, by coordinating comprehensive safeguards in the overall organisation at hand, compiling information, and performing monitoring tasks.

Information security audit based on IT-Grundschutz (IS audit)

Information security auditing is part of every successful information security management system. Only by regularly reviewing established security safeguards and the overarching information security process is it possible to determine whether they are being implemented in an efficient, up-to-date, complete, and appropriate manner and thereby assess the respective organisation's currently level of information security. Hence, an IS audit is a tool for determining, achieving, and maintaining an appropriate level of security within an organisation.

Information domain

An information domain refers to all the infrastructural, organisational, personnel-related, and technical objects that are used to perform tasks in a particular field of application in information processing. An information domain may refer to an entire organisation or to individual areas defined by organisational structures (e.g. departments), or by joint business processes and/or shared applications (e.g. an HR information system).

Infrastructure

In terms of IT-Grundschutz, infrastructure is understood to include the buildings, rooms, power supplies, air conditioning systems, and cabling used for IT. IT systems and network switching elements are not part of infrastructure.

Organisation

In this context, the term “organisation” refers to companies, public authorities, and other public and private organisations.

Integrity

Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term "integrity" is used in connection with the term “data”, it means that the data in question is complete and unchanged. In information technology terms, however, integrity is typically used more broadly to describe “information”. The term “information” is used for data that, depending on the context, can be associated with certain attributes, such as the author or the time and date of creation. Loss of the integrity of information can therefore mean that it was changed without authorisation, the information regarding the author was tampered with, or that the date of creation was manipulated.

IT-Grundschutz Check

In IT-Grundschutz, this term (which has replaced the term "basic security check") refers to the investigation of whether the requirements recommended by IT-Grundschutz have already been met in an organisation and which basic security requirements still need to be fulfilled.

IT-Grundschutz Compendium

The modules of IT-Grundschutz make up the IT-Grundschutz Compendium. It is the successor to the IT-Grundschutz Catalogues, which were available up to their 15th version.

IT system

IT systems are closed technical and functional units designed for information processing. Typical examples include servers, clients, mobile phones, smartphones, tablets, IoT components, routers, switches, and firewalls.

Core protection

Core protection focuses primarily on business processes and assets that are particularly exposed to risks.

Components

In software architecture, a component is an independently usable unit with external interfaces that can be connected to other components. It is both functionally and technically independent and has a certain value (in the economic sense).

In IT-Grundschutz, the term "components" refers to technical target objects (see "target object") or parts thereof.

Crown jewels

Crown jewels are assets that are so crucial to an organisation that its existence would be threatened if they were to be stolen, destroyed, or otherwise compromised.

Cumulative effect

The cumulative effect describes the fact that the protection requirement of an IT system needs to be increased when the accumulation of several (small-scale) damages to an IT system can lead to a higher total damage. One possible case is, for example, if several IT applications or a number of sensitive items of information are processed on an IT system, so that the cumulative effect can result in greater overall damage.

Information security policy

This policy document is central to the information security of an organisation. It describes how information security is to be established in the organisation, for which purposes, and with which resources and structures. It contains the information security objectives aimed at by the organisation and the information security strategy pursued. Through these defined objectives, an information security policy therefore also describes the level of security an organisation is seeking to attain.

Maximum principle

According to the maximum principle, the potential damage or the total damage with the most serious effects determines the protection requirements of a business process, an application, or an IT system.

Modelling

When applying the IT-Grundschutz methodology, the modelling phase involves mapping the information domain considered in a given organisation with the help of the modules from the

IT-Grundschutz Compendium. To this end, the “Not in Scope and Modelling” section of each module contains information on the target objects to which it should be applied and the requirements that may need to be taken into account.

Network plan

A network plan is a graphical overview of the components in a network and their connections.

Non-repudiation

Here, the main focus is on the verifiability of third parties. The aim is to ensure that the sending and receiving of data and information cannot be denied. A differentiation is made between the following:

- Non-repudiation of origin: It should be impossible for the sender to deny having sent a certain message after the fact.
- Non-repudiation of receipt: It should be impossible for the recipient to deny having received a certain message after the fact.

Risk

Risk is also often defined as the combination (i.e. the product) of the likelihood and extent of damage. Damage, meanwhile, is frequently described as the difference between a planned and an unplanned result. Risk is a special form of uncertainty or, more accurately, imponderability.

A CISO also defines risk as the result of imponderables regarding target objects. Along these lines, the term "consequences" is sometimes used rather than "damage" if events occur that deviate from the corresponding expectations. A consequence may be negative (damage) or positive (opportunity). However, the above-mentioned definition has proved more common in practice.

In contrast to the term “applied threat”, the term “risk” already includes an assessment of the extent to which a certain damage scenario is relevant to the scenario under consideration.

Risk analysis

Risk analysis refers to the complete process of determining (identifying, assessing, and evaluating) and treating risks. According to the relevant ISO standards ISO 31000 and ISO 27005, risk analysis is only one part of risk determination, which consists of the following steps:

- Risk identification
- Risk analysis
- Risk evaluation

In the meantime, however, the term "risk analysis" has been established for the entire process of risk determination and risk treatment. Therefore, the term "risk analysis" is still used in this document to refer to the comprehensive process.

Risk appetite (also "risk propensity" or "willingness to take risks")

Risk appetite refers to an organisation's tendencies in assessing and dealing with risks based on its cultural, internal, external, and economic influences.

Risk treatment plan

Meeting all the Basic and Standard Requirements of IT-Grundschutz and any applicable requirements in case of increased protection needs is a considerable challenge for any organisation. In practice, not all requirements can be met due, for example, to circumstances that make meeting them unreasonable (procurement of new information technology, plans to move, etc) or impossible based on the organisational or technical framework conditions at hand (such as when a particular IT system or application is simply not used). Existing deficits in the implementation of security safeguards that pertain to the security requirements at hand and their related risks must be documented in the form of a management report, which should include an implementation plan for the further treatment of the risks present. This risk treatment plan should include a description of the resources planned and the time constraints to be observed. It must be signed and approved by the respective organisation's top management.

The individual requirements of the risk treatment plan must be reviewed at least once a year. An organisation's top management must avoid assuming risks for an extended and undefined period of time because such risks can change in a short time in the field of information security. Assuming risks for an undefined period of time involves the danger that they may only be reviewed and evaluated on a particular reference date and not reconsidered thereafter.

Risk management

Risk management refers to all activities involving the strategic and operative treatment of risks (i.e. identifying, controlling, and monitoring risks) for an organisation.

Strategic risk management describes the essential framework conditions that shape an organisation's approach to handling risks, its culture regarding the handling of risks, and the methodology is follows in doing so. These principles for the treatment of risks within an ISMS must be consistent and aligned with the framework conditions of the organisation's overall risk management efforts.

The framework conditions of operative risk management include a control process consisting of the following steps:

- Risk identification
- Risk assessment and evaluation
- Risk treatment
- Risk monitoring
- Risk communication

Damage / consequence

A deviation from an expected result leads to a consequence (often referred to as “damage”). In principle, this can be a positive or a negative deviation.

A positive consequence within the meaning of risk analysis is also referred to as an opportunity. In most cases, however, only negative consequences (i.e. damage) are considered in risk analysis.

The scale of a damage is defined as extent of damage and can be referred to as directly quantifiable or not directly quantifiable. Quantifiable damage can usually be described in terms of direct efforts (e.g. of a financial nature). Damage that is not directly quantifiable includes, for example, damage to one's image or opportunity costs. In these cases, the actual extent of damage can often only be assumed or estimated. Any specifications in this regard are usually classified in categories based on empirical or industry values.

Protection needs

Protection needs describe the protection that is adequate and appropriate to protect specific business processes, the information processed in conducting them, and the information technology employed in doing so.

Determining protection needs

The process of determining protection needs identifies the safeguards required by specific business processes; the information processed in conducting them; and the IT systems, rooms, and communication connections involved. To this end, the damage to be expected should the core values of information security (confidentiality, integrity, and availability) be impaired is considered for each application and the information it processes. Here, it is also important to realistically estimate the possible consequential damages. Experience has shown that it is best to divide protection needs into three categories: "normal", "high", and "very high".

Vulnerability

A vulnerability is a security-relevant flaw in an organisation's IT system. It may be caused by an error in design, implementation, configuration, operation, the algorithms used, or the organisation itself. A vulnerability may cause a basic threat to become effective and damage an organisation or a system. As a result of a vulnerability, an object (an organisation or a system) is susceptible to basic threats.

Security requirement

The term "security requirement" refers to requirements for organisational, infrastructural, technical, or personnel-related areas that must be fulfilled in order to increase or otherwise support information security. A security requirement also describes what has to be done in order to achieve a specific level of information security. Ways to fulfil such requirements in specific cases are described in corresponding security safeguards (see below). The term “control” is also often used for security requirements.

IT-Grundschutz differentiates between Basic Requirements, Standard Requirements, and requirements in case of increased protection needs. Basic Requirements are fundamental and must always be implemented unless there are substantial reasons against it. Standard Requirements must generally be implemented for normal protection needs unless they are replaced by alternatives that are at least equally effective or the residual risk in question in consciously accepted. Requirements in case of increased protection needs are exemplary suggestions which should be implemented in an appropriate manner to meet corresponding protection requirements.

Security concept

A security concept aids in implementing an organisation's security strategy and describes its planned approach to achieving its security objectives. A security concept is the main document in an organisation's security process. It must be possible to trace every security safeguard back to the respective security concept.

Security design

Security design is one of the primary tasks of information security management. Based on the results of structure analysis and the determination of protection needs, the required security safeguards are identified and documented in a corresponding security concept.

Security safeguard

The term "security safeguard" (or simply "safeguard") refers to any action that serves to control and counteract security risks. This includes organisational, personnel, technical, and infrastructural security safeguards. Security safeguards help fulfil security requirements (see above). The terms “security measure” or simply “measure” are sometimes used as synonyms.

Security policy

A security policy formulates an organisation's official security objectives and general security requirements. Detailed security safeguards are contained in a more comprehensive security concept.

Standard Protection

Standard Protection essentially corresponds to the classic IT-Grundschutz methodology of BSI Standard 100-2. Standard Protection provides a CISO with a means of safeguarding their organisation's assets and processes in a comprehensive and in-depth manner.

Standard requirement

See “Security requirement”.

Strong authentication

Strong authentication refers to the combination of two or more authentication techniques—for example, a password plus a transaction number (a one-time password) or a chip card. For this reason, strong authentication is also often referred to as two-factor or multi-factor authentication.

Structure analysis

As part of a structure analysis, the necessary information on the information domain, business processes, applications, IT systems, networks, rooms, buildings, and connections under consideration is captured and prepared to support the next steps of IT-Grundschutz.

Binding character

Binding character refers to the combined security objectives of authenticity and non-repudiation. For the transmission of information, this means that a source of information has proven its identity and the receipt of the corresponding message cannot be denied.

Availability

Services, information, and the functions of IT systems, IT applications, and IT networks are considered available when users are able to access them as intended at all times.

Distribution effect

The distribution effect may have a relativising influence on protection needs if an individual application has high protection needs, but its protection needs are not applicable to a given IT system due to the fact that only insignificant parts of the application run on said system.

Confidentiality

Confidentiality means protection against the unauthorised disclosure of information. Confidential data and information should only be accessible to those authorised using the methods permitted.

Asset

Assets include anything that is important to an organisation (e.g. financial assets, knowledge, objects, health).

Certificate

The term certificate is used in information security contexts in different ways. The main definitions are as follows:

- ISO 27001 certificate: The standard ISO 27001, "Information Technology – Security Techniques – Information Security Management Systems Requirements Specification", makes it possible to obtain certification for an IT security management system.
- ISO 27001 certificates based on IT-Grundschutz: These certificates confirm that all relevant security requirements according to IT-Grundschutz have been implemented in a specific information domain. One prerequisite of receiving an ISO 27001 certificate based on IT-Grundschutz is an examination by an ISO 27001 IT-Grundschutz auditor licensed by the BSI. The tasks of an ISO 27001 IT-Grundschutz auditor include inspecting the reference documents created by the organisation in question, conducting an on-site examination, and creating an audit report. Based on the audit report, the BSI certificate authority determines whether the necessary security requirements have been implemented. If this is the case, it issues a certificate and publishes it if this is requested by the applicant.
- Key certificate: A key certificate is an electronic confirmation used to assign signature verification keys to a person. A certificate is required as confirmation from a trustworthy third party to prove that the cryptographic key used to generate a digital signature does belong to the signee.
- Certificate of IT product security: Certification is performed according to internationally recognised security criteria, such as the Common Criteria (ISO/IEC 15408). On this basis, a wide range of different products can be evaluated. It is essential, however, that the security properties confirmed in a given certificate at the end of the procedure support the preservation of confidentiality, availability, and integrity.

A digital certificate is a data record that confirms certain properties of persons or objects and can be verified in terms of its authenticity and integrity by cryptographic procedures. Among other things, a digital certificate enables the use of electronic signatures.

Target object

Target objects are the parts of a given information domain that can be assigned to one or more modules of the IT-Grundschutz Compendium within the framework of modelling. Target objects may include physical objects, such as IT systems. In many cases, however, target objects are logical objects such as organisational units, applications, or an entire information domain.

System access

This type of access refers to the use of IT systems, system components, and networks. System access authorisations therefore allow a user to use certain resources, for example IT systems, system components, or networks.

Data access

This type of access refers to the use of information or data. Data access authorisations thus determine who (within the framework of roles) or which IT applications are authorised to execute transactions and use information, data, or IT applications.

Site access

This type of access refers to the entry to restricted areas, for example certain rooms or protected sections of a property. Site access authorisations therefore allow people to enter certain environments, for example a property, a building, or specific rooms in a building.

Elementary Threats

G 0.1 Fire

Fire can cause serious damage to people, buildings and their equipment. In addition to the direct damage caused by fire, there may be consequential damage whose effects, especially to information technology, can reach catastrophic proportions. For example, damage from the water used to fight the fire can occur not only at the immediate site of the fire. It can also occur in lower parts of buildings. Burning PVC generates chlorine gases that form hydrochloric acid when they come into contact with moist air and extinguishing water. If the resulting hydrochloric acid vapours are spread via the air conditioning system, sensitive electronic devices located in a part of the building far from the site of the fire may become damaged. However, even "normal" smoke generated by a fire and spread by the air conditioning system can cause damage to the IT equipment.

Fires can be started by careless handling of sources of fire (e.g. unattended open flames, welding and soldering work, etc.), but also through improper use of electrical equipment (e.g. unattended coffee machines, overloaded power strips). Technical defects in electrical devices can also start a fire.

The following factors can help spread a fire, among other factors:

- Wedging open doors separating fire zones
- Improper storage of flammable material (e.g. waste paper)
- Failure to observe relevant standards and regulations for preventing fires
- Absence of fire detection and alarm systems (e.g. smoke detectors)
- Missing or unusable hand-held fire extinguishers or automatic extinguishing equipment (e.g. gas extinguishing systems)
- Poor fire prevention measures (e.g. the absence of fire seals in cable trays or the use of unsuitable insulation materials in heat and noise insulation).

Examples:

- In the early 1990’s, a mainframe computer centre near Frankfurt suffered catastrophic fire damage that lead to its complete failure.
- Small electrical appliances such as coffee machines and table lamps are frequently installed improperly or in the wrong place, and can then cause fires.

G 0.2 Unfavourable Climatic Conditions

Unfavourable environmental conditions such as heat, frost or excessive humidity can lead to different kinds of damage, such as malfunctions in technical components or damage to storage media. These effects can be aggravated by frequent fluctuations in the climatic conditions. Unfavourable environmental conditions can also mean that people are no longer able work or are even injured or killed.

Each person and each technical device has a temperature range within which their normal way of working (people) or proper functioning (devices) is ensured. A rise or fall in the ambient temperature to a value outside that range could result in shut-downs, non-productive times, operational malfunctions or equipment failures.

The windows in server rooms are frequently opened for ventilation purposes in an unauthorised manner. During seasons in which the outside temperature varies greatly (in the spring or autumn), open windows can cause large temperature fluctuations, and humidity levels may exceed the permissible upper limit due to the sudden drop in temperature.

Examples:

- At midsummer temperatures and without adequate cooling, IT devices may fail because the temperature is too high.
- An IT system that is too dusty may overheat.
- If the temperature is too high, magnetic storage media may be demagnetised.

G 0.3 Water

Water may impair the integrity and availability of information that is stored on analogue and digital data media. Information stored in the memory of IT systems is also at risk. The uncontrolled flow of water into buildings or rooms can be caused by the following, for example:

- Disruptions to the water supply or sewer system
- defects in the heating system
- defects in air conditioning systems connected to a water supply
- defects in sprinkler systems
- water used to extinguish a fire
- sabotage using water, for example by turning on the water taps and blocking the drains.

Regardless of how the water enters a building or room, there is a danger that it will damage the supply systems or IT components or put them completely out of operation (short-circuits, mechanical damage, rust, etc.). Especially if central building supply system equipment (main distributors for the electrical, telephone, or data systems) is installed in rooms in the basement not equipped with automatic water drainage equipment, then water entering these rooms can cause large amounts of damage.

Problems may also be caused by frost. For example, conduits in areas subject to frost can start to leak if water stands still in the case of persistent frost. Existing thermal insulation can also succumb to frost over the course of time.

Example:

- In a server room, a water pipe was routed under the ceiling and then enclosed with plasterboard. When a leak arose in one of the water pipe connections, it was not detected promptly. The water that escaped formed a pool at the lowest point of the plasterboard enclosure first before it escaped from there, causing a short-circuit in a power distributor located beneath it. As a result, both the water and the power supply in the affected part of the building had to be switched off completely until the repair work was finished.

G 0.4 Pollution, Dust, Corrosion

In addition to electronics, many IT devices also contain mechanical operating components, as is the case for hard disks and removable disks, DVD drives, printers, scanners etc., and also for processor and power supply unit fans. The increasing demands on the quality and speed of these components means they must operate more and more precisely. Even minor contamination can cause a device to malfunction. For example, dust and pollution can occur to a larger extent when the following activities are carried out:

- work on walls, raised floors, or other parts of the building-
- hardware upgrades.
- unpacking of devices (e.g. Styrofoam packaging materials).

In most cases, the safety circuits built in to the devices switch them off in time. Although this may reduce the resulting amount of direct damage to the device, repair costs, and downtime, the corresponding device will still be unavailable during this time.

Moreover, devices and the infrastructure can be affected by corrosion. This may even negatively impact building safety, not just the IT.

Corrosion can also lead indirectly to other threats. For example, water can leak from corroded areas (see G 0.3 Water).

In general, pollution, dust or corrosion can cause failures of or damage to IT components and supply systems. As a result, proper information processing may be impaired.

Examples:

- A server was installed in a media room together with a copying machine and a fax machine, after which the processor fan and the power supply fan slowed down due to the large amount of dust in the room. The failure of the processor fan caused the server to crash sporadically. Eventually, the power supply unit fan failed too, causing the power supply unit to overheat and short-circuit, which in turn resulted in the total failure of the server.
- To hang a wall panel in an office, holes were drilled into the wall by the building services personnel. The employee left his office for a short time so the work could be done. When he returned to his workplace, he discovered that his PC no longer worked. The failure was caused by the dust generated by the drilling, which had penetrated into the PC power supply unit through the ventilation slots.

G 0.5 Natural Disasters

Natural disasters refer to natural changes which have devastating consequences for people and infrastructures. Causes for a natural catastrophe can be seismic, climatic or volcanic phenomena, such as earthquakes, flooding, landslides, tsunamis, avalanches and volcanic eruptions. Examples of extreme meteorological phenomena include thunderstorms, hurricanes, or cyclones. Depending on the site of the organisation, it is exposed to the risks from the various types of natural disasters to different degrees.

Examples:

- For computer centres in flood-prone regions, there is often the particular risk of water entering the building in an uncontrolled manner (flooding or rise in groundwater level).
- The frequency of earthquakes and thus also the associated risk depends to a large extent on the geographical location.

Regardless of the type of natural disaster, there is also a danger in regions which are not directly affected that supply systems, communication links or IT components are damaged or put completely out of operation. Especially if central building supply system equipment (main distributors for the electrical, telephone, or data systems) fails, this can cause major damage. Operating and service personnel may be denied access to the infrastructure due to extensive restricted areas.

Examples:

- Many businesses, even large companies, do not take the danger of flooding seriously enough. For example, one company was "surprised" several times by flood damage to their computer centre. The computer centre was literally washed away twice within 14 months. The resulting damage was estimated to be several hundred thousand euros and was not covered by insurance.
- An IT system is located at a site where the geographical location is known for its volcanic activity (intermittent phenomenon for which the emission phases alternate with sometimes long non-emission phases).

G 0.6 Catastrophes in the Vicinity

A public authority or a company may be damaged if there is a serious accident in the environment, for example a fire, an explosion, the release of toxic substances or the emission of dangerous radiation. Here, the risk is not only posed by the event itself, but also by activities which often result from these events, such as road closures or rescue measures.

The properties belonging to an organisation may be subject to a variety of threats from the environment, among other things due to traffic (roads, railways, air, and water), neighbouring businesses, or residential areas.

Prevention or rescue measures may also directly affect the organisation's properties. Such measures can also mean that employees cannot reach their workplaces or that personnel require evacuation. However, problems may also indirectly affect an organisation due to the complexity of the building services and IT equipment.

Example:

- A huge cloud of smoke developed due to a fire in a chemical plant located in the immediate vicinity of a computer centre (approximately 1000 metres away). The computer centre had an air conditioning and ventilation system that was not equipped with an outside air monitor. It was only the attentiveness of an employee (the accident occurred during working hours) who followed the development and spreading of the smoke cloud that allowed the outside air intake to be closed manually before it was too late.

G 0.7 Major Events in the Vicinity

Large events of all kinds can lead to disruptions of the normal operation of a public authority or company. Such events include street festivals, concerts, sporting events, labour disputes, and demonstrations. Rioting in connection with such events can have additional side-effects ranging from intimidation of the organisation's personnel to the use of violence against personnel or the building.

Examples:

- During the hot summer months, a demonstration was held in the vicinity of a computer centre. The situation escalated and led to violence. One window of the computer centre facing a side street was left open. A demonstrator entered through the window and took the opportunity to steal hardware which contained important information.
- An electrical power line was cut accidentally while setting up a large funfair. This lead to a power failure in the computer centre supplied with power by this line, although the centre's emergency power system was able to take over and provide power.

G 0.8 Failure or Disruption of the Power Supply

In spite of high levels of service security, power supply disruptions still occur regularly at power distribution system operators or power supply companies. Most of these malfunctions are so short (less than one second long) that consumers do not even notice them. However, interruptions lasting longer than 10 ms can cause disruptions to IT operations. In addition to malfunctions in the power supply system, however, switching off equipment when performing scheduled maintenance or cables damaged by excavation work can also cause the power supply to be disrupted.

Note that not only the obvious, direct consumers of electricity (PCs, lighting, etc.) depend on the power supply. Much infrastructural equipment used today depends directly or indirectly on electrical power, e.g. lifts, air conditioning technology, alarm systems, security gates, automatic door closing units and sprinkler systems. Even the water supply in high-rise buildings relies on electricity to generate water pressure on the upper floors using pumps. If the power supply disruptions occur over longer periods of time, disruption of infrastructural equipment can mean that no more activities can be carried out in the affected areas.

Apart from disruptions, other malfunctions of the power supply can also impair operations. Overvoltage, for example, can result in malfunctions or even damage to electrical devices.

It must also be noted that the organisation's own business processes may also be affected by disruptions or malfunctions of the power supply in the neighbourhood under certain circumstances, for example if access roads are blocked.

Examples:

- Due to an error in the UPS of a computer centre, the UPS did not switch back to normal operation after a brief power failure. After about 40 minutes, the batteries were empty and all the computers in the affected server room failed.
- At the beginning of 2001, there was a power emergency in California that lasted over 40 days. The power supply situation was so tight that the Californian Independent System Operator mandated rolling blackouts. These power outages, which lasted up to 90 minutes, not only affected households, but also companies in the high-tech sector. Since the power failure also caused alarm systems and surveillance cameras to be switched off, the power supply company kept their rolling blackout timetables secret.
- In November of 2005, many communities in Lower Saxony and North Rhine-Westphalia were without power for days after heavy snowfall because numerous power line towers had collapsed under the weight of the snow and ice. It took several days to restore power.

G 0.9 Failure or Disruption of Communication Networks

Today, many business processes require at least temporarily intact communication links, either by telephone, fax, e-mail or other services using local area networks (LAN) or wide area networks (WAN). If some or several of these communication links fail over a longer period of time, this may have the following consequences:

- business processes can no longer be carried out, since necessary information cannot be retrieved.
- customers can no longer contact the organisation for questions.
- orders cannot be placed or completed.

If time-critical IT applications are run on IT systems that are connected via wide area networks, then the initial damage and consequential damage possible are correspondingly high if no alternative methods are available (such as connecting to a second communication network).

Similar problems may occur if there are malfunctions in the required communication networks, but without a complete failure. For example, communication links may also a have a higher error rate or other quality defects. Incorrect operating parameters may also lead to impairments.

Examples:

- Today, the Internet has become an indispensable means of communication for many organisations, among other things, to retrieve important information, to present themselves and to communicate with customers and partners. Companies which specialise in Internet-based services particularly depend on a properly functioning Internet connection.
- As networks converge, voice and data services are often transported using the same technical components (e.g. VoIP). This, however, increases the risk that the voice services and data services fail at the same time if there is a malfunction in communications technology.

G 0.10 Failure or Disruption of Supply Networks

Buildings normally house a number of basic supply and disposal networks that therefore serve as a foundation for all business processes in an organisation, including its IT. Examples of such supply networks include the following:

- electrical power
- telephone
- cooling
- heating and ventilation
- water and waste water
- fire-fighting water supply
- gas
- alarm and control systems (e.g. for intrusion, fire, building management)
- intercom systems

Amongst other things, the failure or malfunction of a supply network can mean that people can no longer work in the building or that IT operations and thus information processing are impaired.

The networks are mutually dependent to varying degrees, which means that operational disruptions in any of the individual networks will also affect the other networks.

Examples:

- A failure of the heating or ventilation may mean that all employees have to leave the affected buildings. Under certain circumstances this can result in high damages.
- A power failure will not only have a direct impact on the IT, but also on all other networks and systems equipped with electrically operated monitoring and control technology. There may even be electric lifting pumps installed in the sewage pipes under certain circumstances.
- A failure of the water supply may eventually affect the operation of air conditioning systems.

G 0.11 Failure or Disruption of Service Providers

Today, hardly any organisation is able to function without service providers such as suppliers or outsourcing providers. When organisational units depend on service providers, failures of outsourced services may impair the ability of the organisation to perform its tasks. The partial or full failure of an outsourcing service provider or a supplier may have a major effect on business continuity, and especially on critical business processes. There are various different causes for these failures, such as bankruptcy, unilateral termination of the contract by the service provider or supplier, operational problems such as forces of nature or a shortage of personnel. Problems may also occur if the services rendered by the service provider do not meet the quality requirements of the customer.

It must also be noted that service providers also often use subcontractors in order to be able to provide the customer with their services. Malfunctions, defects in the quality and failures on the part of the subcontractors may therefore also indirectly result in impairments at the customer.

Failures of IT systems at the service provider or of the communication links to the service provider may also cause impairments of the customer's business processes.

Retrieval of outsourced processes, if necessary, may be very difficult, for example since the outsourced processes are not documented adequately or because the previous service provider does not support the return of the processes into organisation's own infrastructure.

Examples:

- One company installed its server in the computer centre of an external service provider. After a fire in this computer centre, the financial department of the company was unable to function. This resulted in significant financial losses to the company.
- The just-in-time production of a company was dependent on timely deliveries of supplies and materials by an external service provider. After one of the service provider's vans malfunctioned, the delivery of urgently needed parts was drastically delayed. Thus, it was not possible to supply a number of customers in a timely manner.
- A bank contracted a cash-in-transit company for all cash transports. The cash-in-transit company then unexpectedly declared bankruptcy. The contract negotiations and route planning with the new transportation company took several days. As a consequence, this led to serious problems and long delays in the transportation of cash to and from the branch offices of the bank.

G 0.12 Electromagnetic Interference

Today, information technology consists of electronic components to a large extent. Optical transmission technology is also increasingly used, but computers, network switching elements and storage systems, for instance, usually contain a very large number of electronic components. The function of electronic devices can be impaired or even damaged by electromagnetic interference radiation acting on such components. As a consequence, this may result in failures, malfunctions, incorrect processing results or communication errors amongst other things.

Wireless communication can also be impaired by electromagnetic interference. Under certain circumstances, a sufficiently strong interference of the frequency bands used is enough to cause electromagnetic interference.

In addition, information that is stored on certain types of storage media may be deleted or corrupted by electromagnetic interference. This applies particularly to magnetisable storage media (hard disks, magnetic tapes etc.) and semiconductors. These storage media may even be damaged by electromagnetic interference.

There are many different sources of electromagnetic fields or radiation, for example wireless networks such as WLAN, Bluetooth, GSM, UMTS etc., permanent magnets and cosmic radiation. Moreover, each electrical device emits more or less strong electromagnetic waves which can be spread through the air, amongst other things, and along metallic conductors (e.g. cables, air conditioning ducts, heating pipes etc.).

In Germany, the Electromagnetic Compatibility Act (EMVG) contains rules with respect to this topic.

G 0.13 Interception of Compromising Interference Signals

Electrical devices emit electromagnetic waves. With devices that process information (e.g. computers, monitors, network switching elements, printers), these emissions can also contain the information currently being processed. Emissions carrying such information are referred to as compromising interference signals. An attacker who is in a neighbouring building or even in a vehicle parked in the vicinity, for instance, may try to receive these signals and reconstruct the processed information based on them. The confidentiality of the information is therefore questionable. A possible objective of such an attack is industrial espionage.

The limit values of the Electromagnetic Compatibility Act (EMVG) are generally not low enough to prevent someone from intercepting the compromising interference signals. If this risk cannot be accepted, additional safeguards must therefore be taken as a general rule to prevent this.

Compromising emanations are not limited to electromagnetic waves. Sound waves, for example when using printers or keyboards, may also be used under certain circumstances to obtain useful information.

It must also be noted that compromising interference signals are also caused or increased by external manipulation of devices in certain cases. If, for example, a device is irradiated with electromagnetic waves, it may happen that the reflected waves contain confidential information.

G 0.14 Interception of Information / Espionage

Espionage refers to attacks with the aim of collecting, evaluating and processing information about companies, people, products or other target objects. The processed information can then be used, for example, in order to obtain a specific competitive edge for another company, extort people or be able to copy a product.

In addition to the large number of technically complex attacks, there are often much simpler methods for obtaining valuable information, for example, by combining information from several publicly accessible sources, which seem to be harmless separately, but can be compromising in other contexts. Since confidential data is not adequately protected in many cases, it is possible to obtain this data using visual, acoustic, or electronic methods.

Examples:

- Many IT systems are protected against unauthorised use by identification and authentication mechanisms, for example in the form of user ID and password verification. However, if the passwords are transmitted in unencrypted form over lines, it may be possible for an attacker to read the passwords under certain circumstances.
- In order to be able to withdraw money from an automatic cash dispenser, the correct PIN must be entered for the debit or credit card. Unfortunately, the privacy protection offered by these machines is often inadequate, and an attacker can watch customers entering their PINs simply by looking over their shoulder. If the attacker is then able to steal the card later, they can use it to raid the account.
- To obtain access rights to a PC or to otherwise manipulate the PC, an attacker could send the user an e-mail containing a Trojan horse disguised as a supposedly useful program. In addition to the direct damage caused by Trojan horses, they may also be used to collect a wide range of information on the individual computer, and possibly even on the local network. In fact, the goal of many Trojan horses is to obtain passwords or other access data.
- In many offices, the workplaces are not properly protected to prevent people nearby from listening in on conversations. This way, colleagues, but also visitors may listen in on conversations and may obtain information that was not intended for their ears or is even confidential.

G 0.15 Eavesdropping

Eavesdropping refers to targeted attacks to communication links, conversations, sound sources of any kind or IT systems in order to collect information. This starts with undetected, secret eavesdropping on a conversation and extends up to highly technical, complex attacks in order to intercept signals that are sent via radio or lines, e.g. by means of antenna or sensors.

Due to the low risk of detection, line or radio communications tapping is a potential threat to information security that should not be overlooked. In principle, there is no such thing as a cable impervious to eavesdropping. Due to the low risk of detection, line tapping is a potential threat to IT security that should not be overlooked. Whether a line is actually being tapped can only be determined using sophisticated instruments.

The insecure transmission of authentication data using plain text protocols like HTTP, FTP or Telnet is especially critical, since they can easily be analysed automatically due to the clear structure of the data.

The decision to eavesdrop on information somewhere basically depends on whether the information that could be obtained is worth the technical and financial expenditure and the risk of detection. This question can only be answered by knowing what capabilities the attacker has and what their particular interests are.

Examples:

- In the case of telephone calls, an attacker may be interested in more than just listening in on conversations. The information which is transmitted during signalling can also be misused by an attacker, e.g. if the password is transmitted as plain text when a user logs in due to an incorrect setting on the end device.
- If wireless transmission is unprotected or inadequately protected (e.g. if a WLAN is only secured using WEP), an attacker can easily tap the entire communication.
- E-mails can be read anywhere along their journey through the Internet if they are not encrypted. Unencrypted emails should therefore not be compared to letters in the classical sense, but rather to postcards.

G 0.16 Theft of Devices, Storage Media and Documents

The theft of storage media, IT systems, accessories, software or data not only results in the expense of having to replace the equipment or restore it to working order, but also in losses resulting from a lack of availability. If confidential information is disclosed due to the theft, this can cause additional damage. Mobile IT systems, which are easy to transport inconspicuously, are often targeted for theft as well as servers and other expensive IT systems. However, there are also cases where storage media, such as documents or USB sticks, were stolen specifically in order to obtain access to the confidential information stored on them.

Examples:

- During the spring of 2000, a notebook disappeared from the US State Department. In an official statement, it was stated that the possibility that the notebook contained confidential information could not be ruled out. Nor was it known whether the device was protected against unauthorised access by encryption or any other means.
- In a German government office, several break-ins occurred through the same unprotected window. Some mobile IT systems disappeared in addition to other valuable items. It was impossible to completely rule out the possibility that documents had been copied or manipulated.
- In the United Kingdom, there was a series of data privacy violations in which confidential documents were disclosed because the corresponding storage media had been stolen. In one case, several computer hard disks containing highly personal information recorded during security checks of staff were stolen from the Royal Air Force.
- An employee of a call centre made copies of large amounts of confidential customer data shortly before he was forced to leave the company. After leaving the company, he sold the data to competitors. Since details of the incident eventually reached the press, the call centre lost many important customers.

G 0.17 Loss of Devices, Storage Media and Documents

There are a variety of causes that can lead to the loss off devices, storage media and documents. Availability is directly affected, but confidential information may also fall into the wrong hands if the storage media are not completely encrypted. There are costs associated with the replacement of devices or storage media; even if they reappear, information may have been disclosed or undesired programs may have been installed.

End devices and mobile storage media in particular can be lost easily. Today, huge amounts of data can be stored on small memory cards. However, there are still regular occurrences of documents in paper form accidentally left behind, for example in restaurants or on public transportation.

Examples:

- An employee uses her journey to work in the tram to look through some documents. In the rush to get off the tram at her stop, she accidentally leaves the papers on the seat next to her. The documents are not of a confidential nature, but several signatures of senior managers must be obtained again as a consequence.
- At a big public event, an employee accidentally drops a memory card with confidential calculations on the floor without noticing this when he is looking for something in his briefcase. The finder sifts through the content on their laptop and sells the information to competitors.
- A manufacturer sends CDs with software updates for troubleshooting purposes to customers by post. Some of these CDs are lost on the dispatch route without the sender or recipients being informed about this. As a result, the customers affected have to deal with malfunctions of the software.

G 0.18 Poor Planning or Lack of Adaptation

If organisational procedures that are used directly or indirectly for information processing are not designed properly, security problems may arise. Although each individual process step is carried out correctly, damage is often caused because processes are incorrectly defined in their entirety.

Another possible cause for security problems is dependencies with other processes which are not obviously related to information processing themselves. These dependencies may be easily overlooked during the planning phase and thus cause impairments during operations.

Moreover, there may be security problems when tasks, roles or responsibilities are not clearly assigned. Amongst other things, this may result in procedures being delayed, security safeguards neglected or rules disregarded.

There is also a risk if devices, products, procedures or other means are not used properly to realise information processing. The selection of an unsuitable product or vulnerabilities, for example in the application architecture or in the network design, may lead to security problems.

Examples:

- If maintenance or repair processes are not adjusted to the technical requirements, this may result in unacceptable downtimes.
- An increased risk may arise from attacks to the organisation's own IT systems if security-related requirements are not taken into account when purchasing information technology.
- If the consumables required are not provided in a timely manner, the IT procedures that depend on them may come to a standstill.
- Vulnerabilities may occur if unsuitable transmission protocols are selected when planning an IT procedure.

Information technology and the entire environment of a public authority or company are constantly changing. Such changes can include the addition or relocation of an employee, the purchasing of new hardware or software, or a company supplying operating resources declaring bankruptcy. Threats can result from not taking necessary organisational and technical adjustments into consideration, or only doing so to an insufficient extent.

Examples:

- Due to changes made to the construction of a building, the existing escape routes were changed. Since the employees were not adequately informed of the altered escape routes, the building could be evacuated in the required time.
- When transmitting an electronic document, no one checked if the document was sent in a data format that could be read by the recipient.

G 0.19 Disclosure of Sensitive Information

Confidential data and information must only be accessible by those persons who are authorised to access it. In addition to integrity and availability, confidentiality is one of the key security objectives. For confidential information (such as passwords, personal data, confidential company or governmental information, or development data), there is an inherent danger that it will be disclosed through technical failures, carelessness, or even deliberate action.

Access to confidential information can be gained from a variety of sources, for example:

- storage media in computers (hard disks)
- removable storage media (USB sticks, CDs, or DVDs)
- in printed form on paper (printouts, files)
- transmission routes used during data transmission

There are various ways of actually obtaining information, for example:

- reading files without authorisation
- thoughtlessly passing on information, e.g. in the course of repair orders
- deleting or destroying storage media inadequately
- stealing the storage medium for later evaluation
- tapping transmission lines
- infecting IT systems with malware
- viewing information on the screen or eavesdropping on conversations

Serious consequences can result for an organisation when sensitive information is disclosed. A loss of confidentiality can have the following adverse effects, among others, on an organisation:

- violations of laws, for example laws relating to data protection or banking secrecy
- negative internal effects, for example a loss of employee morale
- negative external effects, for example poorer relationships with business partners or the loss of customer trust
- financial effects, e.g. damage claims, fines, and court costs
- impairment of the right to informational self-determination.

A loss of confidentiality is not always detected immediately. In many cases, it only becomes apparent later, e.g. by means of press enquiries, that unauthorised persons have gained access to confidential information.

Example:

- Buyers of used computers, hard disks, mobile phones or similar devices often find strictly confidential information such as patient data or account numbers on them.

G 0.20 Information or Products from an Unreliable Source

If information, software or devices are used that come from unreliable sources or whose origin and correctness have not been sufficiently verified, their use can involve high risks. This can lead, among other things, to business-relevant information being based on an incorrect database, to calculations producing incorrect results or to incorrect decisions being made. At the same time, the integrity and availability of IT systems may also be impaired.

Examples:

- Recipients may be misled by e-mails, whose origin they have not verified, to carry out certain actions which have adverse effects on themselves or others. For example, the e-mail may contain interesting attachments or links which cause malware to be installed on the recipient's system after they have been clicked. In these cases, the sender of the e-mail may be faked or imitate that of a known communication partner.
- The assumption that a statement is true because you "read it in the newspaper" or "saw it on TV", is not always justified. Thus, incorrect statements may be incorporated into business-critical reports.
- The reliability of information distributed via the Internet varies greatly. Using statements from the Internet without verifying their sources may result in poor decisions.
- When updates or patches from untrusted sources are installed, this may have undesired side effects. When the origin of software is not verified, there is an increased risk that IT systems are infected with malicious code.

G 0.21 Manipulation with Hardware or Software

Manipulation is a term used to refer to each form of targeted, but secret intervention in order to change all kinds of target objects without being noticed. Hardware or software can be manipulated out of revenge to intentionally cause damage or for personal or financial reasons, among others. For these types of attacks, all kinds of devices, accessories, storage media (e.g. DVDs, USB sticks), applications, databases etc. may be the target.

Manipulations of hardware and software do not always result in immediate damage. If, however, the information processed by using hardware and software is impaired, this may cause all types of security impacts (loss of confidentiality, integrity or availability). The impact of such manipulations becomes even greater the later they are detected, the greater the skills and knowledge of the perpetrators, and the deeper the impact on a given workflow. The effects range from unauthorised reading of sensitive data to the destruction of data media or IT systems. Manipulations may thus also lead to significant downtimes.

Examples:

- In a Swiss financial company, an employee had manipulated the application software for certain financial services. It was thus possible for him to obtain sizeable amounts of money illegally.
- By manipulating automatic cash dispensers, attackers have repeatedly succeeded in illegally reading the data stored on payment cards. In connection with the PINs spied out, this data was misused at a later point in time to withdraw money at the expense of the cardholder.

G 0.22 Manipulation of Information

There are a number of ways in which information can be manipulated, e.g. by collecting data incorrectly or in an intentionally false manner, modifying the contents of database fields or business correspondence. In principle, it is not only possible to manipulate digital information, but also documents in paper form, for example. However, perpetrators can only manipulate the information to which they have access. The more access rights a person has to the files and directories of the IT systems and the more ways this person has to access information, the more serious the manipulations they will be able to make. If such manipulations are not detected in time, then the smooth operation of business processes and specialised tasks may be seriously disrupted.

The sensitive information in archived documents usually requires protection. Manipulation of such documents is especially serious because the manipulation can go unnoticed for years, and even when discovered, it may no longer be possible to properly investigate the incident.

Example:

- An employee in accounting became so angry over the promotion of the co-worker with whom she shared an office that she gained access to her co-worker's computer while she stepped out of the office for a short time. She seriously affected the company's published annual operating results just by changing some numbers in the monthly balance sheet.

G 0.23 Unauthorised Access to IT Systems

In general, each interface on an IT system not only provides the opportunity to use certain services of the IT system in an authorised manner, but also carries the risk of the IT system being accessed via these interfaces without authorisation.

Examples:

- If a user ID and the corresponding password are spied out, it is possible that the applications or IT systems protected with these security mechanisms are used in an unauthorised manner.
- Using inadequately secured remote maintenance accesses, hackers could access IT systems without authorisation.
- In the event of inadequately secured interfaces of active network components, it is conceivable that attackers would gain unauthorised access to the network component. If they also succeed in overcoming local security mechanisms, for example if they gained access to administrative authorisations, they could carry out all administration activities.
- Many IT systems provide interfaces for the use of exchangeable data storage devices, for example extended memory cards or USB storage media. When an IT system with the corresponding hardware and software is not supervised, there is a risk that large amounts of data could be read without authorisation or malware could be injected.

G 0.24 Destruction of Devices or Storage Media

Negligence, improper use, but also untrained handling, can lead to the destruction of equipment or data media that can seriously disrupt the operation of the IT system.

Furthermore, there is the risk that important information is lost due to the destruction, which may not be recovered at all or may only be recovered with great effort.

Examples:

- An employee in one company used his knowledge of the fact that an important server was sensitive to excessive operating temperatures and blocked the ventilation slots of the power supply fan by hiding an object behind the server. Two days later, the hard disk in the server malfunctioned due to overheating, and the server was down for several days.
- An employee became so angry after his system crashed repeatedly that he let his anger out on his workstation computer. He kicked the computer so hard that the hard disk was damaged to the point of uselessness. The data stored on this hard disk could only be partially reconstructed by restoring a backup from the day before.
- A spilled cup of coffee or a puddle of water after watering plants can penetrate into an IT system and cause short circuits.

G 0.25 Failure of Devices or Systems

When time-critical applications are run on an IT system, the secondary damage resulting from a system failure will be correspondingly high if there are no alternative systems available.

Examples:

- Firmware is loaded onto an IT system, but the firmware is not intended for use with this type of system. The IT system will no longer start without errors and has to be returned to an operable state by the manufacturer.
- A power failure in the storage system of an Internet Service Provider (ISP) resulted in the shutdown of the storage system. Although it was possible to fix the actual error quickly, the IT systems affected would not boot up correctly as there were inconsistencies in the file system. As a consequence, several web servers operated by the ISP remained unreachable for days.

G 0.26 Malfunction of Devices or Systems

Today, devices and systems used for information processing often have many functions and therefore have a correspondingly complex structure. In general, this applies both to hardware and software components. Due to this complexity, there are many different sources of error in these components. As a result, devices and systems often do not function as intended, resulting in security problems.

There are many causes of malfunctions, for example material fatigue, manufacturing tolerances, conceptual deficiencies, exceeded limit values, application conditions that were not defined or lack of maintenance. Since there are no perfect devices and systems, a certain residual probability for malfunctions must always be accepted anyway.

Malfunctions of devices or systems may impair all fundamental information security values (confidentiality, integrity, availability). In addition, malfunctions may also remain undetected over a longer period of time. It is therefore possible that calculation results are corrupted and cannot be corrected in a timely manner.

Examples:

- A clogged ventilation grille leads to the overheating of a storage system which, as a result, does not fail completely, but malfunctions only sporadically. It is only discovered a few weeks later that the information stored is incomplete.
- A scientific standard application is used to carry out a statistical analysis of a previously collected set of data that is stored in a database. According to the documentation, however, the application has not been approved for the database product used. The analysis seems to work, but random checks showed that the calculated results are incorrect. Compatibility problems between the application and the database were identified as the cause.

G 0.27 Lack of Resources

If the resources available in one area are inadequate, this may also result in supply bottlenecks with these resources, possibly leading to overload and failures. Depending on the type of resources affected, a number of business processes may be impaired in the end by a minor event whose occurrence was also predictable. The lack of resources may occur in IT operations and communication links, but also in other areas of an organisation. If only inadequate personnel, time and financial resources are provided for certain tasks, this may have manifold negative repercussions. For example, the necessary roles in projects may not be staffed with suitable persons. When operating resources such as hardware or software are no longer sufficient to meet the requirements, specialised tasks may not be performed successfully under certain circumstances.

In many cases, compensation can still be made for personnel, scheduling, financial, technical and other shortcomings during regular operations for a limited period of time. Under serious time pressure, however, they become all the more apparent, for example in emergency situations.

Resources can also be overloaded deliberately when somebody generates an intensive demand for an operating resource provoking an intensive and permanent disturbance of the operating resource, see also G 0.40 Denial of Service.

Examples:

- Overloaded electrical cables heat up, which may result in a smouldering fire if they are routed in an unfavourable manner.
- If new applications are operated on the network which have higher bandwidth requirements than those taken into consideration in the planning phase, this may result in a loss of availability of the entire network if it is no longer possible to sufficiently scale the network infrastructure.
- When the administrators check the log files of the IT supported by them only sporadically due to their high workload, it may be possible that attacks are only detected when it is too late.
- Web servers may be overloaded by a large number of simultaneously submitted queries to the point where normal access to the database becomes almost impossible.
- If a company is subject to insolvency proceedings, it may be that there is no money for urgently needed spare parts or that important service providers cannot be paid.

G 0.28 Software Vulnerabilities or Errors

The following applies to every software: the more complex it is, the more frequently errors will occur. Even in intensive tests, all errors are not detected prior to the delivery to the customers in most cases. If software errors are not detected in time, the crashes or errors resulting from the use of the software can have serious consequences. Examples of this are incorrect calculation results, poor decisions of the management and delays in the flow of business processes.

Software vulnerabilities or errors may result in serious security gaps in an application, an IT system or all connected IT systems. These security gaps may be exploited by attackers to inject malware, to read data without authorisation or to make manipulations.

Examples:

- Most of the warnings from Computer Emergency Response Teams (CERTs) in the last few years have been related to security-relevant programming errors. These are errors that arise during software development and that make it possible for the software to be misused by attackers. A large part of these errors was caused by buffer overflows.
- Today, Internet browsers are an important software component on clients. Browsers are often not only used to access the Internet, but also for internal web applications in companies and public authorities. Software vulnerabilities or errors in browsers can therefore cause particularly severe impairments of the information security of the entire organisation.

G 0.29 Violations of Laws or Regulations

If the information, business processes and IT systems of an institution are inadequately protected (for example, as a result of inadequate security management), this can result in violations of regulations relating to information processing or of existing contracts with business partners. The relevant laws to be followed depend on the type of organisation and/or its business processes and services. Depending on the locations of the organisation, various national regulations may need to be followed. This is illustrated by the following examples:

- In Germany, the handling of personal data is regulated by a large number of regulations. These include the Federal Data Protection Act and the State data protection laws, but also a large number of industry-specific regulations.
- The management of a company is obliged to exercise due care for all business processes. This includes the consideration of recognised security safeguards. In Germany, various legal regulations such as KonTraG (Control and Transparency in Business Act), GmbHG (Law on Private Limited (Liability) Companies) or AktG (Public Companies Act) are in force, from which corresponding obligations to act and liabilities of the management and/or the board of directors of a company regarding risk management and information security can be derived.
- The proper processing of accounting-relevant data is regulated by various laws and regulations. In Germany, these include, among others, the Commercial Code (e.g. Sections 238 ff. of the HGB) and the General Tax Code (AO). The proper processing of information naturally comprises its secure processing. In many countries, both must be proven on a regular basis, for example, through external auditors within the scope of the audit of the financial statements. If this reveals major security deficiencies, a positive audit report cannot be issued.
- In many industries (e.g. the automotive industry) it is common practice that manufacturers require their suppliers to comply with certain quality and safety standards. In this context, requirements regarding information security are also being specified to an increasing extent. If a contract partner fails to meet contractually regulated security requirements, this can result in contractual penalties, but also contract terminations or even the loss of business relationships.

Only a few security requirements arise directly from laws. However, as a rule, the law is based on the state of the art as a general basis for assessment of the degree of security that can be achieved. If, in an organisation, the existing security safeguards are not proportionate to the values to be protected and the state of the art, this may have serious consequences.

G 0.30 Unauthorised Use or Administration of Devices and Systems

Without suitable site, system and data control mechanisms, it is virtually impossible to prevent or detect the unauthorised use of devices and systems. For IT systems, the general mechanism is the identification and authentication of users. However, even in IT systems that use a strong identification and authentication function, unauthorised use is possible if the corresponding security features (passwords, chip cards, tokens etc.) fall into the wrong hands. Many errors can also be made when assigning, managing and updating authorisations, for example if authorisations are assigned too extensively or to unauthorised persons or are not updated in a timely manner.

Using devices and systems without authorisation, unauthorised persons may obtain confidential information, carry out manipulations or cause disruptions.

A particularly important special case of unauthorised use is unauthorised administration. When unauthorised persons change the configuration or the operating parameters of hardware or software components, this may result in serious damage.

Example:

- When checking the log data, a network administrator detected initially inexplicable events, which occurred on different days, but often in the early morning and in the afternoon. On closer examination, it transpired that a WLAN router was configured insecurely. People waiting at the bus stop in front of the company building had been using this access to surf the Internet using their portable terminal devices while waiting for the bus.

G 0.31 Incorrect Use or Administration of Devices and Systems

Incorrect use or administration of devices, systems and applications can jeopardise their security especially if existing IT security safeguards are ignored or bypassed through the misuse. In many cases, this results in malfunctions or failures. Depending on the types of systems that are used incorrectly, the confidentiality and integrity of information may also be impaired.

A particularly important special case of incorrect use is incorrect administration. Errors during the installation, configuration, maintenance and support of hardware or software components may lead to serious damage.

For example, security incidents can occur when access rights are granted too generously, the passwords are easy to guess, the data media containing backup copies are inadequately protected, or the terminals are not locked during temporary absences.

Similarly, data can also be accidentally deleted or changed through the incorrect operation of IT systems or applications. However, confidential information could also be disclosed unintentionally, for example when the data access rights are set incorrectly.

When power supply or network cables are routed in such a way that they are not protected, they may be damaged accidentally, causing connections to fail. When device connection cables are exposed, employees or visitors can trip over the cables and disconnect the devices.

G 0.32 Misuse of Authorisation

Depending on their roles and tasks, people are granted corresponding site, system and data access authorisations. In this way, access to information is controlled and monitored on the one hand, and people are enabled to carry out certain tasks on the other hand. For example, people or groups of people need certain authorisations to be able to execute applications or process information.

Authorisations are misused when a user deliberately uses privileges obtained with or without authorisation outside the planned scope. Here, the goal is to obtain personal advantage or to damage an organisation or certain people.

For historical, technical or other reasons, people will often have higher or more extensive site, system and data access rights than they actually need to do their jobs. These rights may be misused for attacks under certain circumstances.

Examples:

- Often, the more fine-grained the data access rights to information are designed, the larger the maintenance effort to keep these authorisations up to date. Therefore, there is a risk that there is too little differentiation between the different roles when assigning data access rights and it is thus made easier to misuse the authorisations.
- In different applications, data access authorisations or passwords are stored in system areas which can also be accessed by other users. Attackers could thus change the authorisations or read passwords.
- People with authorisations that are too extensive could be tempted to access files of other users, for example to read the e-mail of another user, because certain information is urgently needed.

G 0.33 Shortage of Personnel

A shortage of personnel can seriously affect an organisation and its business processes. Personnel may be absent unexpectedly due to illness, accidents, strikes, or death. Furthermore, expected absences of personnel due to holidays or training programs must be considered. In addition, normal terminations of employment must be taken into account, especially when the time the employee is still available for work is shortened due to accrued vacation time. Shortage of personnel may also be caused by an internal change in the workplace.

Examples:

- The network administrator of one company was off work as the result of a prolonged illness. The company network continued to operate without error at first. However, two weeks later the system crashed and no one was able to eliminate the error because this employee was the only one trained in the operation of the network. As a result, the network was unavailable for several days.
- While an administrator was on holiday, the backup media stored in a data safe were needed. The access code for the safe had been changed just prior to this, and the administrator was the only person who knew the new access code. It was only possible to restore the data after several days because it was impossible to reach the administrator any faster, as the administrator was on holiday.
- If there is a pandemic, increasing numbers of personnel will be absent for extended periods of time as the pandemic spreads, whether this is due to the illness itself or the need to take care of children and family members. Some employees will not go to work due to the fear of becoming infected in public transportation or in the organisation. As a consequence, it will only be possible to perform the most essential tasks. The maintenance required for systems, such as the central server or the air-conditioning system in the computer centre, cannot be performed any more. More and more systems will fail as time goes by due to the lack of maintenance.

G 0.34 Assault

An organisation, certain areas of the organisation or individual persons can be exposed to the threat of an assault. The technical possibilities for carrying out an assault are numerous: throwing bricks, creating an explosion using explosives, the use of firearms, or arson, for example. Whether or not an organisation is subject to the risk of an assault, and if so, to what extent, depends highly on the type of tasks performed and the political/social climate as well as on the location of the building and its surroundings. Company and public authorities operating in politically controversial areas are more exposed to this threat than other organisations. Organisations located near areas commonly used for demonstrations are at greater risk than more remote locations. In Germany, the Federal Office of Criminal Investigation or one of the state offices of criminal investigation can be contacted to obtain an assessment of the risk of a politically motivated assault or if you suspect you could be the target of such an assault.

Examples:

- A bomb attack on the computer centre of a large federal agency took place in the 1980s in Cologne. Due to the use of high-power explosives, the explosion not only destroyed windows and walls, but also numerous IT systems in the computer centre.
- The attack on the World Trade Center in New York on 11 September 2001 not only killed many people, but also destroyed a large amount of IT equipment. As a result, several companies had serious problems resuming business.

G 0.35 Coercion, Blackmail or Corruption

Coercion, blackmail or corruption may lead to the impairment of the security of information or business processes. Through the threat of violence or other disadvantages, an attacker may for example try to force the victim to ignore security policies or bypass security safeguards (coercion).

Instead of threatening, attackers may also specifically offer money or other advantages in order to make employees or other people their instruments for carrying out security violations (corruption). For example, there is the risk that a corruptible employee may forward confidential documents to unauthorised persons.

In principle, coercion or corruption can impair all fundamental information security values. Amongst other things, attacks may seek to forward confidential information to unauthorised persons, manipulate business-critical information or disrupt the smooth operation of business processes.

There is a particularly high risk if these attacks are directed against senior managers or people in positions of special trust.

G 0.36 Identity theft

In case of an identity theft, an attacker pretends to be someone else, which means that they use information about another person in order to act on their behalf. For this purpose, data such as the date of birth, address, credit card or account numbers is used, for example, to log in to an Internet service provider at the expense of others or to gain another type of advantage. In many cases, identity theft also results directly or indirectly in damage to the reputation of those concerned, but also leads to huge amounts of time required to clarify the causes and avert adverse consequence for the victims. Some forms of identity fraud are also referred to as masquerade.

Identity theft occurs particularly often in cases in which identity checks are carried out carelessly, especially if expensive services are based on it.

A person who has been deceived regarding the identity of their communication partner may easily be led to disclose information requiring protection.

Examples:

- For different e-mail providers and auction platforms in the Internet, it was initially sufficient to made up an invented name and combine it with a suitable address from the telephone book. At the start, attackers could also register using an obviously invented name, for example using the name of a cartoon character. Once stricter plausibility tests were introduced, names, addresses and account numbers of real persons were also used for this purpose. The victims only discovered this when they received the first payment requests.
- The sender addresses of e-mails can be easily corrupted. Users are commonly deceived into believing that an e-mail comes from a trusted communication partner. Similar attacks are possible by manipulating the calling line identity presentation (CLIP) for voice connections or by manipulating the sender ID for fax connections.
- Attackers may use a masquerade to attempt to intrude on an already established connection without having to authenticate themselves, since this step was already performed by the original communication partners.

G 0.37 Repudiation of Actions

For various reasons, people may deny having performed certain acts, for example because these acts violate instructions, security policies or even laws. However, they could also deny having received a notification, for example because they have forgotten an appointment or deadline. In the area of information security, the binding nature is therefore often pointed out, a characteristic which is used to ensure that acts that actions taken cannot be denied without justification. In this context, the term "non-repudiation" is used.

In communications, an additional distinction is made as to whether a communications subscriber denies the receipt of messages (repudiation of receipt) or the dispatch of messages (repudiation of origin). Denying the receipt of messages may be relevant, amongst other things, for financial transactions, e.g. if someone denies having received an invoice within the time stipulated. A communications subscriber can also repudiate transmission of a message, e.g. deny having sent an order. Having sent or received a message can be denied in the case of post just as with fax or e-mail.

Example:

- An electronic order is placed for an urgently needed spare part. After a week, a complaint about non-delivery of the part was lodged. In the meantime, high costs are incurred by the loss of production. The supplier denies ever having received such an order.

G 0.38 Misuse of Personal Information

In almost all cases, personal information is particularly sensitive information. Typical examples include information about personal or material circumstances of an identified or identifiable natural person. If the protection of personal data is not adequately ensured, there is the risk that the social or financial standing of those concerned will be impaired.

For example, personal data may be misused when an organisation collects too much personal data, has collected it without legal cause or the consent of the individual, uses it for a purpose other than the permitted one for which it was collected, deletes personal data too late or gives it to third parties without authorisation.

Examples:

- Personal data must only be processed for the purpose it was collected or stored for the first time. It is therefore not permissible to use log files, in which the login and logout of users on IT systems are only documented for access control, in order to check attendance and behaviour.
- People who have access to personal data could give it to third parties without authorisation. For example, an employee working at the reception of a hotel could sell the login data of guests to advertising firms.

G 0.39 Malware

Malware is software designed specifically with the goal of executing unwanted and usually damaging functions. Common types of malware include, among others, viruses, worms, and Trojan horses. Malware is usually activated in secret without the knowledge or permission of the user.

These days, malware provides an attacker with extensive communication and control capabilities, as well as a number of functions. Among other purposes, malware may be used to obtain specific passwords, control systems remotely, disable protective software and collect data without authorisation.

The most serious damage that can be caused by malware is the loss or corruption of information or applications. However, the image loss and financial damage that can result from malware can also be significant.

Examples:

- In the past the W32/Bugbear malware spread in two ways: it searched local networks for computers with shares with write access and copied itself to them. In addition, it sent itself in an e-mail in HTML format to the recipients in the e-mail address book of the computers it infected. Due to an error in the HTML routine of certain e-mail programs, the malware was executed when the message was opened without requiring any action by the recipient.
- The W32/Klez worm spread different versions of itself. Infected computers sent the virus to all recipients in the address book of these computers. Once this virus infected a computer, it prevented all further attempts to install commonly available anti-virus software by continuously manipulating the operating system. The continuous manipulation of the operating system made disinfecting the infected computer significantly more difficult.

G 0.40 Denial of Service

There are a large number of different forms of attacks which aim to prevent certain services, functions or devices from being used as intended. The generic term used for these attacks is "denial of service". In many cases, these attacks are often referred to as a "DoS attack".

Amongst others, these attacks can be initiated by disgruntled employees or customers, but also by competitors, blackmailers or politically motivated perpetrators. The target of the attacks may be all kinds of business-relevant values. Typical forms of DoS attacks include:

- disrupting business processes, e.g. by flooding the incoming order department with incorrect orders.
- impairing the infrastructure, e.g. by blocking the doors of the organisation.
- causing IT failures, e.g. by specifically overloading the services of a server in the network.

This type of attack is often connected to the use of distributed resources, with the attacker placing such high demands on these resources that they are no longer available to the actual users. When IT-based attacks are conducted, for example, a shortage of the following resources can be artificially induced: processes, CPU time, memory, disk space, transfer capacity.

Example:

- In spring 2007, strong DoS attacks to numerous Internet websites were carried out in Estonia over a longer period of time. This resulted in significant impairments when using information sites and services in the Internet in Estonia.

G 0.41 Sabotage

Sabotage refers to the intentional manipulation or damaging of objects or processes with the aim of inflicting damage on the victim. Computer centres or communications links owned by public authorities or companies make particularly attractive targets, since a dramatic effect can be achieved here with a relatively low effort.

The complex infrastructure of a computer centre can be selectively manipulated by external attackers, and particularly by insiders, by attacking specific, important components with the goal of disrupting operations. Here, inadequately protected building management systems and communication infrastructures, as well as central supply points are subject to a particular risk, which may not be monitored organisationally or technically and provide outsiders with easy and unobtrusive access.

Examples:

- In a large computer centre, manipulation of the UPS resulted in a temporary total power failure. The perpetrator had repeatedly switched the UPS to the bypass mode manually and then tampered with the main power supply to the building. There were are total of four blackouts over a period of three years. In some cases, this even resulted in damage to hardware. The service outages lasted between 40 and 130 minutes.
- Sanitary facilities were also available in a computer centre. By blocking the drains and turning on all taps at the same time, water penetrated into central technical components. The damage caused in this manner resulted in disruptions to the operation of the production system.
- Sabotage poses a special risk to electronic archives since a large number of documents requiring protection are stored in a small amount of space. In this way, it is possible to cause extensive damage with just minor, selective tampering under some circumstances.

G 0.42 Social Engineering

Social engineering is a method used to gain unauthorised access to information or IT systems by social action. Social engineering exploits human characteristics such as the willingness to help others, trust, fear, or respect for authority. It can be used to manipulate employees into performing unauthorised tasks. Typical examples of attacks carried out using social engineering include the manipulation of employees by calling them on the telephone and masquerading as one of the following persons:

- A receptionist whose supervisor wants to do something quickly but has forgotten their password and needs it urgently now.
- An administrator who calls because of a system error, since they need the user's password to eliminate the error.

If asked critical questions, the enquiring caller may say that they are is somebody "important" or "just a temp".

Another strategy used in systematic social engineering is to build a long-term relationship with the victim. By making numerous trivial telephone calls in advance, the attacker is able to collect information and build trust, which they can then exploit later.

Such attacks can also be conducted in several stages by using the knowledge and techniques gained in the previous stages.

Many users know that they are not allowed to give their passwords to anyone else. Social engineers are aware of this and therefore need to find other ways to reach their goals. Consider the following examples:

- An attacker may ask the victim to execute commands or run programs with which the victim is not familiar, for example to help solve an alleged problem with the IT. However, the request could contain disguised commands for changing the data access rights. The attacker may then be able to gain access to sensitive information.
- Many users use a strong password, but then use the same password for several different accounts. If an attacker is running a useful network service (such as an e-mail address system) that the users need to provide authentication for, then the attacker could obtain the desired passwords and login information. Many users will use the login data for this service for other services as well.

If attackers obtain passwords or other authentication features in an unauthorised manner, for example by means of social engineering, this attack is often also referred to as "phishing" (combination of the words "password" and "fishing").

When conducting a social engineering attack, the attacker will not always be visible. In many cases, the victims never even find out that they have been exploited. If this is the case, the attacker does not even have to worry about criminal prosecution and also has a source for obtaining additional information later.

G 0.43 Attack with Specially Crafted Messages

When conducting this type of attack, attackers send specially crafted messages to systems or people with the aim of obtaining an advantage for themselves or causing damage to the victim. To design the messages for this purpose, the attackers use, for example, interface descriptions, log specifications or records of past communication behaviour.

In practice, there are two important special cases of attack with specially crafted messages:

- When carrying out a "replay attack" (reimporting messages), attackers record valid messages and replay this information at a later point in time (almost) unchanged. It can also be sufficient to use only parts of a message, such as a password, in order to enter an IT system without authorisation.
- When conducting a "man-in-the-middle attack", the attacker takes an intermediary position in the communication between different participants without being noticed. Usually, the attacker deceives the sender of a message by pretending to be the actual recipient, and also deceives the recipient by pretending to be the actual sender. If attackers succeed in deceiving both, they can thus receive messages which are not meant for their eyes and evaluate and specifically manipulate the messages before passing them on to the actual recipient.

An encryption of the communication does not provide for protection against man-in-the-middle attacks when there is no secure authentication of the communication partners.

Examples:

- An attacker records the authentication data (e.g. user ID and password) during the login procedure of a user and uses this information in order to gain access to a system. In the case of authentication protocols that are purely static, a password transmitted in encrypted form can also be used in order to access a third-party system in an unauthorised manner.
- In order to cause financial damage to the employer (public authority or company), an employee places an approved order several times.

G 0.44 Unauthorised Entry to Premises

If unauthorised persons are able to break in to a building or individual rooms in a building, then the organisation may be subject to various other threats as a consequence. Such threats include the theft or manipulation of information or IT systems, for example. When well-planned attacks are conducted, the amount of time the perpetrator has to pursue their goal is decisive.

In many cases, the perpetrators want to steal valuable IT components or other goods which can be easily sold. However, the goal of a burglary may also be to access confidential information, carry out manipulation or disrupt business processes, for example.

Several different types of damage may thus occur if premises are entered without authorisation:

- Property damage can also result from the very act of unauthorised intrusion, Windows or doors are forced opened and damaged, which means they need to be repaired or replaced.
- Stolen, damaged or destroyed devices or components must be repaired or replaced.
- Damage may be caused if the confidentiality, integrity or availability of information or applications is violated.

Examples:

- Vandalism
- When breaking in to a company at a week end, minor damage was caused to a window as it was forced open. It initially appeared as though only a coffee cash box and some small items of furniture were stolen. It was later discovered during a routine check that a central server was cleverly manipulated exactly at the time of the break-in.

G 0.45 Data Loss

The loss of data is an event which means that a database can no longer be used as required (loss of availability). A frequent form of data loss is that data is deleted accidentally or without authorisation, for example due to improper use, malfunctions, power failures, soiling or malware.

However, data may also be lost when devices or storage media are damaged, lost or stolen. This risk is often particularly high for portable terminal devices and mobile storage media.

Furthermore, it must be noted that many mobile IT systems are not always online. Therefore, the data stored on these systems is not always up to date. When databases between mobile IT systems and stationary IT systems are synchronised, data may be lost due to carelessness or malfunction.

Examples:

- A PDA falls out of someone's shirt pocket and breaks into pieces on the floor tiles, or a dog retrieves a mobile phone instead of the newspaper, unfortunately with the corresponding consequences. These and similar events cause many total losses of data on portable terminal devices.
- There is malware which selectively deletes data on infected IT systems. For some malware, the delete function is not run immediately when the system is infected, but only when a defined event occurs, for example when the system clock has reached a specific date.
- Many Internet services can be used to store information online. If the user forgets the password or if the password is not stored, it may not be possible to access the information stored unless the service provider offers a suitable method to reset the password.
- Hard disks and other mass storage media only have a limited service life. If no suitable redundancy measures have been taken, data loss may be caused by technical defects.

G 0.46 Loss of Integrity of Sensitive Information

The integrity of information may be impaired for different reasons, e.g. manipulations, errors caused by people, incorrect use of applications, malfunctions of software or transmission errors.

- Information can be lost due to the ageing of the data media.
- Transmission errors: these can occur when transmitting data.
- Malware: this can be used to change or destroy entire databases.
- Entering the wrong data: this can trigger unwanted transactions, which often go unnoticed for a long time.
- Attackers can attempt to manipulate data for other purposes, e.g. to gain access to other IT systems or databases.
- Manipulation of the index database of an electronic archive can cause it to archive the wrong documents or to archive or retrieve falsified documents.

When the integrity of information is violated, a number of problems can arise:

- In the simplest case, it may just be impossible to read the information, which means it cannot be processed either.
- Data can be accidentally or deliberately falsified and lead to the disclosure of incorrect information. As a result of this, electronic bank transfers may contain the wrong amount, be sent to the wrong recipient, the sender address of emails could be manipulated, or many other kinds of problems could arise.
- If the integrity of encrypted or compressed records is lost (this only takes a change to a single bit), it may be impossible to decrypt or unpack the records under certain circumstances.
- The same also applies to cryptographic keys, i.e. changing just one bit in a key makes the key unusable. In turn, this could then make it impossible to decrypt the data or check its authenticity.
- Documents stored in electronic archives are not considered conclusive evidence when the integrity of the documents cannot be verified.

G 0.47 Harmful Side Effects of IT-Supported Attacks

IT-supported attacks may have effects that

- are not intended by the attackers.
- do not affect the directly attacked target objects.
- damage third parties not involved.

This due to the high complexity and networking of state-of-the-art information technology as well as the fact that the dependences of the attacked target objects and the related processes are usually not obvious.

Among other results, this may mean that the actual protection needs of target objects are miscalculated or that the persons in charge of target objects do not have a vested interest in removing the defects of such target objects.

Examples:

- Often, bots installed on IT systems that attackers may use to perform distributed Denial-of-Service attacks (DDoS attacks) do not represent a direct threat for the infected systems themselves. This is because the DDoS attacks usually are directed against IT systems of third parties.
- Attackers may use vulnerabilities of IoT devices in WLANs as an entry gate to attack other important devices in the same WLAN. That is why such IoT devices must be protected, even if they only have low protection needs themselves.
- In some circumstances, ransomware attacks on IT systems may trigger chain reactions and, correspondingly, also affect critical infrastructures. In turn, this could result in supply bottlenecks for the population, even if the attackers did not intend to achieve this.

ISMS.1 Security Management

1. Description

1.1. Introduction

The planning, management, and monitoring role that is essential to setting up and continuously implementing a well thought-out and effective process for maintaining information security is referred to as (information) security management. A properly functioning security management process must be embedded into the existing management structures of every organisation. For this reason, it is practically impossible to specify an organisational structure for security management that is directly applicable to every organisation. Instead, such structures often need to be adapted to the specific conditions of the organisation at hand.

1.2. Objective

The objective of this module is to illustrate how a functioning information security management system (ISMS) can be established and developed further during live operations. To accomplish this, the module describes a systematic security process and provides instructions for creating a security concept.

1.3. Scoping and Modelling

Module ISMS.1 *Security Management* must be applied once to the entire information domain under consideration.

The module is based on the BSI Standards 200-1, “Information Security Management Systems (ISMS)”, and 200-2, “IT-Grundschutz Methodology”. It summarises the most important aspects of security management.

Security audits should be carried out in organisations on a regular basis. Detailed requirements for this are not covered in this module; they can be found in module DER 3.1 *Audits and Revisions*. The security risk awareness of all an organisation's employees and other relevant persons (such as external employees or project members) should be raised in a suitable and systematic manner for each target group. These individuals should also be trained in aspects of

information security. Detailed requirements for this can be found in ORP.3 *Awareness and Training in Information Security*.

This module does not deal with specific aspects of human resources or organisation. These requirements are dealt with in the modules ORP.2 *Personnel* and ORP.1 *Organisation*.

2. Threat Landscape

For module ISMS.1 *Security Management*, the following specific threats and vulnerabilities are of particular importance.

2.1. Lack of Personal Responsibility in the Security Process

If the roles and responsibilities in an organisation's security process are not clearly defined, it is likely that many employees will reject or forget their responsibility for information security by pointing out that those above them in the organisational hierarchy are responsible. As a result, security safeguards will not be implemented because they almost always initially represent an additional effort on top of employees' usual work.

2.2. Lack of Support from Top Management

If those responsible for security are not fully supported by an organisation's top management, it can be difficult to enforce the necessary safeguards. This is especially true for persons who are above the person responsible for security in an organisation's hierarchy. In such cases, it is impossible to fully implement the security process.

2.3. Inadequate Strategic and Conceptual Specifications

Many organisations create a security concept, but fail to communicate its contents beyond a small circle of people. This leads to a conscious or unconscious failure to comply with requirements in situations where organisational time and effort would be required.

Even if a given security concept contains strategic objectives, these are often regarded by the organisation's top management as just a collection of declarations of intent. The resources then made available to achieve these objectives are often insufficient. It is also often wrongly assumed that security is automatically maintained in an automated environment.

Without strategic guidelines, there is often an unstructured response to instances of damage. This means only some aspects can be improved in the best case scenario.

2.4. Inadequate or Misdirected Investments

If an organisation's top management is not adequately informed of the security status of all business processes, IT systems, and applications (as well as existing shortcomings), insufficient resources will be provided for the security process, or these resources will not be used properly. In the latter case, this may result in one area having an excessive level of security, while other areas have serious security shortcomings.

It is not unusual to find expensive technical security solutions being used incorrectly to the point that they are ineffective or even pose a security risk themselves.

2.5. Inadequate Enforcement of Security Safeguards

In order to achieve a consistent and adequate level of security, different areas of responsibility within an organisation must cooperate with each other. However, a lack of strategic guidance and unclear objectives sometimes lead to different interpretations of the importance of information security. This can mean the required cooperation fails to take place because the job of “information security” is not prioritised or seen as a necessity. Security safeguards may not be implemented as a result.

2.6. Failure to Update the Security Process

New business processes, applications, and IT systems, as well as new basic threats, constantly affect the status of information security within an organisation. If there is no effective audit concept that also increases awareness of new threats, the organisation's level of security will decline. Its actual security will then gradually become a dangerous illusion of security.

2.7. Violation of Statutory Regulations and Contractual Agreements

If the information, business processes, and IT systems of an organisation are inadequately protected (for example, as a result of inadequate security management), this can result in violations of regulations relating to information processing or of existing contracts with business partners. The laws that apply depend on the type of organisation at hand and its business processes and services.

Depending on the locations of the organisation, various national and international regulations may also need to be followed. If an organisation has insufficient knowledge of international legal requirements (regarding data protection, the duty to supply information, insolvency law, liability, or access to information for third parties, for example), this increases the risk of corresponding violations and related legal consequences.

In many industries, it is common for users to require their suppliers and service providers to comply with certain quality and security standards. If a contractual partner violates contractually regulated security requirements, this can result in contractual penalties, contract termination, or even the loss of business relationships.

2.8. Business Process Disruptions due to Security Incidents

Security incidents can be triggered by a single event or a chain of unfortunate circumstances. They can result in the confidentiality, integrity, or availability of information and IT systems being compromised. This will then quickly have an adverse effect on essential specialised tasks and business processes in the organisation affected. Even if most security incidents do not become public, they may still have a negative impact on the organisation’s relationships with business partners and customers. Such incidents can also result in legal violations. The most serious and far-reaching security incidents are not triggered by the most serious security

vulnerabilities. In many cases, a chain reaction of minor factors leads to the most extensive damage.

2.9. Uneconomical Use of Resources due to Inadequate Security Management

Inadequate security management can result in the wrong priorities being set and investments not being made in areas that would bring the greatest benefits to a given organisation. This may lead to the following errors:

- an organisation may invest in expensive security solutions without providing for the basic organisational regulations required. when not clearly defined, competencies and responsibilities can still lead to serious security incidents in spite of a high investment.
- an organisation may invest in information security in areas which already have a keen awareness of information security Other areas that are important to carrying out business processes and reaching business objectives may be ignored due to a lack of resources or a lack of interest on the part of the persons in charge. Imbalanced investments may then be made in some areas while security risks that are particularly significant for the system as a whole are ignored.
- By unilaterally increasing the protection of individual key security objectives, the overall protection can even be reduced: The encryption of information
- The inconsistent and uncoordinated use of security products may result in the use of a great deal of financial and personnel resources.

3. Requirements

The specific requirements of module ISMS.1 *Security Management* are listed below. As a matter of principle, the Chief Information Security officer (CISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Supervisor, Top Management

3.1. Basic Requirements

For module ISMS.1 *Security Management*, the following requirements MUST be met as a matter of priority:

ISMS.1.A1 Acceptance of Overall Responsibility for Information Security by Top Management [Top Management] (B)

An organisation's Top Management MUST take overall responsibility for information security in the organisation. This MUST be clear to everyone involved. The Top Management MUST initiate, control, and monitor the security process. The Top Management MUST set a good example regarding information security.

The Top Management MUST define the responsibilities for information security. The responsible employees MUST be equipped with the necessary skills and resources.

The Top Management MUST be regularly informed about the organisation's information security status. In particular, the Top Management MUST be informed about possible risks and consequences due to a lack of security safeguards.

ISMS.1.A2 Defining Security Objectives and Strategy [Top Management] (B)

An organisation's Top Management MUST initiate and establish the security process. For this purpose, the Top Management MUST define and document appropriate security objectives and an information security strategy. Conceptual specifications MUST be developed and organisational framework conditions established to enable the proper and secure handling of information within all the organisation's business processes or specialised tasks.

The Top Management MUST support and take responsibility for its organisation's security strategy and security objectives. The Top Management MUST regularly review these security objectives and the security strategy to ensure that they are still relevant and appropriate and can be implemented effectively.

ISMS.1.A3 Drawing Up an Information Security Policy [Top Management] (B)

An organisation's Top Management MUST adopt an overarching information security policy. This MUST describe the value of information security, the organisation's security objectives, the most important elements of the security strategy, and the organisational structure for information security. The scope of the security policy MUST be clearly defined. The policy for information security MUST explain the security objectives and how they relate to the business objectives and tasks of the organisation.

The Top Management MUST communicate the information security policy to all staff and other members of the organisation. The information security policy SHOULD be updated regularly.

ISMS.1.A4 Appointment of a Chief Information Security Officer [Top Management] (B)

An organisation's Top Management MUST appoint a Chief Information Security Officer (CISO). The CISO MUST promote information security in the organisation and help steer and coordinate the security process.

The Top Management MUST provide the CISO with adequate resources. The Top Management MUST allow the CISO to report directly to it when required.

The CISO MUST be involved at an early stage in all larger projects and in the introduction of new applications and IT systems.

ISMS.1.A5 Contract Design When Appointing an External Chief Information Security Officer [Top Management] (B)

An organisation's Top Management MUST appoint an external Chief Information Security Officer (CISO) if the role of CISO cannot be filled by an internal employee. The contract with the external CISO MUST include all the tasks of the CISO and their related rights and obligations. The contract MUST include an appropriate confidentiality agreement. The contract MUST ensure that the corresponding relationship is terminated in an orderly fashion, including with regard to the handover of tasks back to the organisation in question.

ISMS.1.A6 Establishment of a Suitable Organisational Structure for Information Security [Top Management] (B)

An organisation MUST have a suitable higher-level organisational structure for information security. For this purpose, roles MUST be defined that will take on specific tasks to achieve the security objectives at hand. Qualified persons MUST also be appointed with sufficient resources to take on these roles. The tasks, roles, responsibilities, and competencies in security management MUST be defined and assigned in a transparent manner. Effective deputising rules MUST be in place for all the important functions within an information security organisation.

Communication channels MUST be planned, described, set up, and publicised. For all tasks and roles, it MUST be specified who will inform whom, who must be informed of which actions, and what information is to be provided.

It MUST be checked at regular intervals whether the organisational structure for information security is still adequate or needs to be adapted to new framework conditions.

ISMS.1.A7 Definition of Security Safeguards (B)

As part of the security process, detailed and adequate security safeguards MUST be defined for all aspects of information processing. All security safeguards SHOULD be documented systematically in security concepts. These security safeguards SHOULD be updated at regular intervals.

ISMS.1.A8 Integration of Employees into the Security Process [Supervisor] (B)

All of an organisation's employees MUST be integrated into its security process. For this purpose, they MUST be informed about the background and the hazards relevant to them. They MUST know and implement security safeguards that affect their workplace.

All employees MUST be enabled to make active contributions to security. Employees SHOULD therefore be involved at an early stage in planning security safeguards or devising organisational regulations.

When introducing security policies and security tools, employees MUST be adequately informed about how these should be used.

Employees MUST be made aware of the consequences of breaching security rules.

ISMS.1.A9 Integrating Information Security into Organisation-Wide Procedures and Processes [Top Management] (B)

Information security MUST be integrated into all business processes and specialised tasks. In so doing, it MUST be ensured that all necessary security aspects are not only taken into account in new processes and projects, but also in ongoing activities. The Chief Information Security Officer MUST be adequately involved in making security-relevant decisions.

Moreover, information security SHOULD be coordinated with other areas of an organisation that deal with security and risk management.

3.2. Standard Requirements

For module ISMS.1 *Security Management*, the following requirements correspond to the state-of-the-art together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

ISMS.1.A10 Drawing Up a Security Concept (S)

For the specified scope (the information domain), an adequate security concept SHOULD be drawn up as the central document in the security process. It SHOULD also be decided whether the security concept can also consist of several sub-concepts that are drawn up successively to establish the required level of security in selected areas first.

In the security concept, specific security safeguards appropriate for the information domain under consideration MUST be derived from the security objectives of the organisation in question, the protection needs identified, and the risk evaluation conducted. The security process and the security concept MUST take the individually applicable regulations and provisions into account.

The safeguards provided in the security concept MUST be implemented promptly in practice. Their implementation MUST be planned and monitored.

ISMS.1.A11 Continuity of Information Security (S)

An organisation SHOULD review its security process, security concepts, information security policy, and organisational structure for information security in terms of their appropriateness and effectiveness and update them at regular intervals. Completeness and update checks of the security concept SHOULD also be performed regularly in this regard.

Security audits SHOULD be performed regularly. In this regard, there SHOULD be rules that specify which areas and security safeguards need to be checked when and by whom. The level of security SHOULD be reviewed regularly (at least once a year) and whenever there is a reason to do so.

These reviews SHOULD be performed by qualified and independent persons. The results of the reviews SHOULD be documented in a transparent manner. Based on this, shortcomings SHOULD be eliminated and corrective measures taken.

ISMS.1.A12 Management Reports on Information Security [Top Management] (S)

An organisation's Top Management SHOULD be regularly informed about the status of information security—in particular, about the current threat landscape and the effectiveness and efficiency of its security process. In addition, management reports SHOULD be written that contain the most important information relevant to the security process, especially with regard to problems, successes, and potential improvements. The management reports SHOULD contain clearly prioritised proposals for action. The proposed actions SHOULD be accompanied by realistic estimates of the expected implementation effort. The management reports SHOULD be archived in an audit-compliant manner.

Management decisions relating to required actions, the handling of residual risks, and changes to security-relevant processes SHOULD be documented. These management decisions SHOULD be archived in an audit-compliant manner.

ISMS.1.A13 Documentation of the Security Process (S)

The security process SHOULD be documented. Important decisions and the work results of the individual phases, such as the security concept, policies, or findings resulting from examinations of security incidents, SHOULD be documented adequately.

A procedure SHOULD be defined for the creation and archiving of documentation within the framework of the security process. Rules SHOULD be in place to ensure that documentation is kept up to date and confidential. The respective current versions of existing documents SHOULD be available on short notice. Furthermore, all previous versions SHOULD be archived centrally.

ISMS.1.A14 ELIMINATED (S)

This requirement has been eliminated.

ISMS.1.A15 Cost-Effective Use of Resources for Information Security (S)

An organisation's security strategy SHOULD take economic aspects into account. If security safeguards are defined, the resources required for them SHOULD be quantified. The resources planned for information security SHOULD be provided on time. Additional internal employees or external experts SHOULD be called in for workload peaks or special tasks.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module ISMS.1 *Security Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

ISMS.1.A16 Creating Target-Group-Orientated Security Policies (H)

In addition to general security policies, there SHOULD be target-group-oriented security policies that cover the relevant security topics as needed.

ISMS.1.A17 Taking Out Insurance (H)

It SHOULD be examined whether insurance can be taken out against residual risks. An organisation's existing insurance policies SHOULD be checked regularly to ensure they are still appropriate for the current situation.

4. Additional Information

4.1. Useful Resources

The BSI Standard 200-1 defines general requirements of an information security management system (ISMS). It is also compatible with the ISO 27001 standard and includes the recommendations of many other ISO standards.

BSI Standard 200-2 forms the basis of the proven BSI methodology for the development of a sound information security management system (ISMS). It establishes three new approaches to the implementation of IT-Grundschutz. Since standards 200-1 and 200-2 have a similar structure, users can easily navigate within both documents.

ISO/IEC 27000 ("Information Security Management Systems — Overview and Vocabulary") provides an overview of information security management systems (ISMS) and the connections among the various standards of the ISO/IEC 2700x family. Furthermore, the standard includes the basic terms and definitions pertaining to an ISMS.

The ISO/IEC 27001 standard ("Information Security Management Systems – Requirements) is an international standard on information security management for which certification can also be obtained.

ISO/IEC 27002 ("Code of Practice for Information Security Controls") supports the selection and implementation of the safeguards described in ISO/IEC 27001 in order to establish a working security management system and embed it in an organisation.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module ISMS.1 *Security Management*.

G 0.18 Poor Planning or Lack of Adaptation

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

ORP.1 Organisation

1. Description

1.1. Introduction

Every organisation needs a service that is responsible for controlling and regulating general operations and planning, organising, and implementing administrative services. For these purposes, most organisations have an organisational unit which controls the interaction of various roles and units with the corresponding business processes and resources. At this overarching level, aspects of information security must be incorporated and defined in a binding manner.

1.2. Objective

This module lists general and overarching requirements in the area of organisation which help to increase and maintain information security. To achieve this, information flows, processes, the distribution of roles, and structural and procedural organisation must be regulated.

1.3. Scoping and Modelling

Module ORP.1 *Organisation* must be applied at least once to the entire information domain under consideration. If parts of the information domain are assigned to another organisational unit and are therefore subject to different general conditions, this module should be applied separately to each unit.

The module forms an overarching basis for implementing information security in an organisation. It does not deal with specific aspects of personnel, employee training, the administration of identities and authorisations, or compliance management. These aspects are covered in the modules ORP.2 *Personnel,* ORP.3 *Awareness and Training in Information Security,* ORP.4 *Identity and Access Management,* and ORP.5 *Compliance Management*.

2. Threat Landscape

For module ORP.1 *Organisation*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Rules

A lack of rules can result in severe vulnerabilities because employees do not know how they should react if there is an incident, for example. Problems can also result from rules that are outdated, impracticable, or not clearly formulated.

The importance of these overarching organisational regulations increases with the complexity of the business processes and the scope of information processing at hand, but also with the protection requirements of the information to be processed.

2.2. Non-Compliance with Regulations

The applicable regulations must be made known to all employees and be available for reference. Experience shows that it is not enough to merely lay down security rules. Communicating them to employees is fundamental to enabling all those affected to actively use these specifications in their everyday work.

If regulations are disregarded by employees, the following security gaps can arise, for example:

- Confidential information may be discussed within earshot of outsiders—for example, while talking during a break in a meeting or on a mobile telephone in a public environment.
- Documents may be published on a web server without checking whether or not they are actually intended and approved for publication.
- Due to the incorrect administration of access rights, an employee may be able to modify data without realising the critical impact this violation of integrity could have.

2.3. Inadequate or Incompatible Resources

If required resources are not available in sufficient quantities or not provided on time, it can lead to disruptions in an organisation. In some cases, unsuitable or even incompatible resources are also purchased that cannot be used.

Example: The storage space of hard disks in clients and servers, as well as that of mobile storage media, is constantly increasing. People often neglect to purchase IT components and storage media with enough capacity for regular backups.

The proper functioning of the resources used must also be ensured. Inadequate maintenance may lead to significant damage.

Examples:

- The capacity of the batteries of an uninterruptible power supply (UPS system) was not checked on time. If its capacity or acid content is too low, a UPS system will no longer be able to compensate for a power failure for a sufficient amount of time.

- Fire extinguishers were not serviced on time and therefore no longer have sufficient pressure. Their extinguishing capacity will thus no longer be guaranteed in case of a fire.

2.4. Threats from Outside the Organisation

In cases involving external individuals, it cannot be assumed that they will handle information and information technology according to the rules specified by the organisation they are visiting.

Visitors, cleaning staff, and third-party personnel can pose a threat to internal information, business processes, and IT systems in various ways, ranging from the improper handling of technical equipment and attempts to "play" with IT systems to the theft of documents or IT components.

Examples:

- Unaccompanied visitors can access documents, storage media, or equipment, damage these items, or extract sensitive information.
- Cleaners can accidentally loosen connectors, let water leak into equipment, misplace records, or dispose of them with the rubbish.

3. Requirements

The specific requirements of module ORP.1 *Organisation* are listed below. As a matter of principle, Central Administration is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Central Administration
Further responsibilities	Employee, User, IT Operation Department, Building Services, Top Management

3.1. Basic Requirements

For module ORP.1 *Organisation*, the following requirements MUST be met as a matter of priority:

ORP.1.A1 Specification of Responsibilities and Provisions [Top Management]

Within an organisation, all relevant tasks and roles MUST be clearly defined and separated from each other. Binding provisions for information security MUST be defined globally for the different operational aspects at hand. The organisational structures and binding regulations MUST be revised when required. All employees MUST be informed of such changes.

ORP.1.A2 Assigning Responsibilities [Top Management] (B)

For all business processes, applications, IT systems, rooms and buildings, and communication links, the persons responsible for them and their security MUST be defined. All employees MUST be informed accordingly, particularly with regard to what they are responsible for and the related tasks they are to perform.

ORP.1.A3 Supervising or Escorting External Individuals [Employee] (B)

Persons from outside an organisation MUST be escorted to rooms by employees. Employees within the organisation MUST also supervise external persons in sensitive areas. Employees SHOULD be encouraged not to leave external persons unattended within their organisation's premises.

ORP.1.A4 Separation of Roles Between Incompatible Tasks (B)

Tasks and the roles and functions they require MUST be structured in such a way that incompatible tasks (such as operative and controlling roles) are assigned to different persons. The separation of incompatible roles MUST be defined and documented. Representatives MUST also be subject to the separation of roles.

ORP.1.A5 ELIMINATED (B)

This requirement has been eliminated.

ORP.1.A15 Contact Persons for Information Security Issues (B)

In every organisation, there MUST be contact persons for security issues who can answer both seemingly simple and complex questions. These contact persons MUST be known to all the employees of their organisation. Corresponding information MUST be available and easily accessible to everyone in the organisation.

3.2. Standard Requirements

For module ORP.1 *Organisation*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

ORP.1.A6 ELIMINATED (S)

This requirement has been eliminated.

ORP.1.A7 ELIMINATED (S)

This requirement has been eliminated.

ORP.1.A8 Managing Resources and Devices [IT Operation Department] (S)

All devices and resources that influence information security and are required to perform tasks and comply with security requirements SHOULD be available in sufficient quantities. Suitable verification and approval processes SHOULD take place before these devices and resources are used. Devices and resources SHOULD be listed in appropriate inventories. To prevent the misuse of data, the reliable deletion or destruction of devices and resources SHOULD be regulated (see CON.6 *Deleting and Destroying Data and Devices*).

ORP.1.A9 ELIMINATED (S)

This requirement has been eliminated.

ORP.1.A10 ELIMINATED (S)

This requirement has been eliminated.

ORP.1.A11 ELIMINATED (S)

This requirement has been eliminated.

ORP.1.A12 ELIMINATED (S)

This requirement has been eliminated.

ORP.1.A13 Security During Relocation [IT Operation Department, Building Services] (S)

Prior to a relocation, security policies SHOULD be drawn up or updated in good time. All employees SHOULD be informed of the relevant security safeguards before, during, and after the relocation. The items transported SHOULD be checked after relocation to ensure they have all arrived undamaged and unmodified.

ORP.1.A16 Policy for Secure IT Use [User] (S)

A policy SHOULD be drawn up for all employees which transparently describes the framework conditions that must be observed during IT use and the security safeguards that must be implemented. The policy SHOULD cover the following aspects:

- the security objectives of the organisation in question
- important terms
- tasks and roles with respect to information security
- contact persons for questions regarding information security
- security safeguards to be implemented and observed by employees

The policy SHOULD be brought to the attention of all users. Every new user SHOULD confirm in writing that they have read and will comply with the policy before being allowed to use information technology. Users SHOULD reconfirm the policy regularly and after major changes. The policy should be made freely available for all staff to read (on the organisation's intranet, for example).

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module ORP.1 *Organisation* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

ORP.1.A14 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

No further information is available for module ORP.1 *Organisation*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module ORP.1 *Organisation*.

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.38 Misuse of Personal Information

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

ORP.2 Personnel

1. Description

1.1. Introduction

The staff of a company or public authority are crucial to its success or failure. In particular, employees have an important task in implementing information security. Even the most elaborate security precautions can come to nothing if they are not put into active use. The fundamental importance of information security to an organisation and its business processes must therefore be transparent and comprehensible to its staff.

1.2. Objective

The aim of this module is to highlight the security safeguards HR departments and supervisors must take to ensure that employees handle their organisation's information responsibly and behave in accordance with the relevant guidelines.

1.3. Scoping and Modelling

Module ORP.2 *Personnel* must be applied once to the entire information domain under consideration.

The module covers the requirements which must be observed and fulfilled by the human resources department and supervisors of an organisation. Personnel requirements linked to a specific role, such as the appointment of a system administrator for a LAN, are provided in the modules on the corresponding topics. Module ORP.2 *Personnel* does not deal with specific aspects of employee training or the management of identities and permissions. These aspects are covered in the modules ORP.3 *Awareness and Training in Information Security* and ORP.4 *Identity and Access Management*.

2. Threat Landscape

For module ORP.2 *Personnel*, the following specific threats and vulnerabilities are of particular importance:

2.1. Shortage of Personnel

The unavailability of personnel can mean that certain tasks will no longer be performed in a timely manner (or at all).

2.2. Insufficient Knowledge of Rules and Procedures

The mere specification of rules does not ensure they will be followed, nor does it ensure trouble-free operations. All employees, especially relevant roles, must be familiar with the rules that apply. Damage resulting from a lack of knowledge of the existing rules should not be excused simply by saying, “I didn’t know I was responsible for that,” or “I didn’t know what to do.”

2.3. Carelessness in Handling Information

Although there can be many organisational and technical security procedures in organisations, it is often the case that these are circumvented by careless handling on the part of employees. One typical case involves an employee who keeps a sticker on their monitor containing a list of all their passwords.

2.4. Insufficient Employee Qualifications

Many faults and errors can occur in the day-to-day IT operations of an organisation. If the responsible employees are not sufficiently qualified, aware, and trained—for example, if they have an outdated level of knowledge for the tasks they perform—they may not identify security-relevant events as such and allow attacks to go undetected. Even if the employees are adequately qualified, trained, and aware of issues relating to information security, it cannot be ruled out that they may fail to recognise security incidents. In some situations (e.g. those involving staff shortages or layoffs), employees may have to temporarily take on the tasks of other employees. Errors can occur if staff members do not have the necessary qualifications or are insufficiently trained for the tasks they take on.

3. Requirements

The specific requirements of module ORP.2 *Personnel* are listed below. As a matter of principle, the Human Resources Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Human Resources Department
Further responsibilities	IT Operation Department, Supervisor

3.1. Basic Requirements

For module ORP.2 *Personnel*, the following requirements MUST be met as a matter of priority:

ORP.2.A1 Well-Regulated Orientation of New Employees [Supervisor] (B)

An organisation's human resources department and supervisors MUST ensure that employees are provided with orientation regarding their new tasks at the start of their employment. Employees MUST be informed about existing regulations, instructions, and procedures. A corresponding checklist and a direct contact person (mentor) can be helpful and SHOULD be established.

ORP.2.A2 Regulated Procedure for Employees Leaving the Organisation [Supervisor, IT Operation Department] (B)

If an employee leaves an organisation, their successor MUST be briefed in good time, ideally by the departing staff member. If a direct handover is not possible, detailed documentation MUST be prepared by the employee leaving the organisation.

Moreover, all documents, keys, and devices, as well as ID cards, badges, and site-access authorisations received in connection with their tasks, MUST be returned by employees leaving an organisation.

Before an employee leaves an organisation, they MUST be reminded of their ongoing confidentiality obligations. In particular, it SHOULD be ensured that no conflicts of interest arise. In order to avoid conflicts of interest when someone takes a position at a different organisation, non-competition agreements and waiting periods SHOULD be agreed.

Moreover, business continuity plans and other schedules MUST be updated. All the parties affected within the organisation, such as the security personnel or the IT Operation Department, MUST also be informed about the employee leaving the organisation. A checklist SHOULD also be created here to ensure the completion of all the tasks that arise when an employee leaves. In addition, there SHOULD be a permanent contact person from the Human Resources Department who supports the departure procedure for employees.

ORP.2.A3 Defining Deputising Rules [Supervisor] (B)

Supervisors MUST ensure that deputising rules are implemented in day-to-day operations. This MUST be done by ensuring that workable deputising rules are in place for all key business processes and tasks. With respect to these arrangements, a deputy’s scope of tasks MUST be defined clearly in advance. It MUST be ensured that the deputy has the knowledge required for the position in question. If this is not the case, considerations MUST be made as to how the deputy is to be trained or whether it is sufficient to adequately document the current process or project status. Should it prove impossible to appoint or train a competent deputy for individual employees in exceptional cases, it MUST be determined in advance whether external personnel could be called in to act as deputies.

ORP.2.A4 Defining Procedures for Using Third-Party Personnel (B)

If third-party personnel are employed, they MUST be required to comply with applicable laws, regulations, and internal rules in the same way as the employees of the organisation in question. Third-party personnel employed on a short-term or one-off basis MUST be

supervised in security-relevant areas. If third-party personnel are engaged for longer periods, however, they MUST be instructed in their tasks in the same way as the organisation's own employees. Deputising rules MUST also be introduced for these employees. If third-party personnel leave the organisation, they MUST follow the same procedures as internal staff with regard to handing over the results of their work and returning any access authorisations they have been issued.

ORP.2.A5 Confidentiality Agreements for Third-Party Personnel (B)

Before external persons are granted data and site access to confidential information, confidentiality agreements MUST be concluded with them in writing. The confidentiality agreements MUST consider all the important aspects relating to the protection of the respective organisation's internal information.

ORP.2.A14 Tasks and Responsibilities of Employees [Supervisor] (B)

All employees MUST be obliged to comply with the relevant laws, regulations, and internal provisions. Employees MUST be aware of the legal framework that governs their work. Employees' tasks and responsibilities MUST be documented in a suitable manner. Furthermore, all employees MUST be informed that all the information they receive during their work is intended for internal use only. Employees MUST be made aware of their obligations to protect their organisation's information security outside of working hours and the organisation's premises.

ORP.2.A15 Qualifications of Personnel [Supervisor] (B)

Employees MUST receive regular training and other opportunities to further their development. In all areas, it MUST be ensured that no employee is working with outdated knowledge. Moreover, employees SHOULD be given the opportunity to acquire new skills within their field of work during their employment.

When filling positions, the required qualifications and skills MUST be clearly stated. It SHOULD then be checked whether the job applicants meet these criteria. It MUST be ensured that positions are only filled by qualified employees.

3.2. Standard Requirements

For module ORP.2 *Personnel*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

ORP.2.A6 ELIMINATED (S)

This requirement has been eliminated.

ORP.2.A7 Verifying the Trustworthiness of Employees (S)

New employees SHOULD be screened for trustworthiness before they are hired. Whenever possible, all those involved in the selection process SHOULD check that the information provided by applicants that is relevant to the assessment of their trustworthiness is credible. In particular, careful consideration SHOULD be given to whether submitted CVs are accurate, plausible, and complete. Any information that seems abnormal SHOULD be checked.

ORP.2.A8 ELIMINATED (S)

This requirement has been eliminated.

ORP.2.A9 ELIMINATED (S)

This requirement has been eliminated.

ORP.2.A10 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module ORP.2 *Personnel* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

ORP.2.A11 ELIMINATED (H)

This requirement has been eliminated.

ORP.2.A12 ELIMINATED (H)

This requirement has been eliminated.

ORP.2.A13 Security Vetting (H)

In high-security areas, additional security vetting beyond the basic verification of employees' trustworthiness SHOULD be carried out.

If employees deal with material that is classified as confidential, they SHOULD be subjected to security vetting in line with the German Security Clearance Check Act (SÜG). In this regard, the CISO SHOULD involve their organisation's Confidentiality Officer or Security Representative.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for handling security incidents in annex A.7 (“Human Resource Security”) of ISO/IEC 27001:2013, “Information Technology – Security Techniques – Information Security Management Systems – Requirements”.

“The Standard of Good Practice for Information Security” published by the Information Security Forum (ISF) provides guidelines for HR security under "PM: People Management".

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module ORP.2 *Personnel*.

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

ORP.3 Awareness and Training in Information Security

1. Description

1.1. Introduction

Employees are a crucial factor in ensuring a high level of information security in an organisation. It is therefore important that each and every one of them know their organisation's security objectives, understand the corresponding security safeguards, and be willing to implement them. This requires security awareness within the organisation in question. Furthermore, a culture of security should be established that forms an active part of employees' everyday work.

Employees should be made aware of relevant risks and know how they may affect their organisation. They must know what is expected of them in terms of information security and how they should respond in situations critical to security.

1.2. Objective

This module describes how to establish and maintain an effective program for raising awareness and conducting training on information security. The aim of the program is to raise employees' awareness of security risks and provide them with the knowledge and skills required to act in a security-conscious manner.

1.3. Scoping and Modelling

Module ORP.3 *Awareness and Training in Information Security* must be applied once to the entire information domain under consideration.

This module formulates requirements for information security awareness and training which relate to the working environment not only within an organisation, but in teleworking and mobile working settings, as well.

Module ORP.3 *Awareness and Training in Information Security* describes process-related, technical, methodological, and organisational requirements for information security awareness and training. An organisation's human resources department or training management department typically plans, manages, and implements other training topics, as well.

Specific training content for these topics is covered in many of the other IT-Grundschutz modules. This module deals with how a planned approach can be efficiently structured with regard to information security awareness and training.

2. Threat Landscape

For module ORP.3 *Awareness and Training in Information Security*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Knowledge of Rules and Procedures

Merely defining rules for information security does not guarantee that they will also be followed. All employees, and particularly relevant roles, must be familiar with the rules that apply. Although a failure to comply with rules is not the sole trigger of many security incidents, it is one of the reasons why they occur. Vulnerabilities stemming from insufficient knowledge of rules can pose a threat to the confidentiality, availability, and integrity of the information involved. This can hinder the fulfilment and execution of business processes and specialised tasks.

2.2. Insufficient Awareness of Information Security

Experience shows that it is not enough to merely impose security safeguards. Employees should know the importance and purpose of the measures; otherwise, they may be ignored in everyday work. If employees are not sufficiently aware of information security issues, their organisation's security culture, security goals, and security strategy may be at risk.

2.3. Ineffective Awareness and Training Activities

Activities implemented to raise awareness and provide training are not always as successful as hoped. This may be due to:

- lack of management support
- unclear objectives
- poor planning
- lack of performance monitoring
- lack of continuity
- insufficient financial or staffing resources

If no appropriate measures are taken to ensure the success of the training activities implemented, it is often not possible to achieve their objectives. If an organisation does not

implement sufficient activities to ensure employee awareness and training, aspects of information security can be put at risk, which directly hinders the fulfilment of tasks.

2.4. Insufficient Employee Training Regarding Security Functions

Employees often do not use newly introduced security programs and functions because they do not know how to operate them and learning how to use them independently in parallel to their daily work routine is considered too time-consuming. In addition, a lack of training after the introduction of new software can result in employees operating or configuring it incorrectly and cause unnecessary delays in work processes. For this reason, it is not enough just to purchase and install (security) software. In critical IT systems and applications in particular, an operating error can result in consequences that threaten the existence of the organisation in question.

2.5. Undetected Security Incidents

Many faults and errors can occur during the day-to-day operation of IT and ICS components. In such cases, security incidents may not be identified as such by personnel and cyber attacks (or related attempts) could go undetected. It is sometimes not easy to differentiate between security incidents and technical faults. If users and administrators are not specifically trained to recognise security incidents and react to them appropriately, vulnerabilities can remain undetected and be exploited. If security incidents are recognised too late or not at all, effective countermeasures cannot be taken in time. Small vulnerabilities in an organisation can grow into critical threats to integrity, confidentiality, and availability. This can hamper business processes, cause financial damage, or lead to regulatory and legal sanctions.

2.6. Non-Compliance with Security Safeguards

A wide variety of reasons, such as carelessness or hecticness, can lead to confidential documents lying around in the open at workplaces or e-mails not being encrypted. Even seemingly minor inattentiveness can result in damage that well-trained employees generally avoid causing.

2.7. Carelessness in Handling Information

Even when organisations establish a large number of organisational and technical security procedures, they are often circumvented by carelessness on the part of employees. A typical example of this is the proverbial sticker on an employee's monitor that contains a list of all their passwords. In the same way, hard disk encryption on a laptop does not stop a person sitting next to it on a train from reading confidential information off its screen. Even the best technological security solutions are no use if sheets of confidential information are left lying on a printer or end up in freely accessible waste paper bins.

If employees handle information carelessly, the defined information security processes become ineffective. Unauthorised persons can take advantage of negligence in handling information in order to carry out targeted industrial espionage (for example).

2.8. Lack of Acceptance of Information Security Policies

There can be various reasons why employees do not implement information security requirements. They include a lack of a security culture in the employees' organisation or a failure by its top management to set a good example. However, excessive security requirements can also result in employees dismissing security safeguards. Problems can also arise when certain user rights or certain hardware or software are viewed as status symbols. Restrictions in these areas may meet with significant resistance.

2.9. Social Engineering

Social engineering is a method used to gain unauthorised access to information or IT systems by eavesdropping on employees. In social engineering, an attacker generally makes direct contact with a victim (e.g. over the phone, by e-mail, or even on social networks). Attacks using social engineering often comprise several stages. By simulating insider knowledge and simultaneously appealing to an employee's willingness to help, an attacker can expand their knowledge step by step. If employees are not made sufficiently aware of this type of attack, they could be manipulated into performing unauthorised tasks through skilled persuasion. This may result in them passing on internal information, being infected by malware or even transferring money to purported business partners.

In the case of CEO fraud, for example, employees who are allowed to transfer money in the name of their organisation are made to believe that they have a fictitious order from their boss. They are told to execute transactions for a supposedly urgent and confidential deal which is vitally important to the continued existence of the organisation.

3. Requirements

The specific requirements of module ORP.3 *Awareness and Training in Information Security* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	IT Operation Department, Supervisor, Human Resources Department, Top Management

3.1. Basic Requirements

For module ORP.3 *Awareness and Training in Information Security*, the following requirements MUST be met as a matter of priority:

ORP.3.A1 Top Management Awareness of Information Security Issues [Supervisor, Top Management] (B)

An organisation's Top Management MUST be sufficiently aware of security issues. Security campaigns and training activities MUST be supported by the Top Management. The support of the Top Management MUST be obtained before the start of an information security awareness and training program.

All Supervisors MUST support information security by setting a good example. Managers MUST implement their organisation's security requirements. In addition, they MUST make their staff aware of their compliance obligations.

ORP.3.A2 ELIMINATED (B)

This requirement has been eliminated.

ORP.3.A3 Training Employees in the Secure Handling of IT [Supervisor, Human Resources Department, IT Operation Department] (B)

All employees and external users MUST be trained in and made aware of the secure handling of IT, ICS, and IoT components insofar as this is relevant to their work. To this end, binding, clear, and up-to-date policies for the use of the respective components MUST be available. If IT, ICS, or IoT systems or services are used in a manner that runs counter to the interests of the respective organisation, this MUST be communicated.

3.2. Standard Requirements

For module ORP.3 *Awareness and Training in Information Security*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

ORP.3.A4 Designing and Planning an Information Security Awareness and Training Program (S)

Awareness and training programs for information security SHOULD be designed for the appropriate target groups. A requirements analysis should be carried out for this purpose. Training measures SHOULD be able to focus on the specific requirements and different backgrounds.

A target-group-oriented awareness and training program SHOULD be created on the topic of information security. This training program SHOULD provide employees with all the information and skills necessary to implement the security rules and safeguards applicable within the organisation in question. It SHOULD be checked and updated regularly.

ORP.3.A5 ELIMINATED (S)

This requirement has been eliminated.

ORP.3.A6 Implementation of Information Security Awareness and Training Measures (S)

All employees SHOULD receive information security training in line with their tasks and responsibilities.

ORP.3.A7 Training in the IT-Grundschutz Methodology (S)

Chief Information Security Officers SHOULD be familiar with the IT-Grundschutz methodology. Once a need for training has been identified, a suitable IT-Grundschutz training course SHOULD be planned. The BSI's online course on IT-Grundschutz SHOULD be taken into account when planning a training course. Within the training, the approach SHOULD be drilled using practical examples. It SHOULD be examined whether Chief Information Security Officers should be qualified as BSI IT-Grundschutz practitioners.

ORP.3.A8 Measurement and Evaluation of Training Success [Human Resources Department] (S)

The success of information security training SHOULD be measured and evaluated according to the target groups at hand in order to determine the extent to which the objectives set out in awareness and training programs on information security are achieved. The measurements SHOULD consider both quantitative and qualitative aspects of awareness and training programs for information security. The results SHOULD be used appropriately to improve the respective awareness and training program.

The Chief Information Security Officer SHOULD exchange information regularly with the Human Resources Department and the other contacts relevant to security (data protection, health and safety, fire prevention, etc) on the effectiveness of training and further development activities.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module ORP.3 *Awareness and Training in Information Security* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

ORP.3.A9 Special Training for Exposed Persons and Organisations (H)

Particularly exposed persons SHOULD receive in-depth training with regard to possible hazards and appropriate behaviour and precautions.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides requirements for training employees and raising their awareness in the ISO/IEC 27001:2013 standard, section 7.2.

The Information Security Forum (ISF) defines various requirements for training employees and raising their awareness in "The Standard of Good Practice for Information Security", section PM2.

The BSI offers an online course on IT-Grundschutz at https://www.bsi.bund.de/grundschutzkurs, which introduces the methodology of IT-Grundschutz.

The BSI offers a two-stage training concept on the subject of IT-Grundschutz. In this training concept, participants can acquire an IT-Grundschutz practitioner certificate and be further certified as an IT-Grundschutz consultant by the BSI.

A list of training providers that offer BSI training to become an IT-Grundschutz practitioner and an IT-Grundschutz consultant can be found at https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/ITGrundschutzBerater/itgrundschutzberater_node.html.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module ORP.3 *Awareness and Training in Information Security*.

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.19 Disclosure of Sensitive Information

G 0.24 Destruction of Devices or Storage Media

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.42 Social Engineering

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

ORP.4 Identity and Access Management

1. Description

1.1. Introduction

Access to sensitive resources in an organisation must be restricted to authorised users and authorised IT components. Users and IT components must be identified and authenticated with certainty. The management of the information this requires is referred to as "identity management".

Access management, meanwhile, defines whether and how users or IT components may access and use information or services (i.e. whether they are granted or refused site, system, and data access based on their user profile). Access management includes the processes that are required to assign, withdraw, and control rights.

Since these two terms are closely connected, the term "identity and access management" (IAM) will be used from now on in this module. For better comprehensibility, the term "user ID" or "ID" is used synonymously with "user account", "login", and "account" in this module. The term "password" is used here as a general term for "passphrase", "PIN", or "passcode".

1.2. Objective

The objective of this module is to ensure that users and IT components can access only the IT resources and information that are required for their work and for which they are authorised, and that no access is granted to unauthorised users and IT components. To this end, it formulates requirements to be followed by organisations in establishing secure identity and access management.

1.3. Scoping and Modelling

Module ORP.4 *Identity and Access Management* must be applied once to the entire information domain under consideration.

This module describes fundamental requirements for implementing identity and access management.

Requirements that relate to components of identity and access management such as operating systems or directory services can be found in the corresponding modules (e.g. SYS.1.3 Unix Server, SYS.1.2.2 Windows Server 2012, APP.2.1 General Directory Service, APP.2.2 Active Directory).

2. Threat Landscape

For module ORP.4 *Identity and Access Management*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Processes in Identity and Access Management

If identity and access management processes are inadequately defined or implemented, there is no guarantee that access will be restricted to the extent necessary, which violates the need-to-know or least-privilege principles. Administrators may not receive information about personnel changes as a result, which means the user ID of an employee who has left may not be deleted, for example, allowing the employee to continue to access sensitive information.

It is also possible that employees who move to another department will keep their old authorisations and thereby collect extensive authorisations over time.

2.2. No Central Means of Disabling User Access Authorisations

Employees often have user access authorisations for various IT systems in their organisations, such as production, test, quality assurance, or project systems. In most cases, these systems are located in different areas of responsibility and often managed by different administrators. In some circumstances, this can mean that identical and unique user IDs are not used on all IT systems and there is no central overview of user access to the individual IT systems. In such scenarios, it is not possible to disable all of an employee's access in one step in the event of an attack or password theft. It is also not possible to block all of an employee's access in one step when they leave the organisation.

2.3. Incorrect Administration of Site, System, and Data Access Rights

If the assignment of site, system, and data access rights is controlled poorly, this may quickly result in serious vulnerabilities (e.g. due to unchecked growth in assigned rights). When introducing identity management systems or performing audits, it often becomes apparent that various persons in different organisational units are responsible for assigning rights. In some circumstances, this can result in users being granted authorisations upon request or only via unnecessarily complicated methods. The resulting lack of authorisations may impede daily work, but granting authorisations when there is no need also leads to security risks.

3. Requirements

The specific requirements of module ORP.4 *Identity and Access Management* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	User, IT Operation Department

3.1. Basic Requirements

For module ORP.4 *Identity and Access Management*, the following requirements MUST be met as a matter of priority:

ORP.4.A1 Regulation for Creating and Deleting Users and User Groups [IT Operation Department] (B)

Rules MUST be created to define how user IDs and user groups are to be established and deleted. It MUST be possible to associate every user ID with a unique user. User IDs that are inactive for longer periods SHOULD be disabled. All users and user groups MUST ONLY be created and deleted via separate administrative roles. User IDs that are not required, such as guest accounts set up by default or default administrator IDs, MUST be appropriately disabled or deleted.

ORP.4.A2 Creating, Changing, and Revoking Authorisations [IT Operation Department] (B)

User IDs and authorisations MUST ONLY be granted on the basis of actual need in connection with specific tasks (in line with the least-privilege and need-to-know principles). If there are personnel changes, the user IDs and authorisations that are no longer required MUST be removed. If employees apply for authorisations that are beyond the respective standard, they MUST ONLY be assigned after additional justification and verification are provided. Access permissions to system directories and files SHOULD be restricted. All authorisations MUST be established via separate administrative roles.

ORP.4.A3 Documentation of User IDs and Rights Profiles [IT Operation Department] (B)

The user IDs, user groups, and rights profiles that have been approved and created MUST be documented. The documentation of authorised users, user groups, and rights profiles MUST be examined regularly to see if it reflects the rights actually assigned to the users and profiles, and if the rights granted still meet the security requirements and are appropriate for the current tasks of the corresponding users. The documentation MUST be protected against

unauthorised access. If the documentation is made available in electronic form, it SHOULD be integrated into a backup procedure.

ORP.4.A4 Distribution of Tasks and Separation of Roles [IT Operation Department] (B)

The tasks and functions defined as incompatible by an organisation (see module ORP.1 *Organisation*) MUST be separated by its identity and access management system.

ORP.4.A5 Assignment of Site Access Rights [IT Operation Department] (B)

The site access rights that are to be granted to or withdrawn from certain people in certain roles MUST be defined. The issue and withdrawal of means of access such as chip cards MUST be documented. If site access resources have been compromised, they MUST be replaced. Persons with site access rights SHOULD be trained in the proper use of site access resources. Authorised persons SHOULD be blocked temporarily if they are to be absent for a longer period of time.

ORP.4.A6 Assignment of System Access Rights [IT Operation Department] (B)

The system access rights that are to be granted to and/or withdrawn from certain people in certain roles MUST be defined. If system access resources like chip cards are used, their issue and withdrawal MUST be documented. If system access resources have been compromised, they MUST be replaced. Persons with system access rights SHOULD be trained in the proper use of system access resources. Authorised persons SHOULD be blocked temporarily if they are to be absent for a longer period of time.

ORP.4.A7 Assignment of Data Access Rights [IT Operation Department] (B)

The data access rights that are to be granted to or withdrawn from certain people in certain roles MUST be defined. If data access resources like chip cards or tokens are used, their issue and withdrawal MUST be documented. Users SHOULD be trained in the proper use of chip cards or tokens. Authorised persons SHOULD be blocked temporarily if they are to be absent for a longer period of time.

ORP.4.A8 Provisions Governing the Use of Passwords [User, IT Operation Department] (B)

Organisations MUST regulate the use of passwords in a binding manner (see also ORP.4.A22 *Regulating Password Quality* and *ORP.4.A23 Regulating Password-Processing Applications and IT Systems*). In doing so, they MUST consider whether passwords are to be used as the sole authentication method, or whether other authentication features or methods may be used in addition to or instead of passwords.

Passwords MUST NOT be used for multiple purposes. A separate password MUST be used for each IT system or application. Passwords that are easy to guess or are kept in common password lists MUST NOT be used. Passwords MUST be kept secret. They MUST ONLY be known by the respective users. When entering their passwords, users MUST ensure that no one else is watching. Passwords MUST NOT be stored on programmable function keys on keyboards or mice. Passwords MUST ONLY be written down in case of an emergency. They MUST then be stored securely. The use of a password manager SHOULD be considered. If password managers have features or plug-ins that synchronise passwords via third-party

online services or otherwise transmit passwords to third parties, these features or plug-ins MUST be disabled. Passwords MUST be changed if it is suspected or discovered that they have become known to unauthorised persons.

ORP.4.A9 Identification and Authentication [IT Operation Department] (B)

Access to all IT systems and services MUST be protected by appropriate identification and authentication of users, services, and IT systems. Pre-configured authentication resources MUST be changed before being put into production use.

ORP.4.A22 Regulating Password Quality [IT Operation Department] (B)

Secure passwords of suitable quality MUST be chosen in line with their intended use and protection requirements. Passwords MUST be sufficiently complex so that they are difficult to guess. Passwords MUST NOT be so complex that users cannot utilise them regularly with a reasonable amount of effort.

ORP.4.A23 Regulating Password-Processing Applications and IT Systems [IT Operation Department] (B)

IT systems or applications SHOULD ONLY prompt users to change their password with a valid reason. Changes based on the passage of time alone SHOULD be avoided. Safeguards MUST be taken to detect compromised passwords. If this is not possible, consideration SHOULD be given to whether passwords can be changed at certain intervals in spite of the related disadvantages.

Default passwords MUST be replaced by sufficiently strong passwords, and pre-defined IDs MUST be changed. It SHOULD be ensured that IT systems fully check the possible password length. When a password is changed, the old password MUST NOT be used again. Passwords MUST be stored as securely as possible. In cases involving IDs for technical users, service accounts, interfaces, or similar elements, a password change SHOULD be carefully planned and, if necessary, coordinated with the persons in charge of the application in question.

When providing authentication in networked systems, passwords MUST NOT be transmitted unencrypted over insecure networks. When passwords are transmitted on an intranet, they SHOULD be encrypted. In case of unsuccessful login attempts, the system in question SHOULD not indicate that the password or user ID is wrong.

3.2. Standard Requirements

For module ORP.4 *Identity and Access Management*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

ORP.4.A10 Protection of User IDs with Wide-Ranging Authorisations [IT Operation Department] (S)

User IDs with broad privileges SHOULD be protected with multi-factor authentication (e.g. cryptographic certificates, chip cards or tokens).

ORP.4.A11 Resetting Passwords [IT Operation Department] (S)

An appropriate and secure procedure SHOULD be defined and implemented for resetting passwords. The support staff members that are able to reset passwords SHOULD be trained accordingly. In case of higher password protection needs, a strategy SHOULD be defined for cases in which a support staff member cannot accept responsibility for providing a password due to the lack of secure options available.

ORP.4.A12 Developing an Authentication Concept for IT Systems and Applications [IT Operation Department] (S)

An authentication concept SHOULD be drawn up that includes a definition of the functional and security requirements of authentication for each IT system and application at hand. Authentication information MUST be stored in a cryptographically secure manner. Authentication information MUST NOT be transmitted unencrypted over insecure networks.

ORP.4.A13 Selection of Suitable Authentication Mechanisms [IT Operation Department] (S)

Identification and authentication mechanisms that meet the protection needs at hand SHOULD be used. Authentication data SHOULD be protected by IT systems and/or applications against espionage, modification, and destruction during processing. IT systems and applications SHOULD increasingly delay further authentication attempts after each unsuccessful attempt. It should be possible to limit the total duration of a login attempt. After the specified number of unsuccessful authentication attempts is exceeded, IT systems and applications SHOULD block the user ID in question.

ORP.4.A14 Checking the Effectiveness of User Separation in IT Systems or Applications [IT Operation Department] (S)

Checks SHOULD be performed at appropriate intervals to ensure that users of IT systems or applications log off regularly after completing their tasks. It SHOULD also be checked that several users are not working under the same ID.

ORP.4.A15 Approach and Design of Identity and Access Management Processes [IT Operation Department] (S)

The following processes SHOULD be defined and implemented for identity and access management:

- policy management
- identity profile management
- user ID management
- authorisation profile management
- role management

ORP.4.A16 Policies for Data and System Access Control [IT Operation Department] (S)

A policy for data and system access control SHOULD be drawn up for IT systems, IT components, and data networks. Standard rights profiles that correspond to employees' roles

and tasks SHOULD be used. A data access rule SHOULD be established in writing for every IT system and IT application.

ORP.4.A17 Suitable Selection of Identity and Access Management Systems [IT Operation Department] (S)

An organisation's identity and access management system SHOULD be appropriate for its relevant business processes, organisational structures, and workflows, as well as for its protection needs. The identity and access management system SHOULD be able to map the specifications of the organisation for handling identities and authorisations. The identity and access management system chosen SHOULD support the principle of role separation. The identity and access management system SHOULD be adequately protected against attacks.

ORP.4.A18 Using a Central Authentication Service [IT Operation Department] (S)

A central authentication service SHOULD be used to establish central identity and access management. The use of a central network-based authentication service SHOULD be planned carefully. To this end, the security requirements relevant in selecting a service of this kind SHOULD be documented.

ORP.4.A19 Instruction of All Employees in the Handling of Authentication Methods and Mechanisms [User, Head of IT] (S)

All employees SHOULD be instructed in how to properly handle the authentication methods used. There SHOULD be comprehensible policies for handling authentication procedures. Employees SHOULD be informed of the relevant rules in this regard.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module ORP.4 *Identity and Access Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

ORP.4.A20 Contingency Planning for the Identity and Access Management System [IT Operation Department] (H)

The extent to which a failed identity and access management system is critical to the security of business processes SHOULD be determined. Provisions SHOULD be made to maintain operations in the event of a failed identity and access management system. In particular, the access control policy specified in the contingency concept at hand SHOULD still be applicable if the identity and access management system has failed.

ORP.4.A21 Multi-Factor Authentication [IT Operation Department] (H)

Secure multi-factor authentication (e.g. using cryptographic certificates, chip cards, or tokens) SHOULD be used for authentication.

ORP.4.A24 Dual Control for Administrative Activities [IT Operation Department] (H)

Administrative activities SHOULD require the involvement of two persons. If multi-factor authentication is required, the factors SHOULD be distributed between the two persons. Passwords SHOULD be split into two parts and issued to each of the two persons.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for identity and access management in annex A.9 ("Access Control") of ISO/IEC 27001:2013, “Information Technology – Security Techniques – Information Security Management Systems – Requirements”.

The International Organization for Standardization (ISO) provides specifications for identity and access management in the standard ISO/IEC 29146:2016, “Information Technology – Security Techniques – A Framework for Access Management”.

The Information Security Forum (ISF) provides specifications on identity and access management in chapter TS1.4 (“Identity and Access Management”) of “The Standard of Good Practice for Information Security”.

The National Institute of Standards and Technology (NIST) provides guidance on identity and access management in NIST Special Publication 800-53A, specifically in areas AC and IA.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module ORP.4 *Identity and Access Management*.

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.44 Unauthorised Entry to Premises

G 0.46 Loss of Integrity of Sensitive Information

ORP.5 Compliance Management

1. Description

1.1. Introduction

Every organisation has relevant statutory, contractual, and other requirements (such as internal guidelines) which must be observed. Many of these requirements have a direct or indirect impact on information security management.

The requirements differ by industry, country, and other framework conditions. In addition, a public authority (for example) is subject to different external rules and regulations than a public limited company. An organisation's top management must ensure compliance with such requirements by means of adequate monitoring safeguards.

Depending on the size of an organisation, this task may involve different management processes that deal with different aspects of risk management. These include security management, data protection management, compliance management, and controlling. The different units in question should collaborate in a spirit of trust to take advantage of synergies and eliminate conflicts before they arise.

1.2. Objective

The objective of this module is to illustrate how persons in charge can obtain an overview of the various requirements the individual areas within their organisation need to fulfil. For this purpose, suitable security requirements must be identified and implemented in order to avoid related violations.

1.3. Scoping and Modelling

Module ORP.5 *Compliance Management* must be applied once to the entire information domain under consideration.

The obligation of employees to comply with the statutory, contractual, and other requirements identified in this module is not part of this module; it is dealt with in module ORP.2 *Personnel*.

This module does not address specific laws, contractual regulations, or other guidelines.

2. Threat Landscape

For module ORP.5 *Compliance Management*, the following specific threats and vulnerabilities are of particular importance:

2.1. Violations of Legal Provisions

If information security is implemented incorrectly or inadequately, organisations may be in breach of statutory regulations or contractual agreements. Organisations must also comply with many different industry-specific, national, and international legal frameworks. As this can be very complex, users can unintentionally violate legal requirements or even knowingly accept this risk. For example, many cloud service providers offer their services in an international environment. These providers are thus often subject to the laws of different countries. Cloud users, however, often focus solely on low costs and make incorrect assumptions about legal framework conditions that should be taken into account with regard to data protection, information requirements, insolvency law, liability, or information access for third parties.

2.2. Improper Forwarding of Information

Misconduct on the part of individuals can result in sensitive information being passed on without permission. Confidential information could be discussed within earshot of outsiders—for example, while chatting during a break at a conference or talking on a mobile telephone in a public place. It is equally conceivable that the supervisor of a department might suspect an employee of collaborating with the competition. In order to prove it, the supervisor asks the head of the IT Operation Department to provide "unofficial" access to the employee's e-mails. The head of the IT Operation Department instructs the e-mail administrator to set up this access without obtaining the necessary approval.

2.3. Inadequate Checking of the Identity of Communication Partners

In personal conversations on the phone or by e-mail, many employees are willing to disclose far more information than they would in a letter or if more people were present. Furthermore, the identity of a communication partner is usually not questioned, as this is perceived as impolite. In the same way, permissions are often not sufficiently checked; they are implicitly deduced from a contact's (purported) role instead. An employee can receive an e-mail from someone claiming to know their supervisor, who has agreed to the urgent transfer of an outstanding sum of money. A stranger wearing work clothes and carrying a tool box may also be granted access to a data centre after mentioning something about "water pipes".

2.4. Accidental Sharing of Internal Information

Additional details are often inadvertently passed on with the information people intend to share with others. This can result in confidential information falling into the wrong hands.

This can occur if old files or residual information on storage media are passed on, for example. Users can also transmit incorrect data or send it to the wrong recipients.

3. Requirements

The specific requirements of module ORP.5 *Compliance Management* are listed below. As a matter of principle, the Compliance Manager is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	Compliance Manager
Further responsibilities	Chief Information Security Officer (CISO), Central Administration, Supervisor, Top Management

3.1. Basic Requirements

For module ORP.5 *Compliance Management*, the following requirements MUST be met as a matter of priority:

ORP.5.A1 Identification of Framework Conditions [Central Administration, Top Management] (B)

All statutory, contractual, and additional provisions that affect information security management MUST be identified and documented. The statutory, contractual, and additional provisions that are relevant to an organisation's individual departments SHOULD be presented in detail in a structured overview. This documentation MUST be kept up to date.

ORP.5.A2 Compliance with Framework Conditions [Supervisor, Central Administration, Top Management] (B)

Requirements identified as security-relevant MUST be incorporated when planning and designing business processes, applications, and IT systems, and when acquiring new components.

Managers who have a statutory responsibility for their organisation MUST ensure its compliance with statutory, contractual, and additional requirements. The responsibilities and authorities regarding compliance with these provisions MUST be defined.

Suitable safeguards MUST be identified and implemented in order to prevent violations of relevant requirements. If violations are identified, appropriate corrective measures MUST be taken in order to ensure compliance.

ORP.5.A3 ELIMINATED (B)

This requirement has been eliminated.

3.2. Standard Requirements

For module ORP.5 *Compliance Management*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

ORP.5.A4 Design and Organisation of Compliance Management [Top Management] (S)

A process for identifying all relevant statutory, contractual, and additional provisions that impact information security management MUST be established within organisations. Suitable processes and organisational structures SHOULD be established to ensure an overview of the various statutory requirements for the individual areas of a given organisation based on its identification of and compliance with the legal framework at hand. Persons responsible for compliance management SHOULD be appointed for this purpose.

An organisation's Compliance Manager and Chief Information Security Officer (CISO) SHOULD exchange information on a regular basis. They SHOULD integrate security requirements into compliance management, translate security-related requirements into security safeguards, and monitor their implementation together.

ORP.5.A5 Granting Exceptions [Supervisor, Chief Information Security Officer (CISO)] (S)

If it is necessary to deviate from regulations in a particular case, the exception SHOULD be justified and approved by an authorised body after a risk assessment. There SHOULD be an approval procedure for granting exceptions. An overview of all exemptions granted SHOULD be established and maintained. An appropriate procedure for documentation and a corresponding review process SHOULD be established. All exceptions SHOULD be granted for a limited period.

ORP.5.A6 ELIMINATED (S)

This requirement has been eliminated.

ORP.5.A7 ELIMINATED (S)

This requirement has been eliminated.

ORP.5.A8 Regular Reviews of Compliance Management (S)

A procedure SHOULD be established for regular checking of the efficiency and effectiveness of compliance management and the resulting requirements and safeguards (see also DER.3.1 *Audits and Revisions*). Regular examination of whether a given organisational structure and processes for compliance management are appropriate SHOULD be carried out.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module ORP.5 *Compliance Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

ORP.5.A9 ELIMINATED (H)

This requirement has been eliminated.

ORP.5.A10 ELIMINATED (H)

This requirement has been eliminated.

ORP.5.A11 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides information on compliance management systems in the standard ISO 19600:2014, "Compliance Management Systems – Guidelines".

The ISO standard ISO/IEC 27001:2013, "Information Technology – Security Techniques – Code of Practice for Information Security Controls", also addresses requirements management in section 18.

The Institute of Public Auditors in Germany (IDW) defines reference points for the auditing of compliance management systems in the publication IDW PS 980, “Principles for the Proper Auditing of Compliance Management Systems”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module ORP.5 *Compliance Management*.

G 0.29 Violation of Laws or Regulations

CON.1 Crypto Concept

1. Description

1.1. Introduction

Cryptography is widely used as a means of ensuring confidentiality, integrity, and authenticity in information security. Cryptographic procedures are used to encrypt information so that its content cannot be read without the corresponding key. These can be symmetrical procedures, where the same key is used for encryption and decryption, or asymmetrical procedures, where one key is used for encryption and another for decryption.

In a heterogeneous environment, both the data an organisation stores locally and that which it transfers can be effectively protected by cryptographic procedures and techniques.

Further safeguards are needed at the organisational and procedural levels. The use of cryptographic procedures alone is not sufficient to guarantee the confidentiality, integrity, and authenticity of encrypted information.

Within the framework of a crypto concept, all the cryptographic procedures used and the associated safeguards are considered together. Only a holistic view of this subject enables effective protection through cryptography.

Crypto modules are a special feature that can be used for cryptographic procedures to meet increased protection requirements. The term "crypto module" refers to a product that offers the security function specified in a given crypto concept. Such products may consist of hardware, software, firmware, or a combination thereof. In addition, components such as memory, processors, buses, and power supplies are necessary to implement crypto processes. A crypto module may be used in a wide variety of IT or telecommunication systems in order to protect sensitive data and information.

1.2. Objective

This module describes how a crypto concept can be created and how information in organisations can be cryptographically secured.

1.3. Scoping and Modelling

Module CON.1 *Crypto Concept* must be applied once for the entire information domain under consideration. This module covers general requirements, organisational framework conditions, and procedures for cryptographic products and methods. The core IT tasks associated with the operation of crypto modules are not addressed here. In this regard, the requirements of the modules of layer OPS.1.1 *Core IT Operation* must be met.

Ways to cryptographically secure individual IT systems (e.g. laptops) or communication links at the application level (e.g. encryption or hashing of passwords in a database) are not included in this module either. These topics are covered in the corresponding modules of the APP *Applications*, SYS *IT Systems* and NET *Networks and Communication* layers.

2. Threat Landscape

For module CON.1 *Crypto Concept*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inadequate Key Management for Encryption

Inadequate key management may grant attackers access to encrypted data. For example, a lack of rules may result in keys and the associated encrypted information being stored on the same data storage medium or being transmitted (unencrypted) via the same communication channel. When symmetrical methods are used, every person who can access the data storage medium or communication channel in question will thus be able to decrypt the information if the encryption method used is known.

2.2. Violation of Legal Framework Conditions Regarding the Use of Cryptographic Methods

If organisations use cryptographic methods and products, they must consider numerous legal framework conditions. In some countries, cryptographic methods may not be used without the consent of the government, for example. This may prevent recipients located abroad from reading encrypted datasets because they are not allowed to use the required cryptographic products, which may even make them liable to prosecution.

Furthermore, using products with strong encryption is significantly restricted in many countries. Users may thus be tempted to leave sensitive data unencrypted or to protect it using insecure methods. Besides making attacks easy, this may also violate national laws. For example, a country's data protection laws may specify that adequate cryptographic methods must be used in order to protect personal data.

2.3. Loss of Data Confidentiality or Integrity Due to Misbehaviour

If an organisation uses crypto modules that are too complicated, for example, its users may dispense with them for the sake of convenience or practicality and transfer information in plain text instead. As a consequence, attackers may eavesdrop on the information transmitted.

Errors in operating crypto modules may also result in confidential information being intercepted by attackers—for example, if the information is transmitted in plain text because the plain text mode has been enabled accidentally.

2.4. Software Vulnerabilities or Errors in Crypto Modules

Software vulnerabilities or errors in crypto modules impair the security of cryptographic procedures and can allow the information they protect to be read, among other consequences. Furthermore, attackers can manipulate crypto modules (including via malware) and thereby obtain organisation-critical data, or even bring entire production processes to a standstill if data can no longer be decrypted.

2.5. Failure of a Crypto Module

Crypto modules may fail due to technical defects, power failures, or wilful destruction. As a consequence, the decryption of data may not be possible while the required crypto module is unavailable. This could result in entire process chains coming to a standstill (e.g. if other IT applications depend on the data).

2.6. Insecure Cryptographic Algorithms or Products

Insecure or obsolete cryptographic algorithms can be cracked by an attacker using a modest amount of resources. In terms of encryption algorithms, this means that an attacker can succeed in converting encrypted text back into the original plain text without having to know any additional information, such as the cryptographic key. If insecure cryptographic algorithms are used, attackers may undermine the cryptographic protection and thereby access sensitive information within the respective organisation. Even if only secure (e.g. certified) products are used in an organisation, communication can still become insecure. This is the case, for example, if a communication partner uses cryptographic procedures that do not correspond to the state of the art.

2.7. Errors in Encrypted Data or Cryptographic Keys

If information is encrypted and the encrypted data is subsequently changed, it may no longer be possible to decrypt it properly. Depending on the mode of operation of the encryption routines, this may result in just a few bytes being decrypted incorrectly, or all of the data in question. If there is no backup, such data will be lost.

An error in the cryptographic keys used may be even more critical. Changing even a single bit of a cryptographic key may make it impossible to decrypt the data encrypted using the key.

2.8. Unauthorised Use of a Crypto Module

If an attacker manages to use a crypto module without authorisation, they may manipulate critical security parameters. As a consequence, the corresponding cryptographic methods will no longer provide for sufficient security. Moreover, an attacker may manipulate the crypto module in such a way that it works properly at first glance, but is actually in an insecure

condition. This way, the attacker may remain undetected for an extended period of time and access a great deal of information that is critical to the organisation in question.

2.9. Compromised Cryptographic Keys

The security of cryptographic methods depends to a great extent on how well the confidentiality of the cryptographic keys is maintained. A potential attacker will therefore usually try to determine the keys used. The attacker may succeed in this regard by reading volatile memory or finding unprotected keys that are stored in a backup, for example. If they know the key and the crypto method used, they can decrypt data with relative ease.

2.10. Forged Certificates

Certificates are designed to link a public cryptographic key to a person, IT system, or organisation. This link with the key is then protected cryptographically using a digital signature, which usually comes from a trustworthy neutral organisation.

These certificates are then used by third parties to verify digital signatures of the person, IT system, or organisation identified in the certificate. Alternatively, the key stored in the certificate can be used for an asymmetric encryption procedure to encrypt communication with the certificate holder.

If a certificate like this is forged, the digital signatures may be falsely verified as correct and associated with the person, IT system, or organisation in the certificate. Furthermore, data may be encrypted and sent with a key that is potentially insecure.

3. Requirements

The specific requirements of module CON.1 *Crypto Concept* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Process Owner, IT Operation Department, Supervisor

3.1. Basic Requirements

For module CON.1 *Crypto Concept*, the following requirements MUST be met as a matter of priority:

CON.1.A1 Selecting Appropriate Cryptographic Methods [Process Owner]

Appropriate cryptographic methods MUST be selected. In so doing, it MUST be ensured that established algorithms are used that have been examined intensively by experts and do not have any known vulnerabilities. The key lengths recommended at the time MUST also be used.

CON.1.A2 Backups When Using Cryptographic Methods [IT Operation Department] (B)

In backups, cryptographic keys MUST be stored and kept by the IT Operation Department in such a way that unauthorised persons cannot access them. Long-term cryptographic keys MUST be stored outside of the IT systems used.

For long-term storage of encrypted data, checks SHOULD be performed at regular intervals to determine whether the cryptographic algorithms and key lengths used still reflect the state of the art. The IT Operation Department MUST guarantee that data stored in encrypted form can still be accessed after longer periods. The crypto products used SHOULD be archived. The configuration data of crypto products SHOULD be backed up.

3.2. Standard Requirements

For module CON.1 *Crypto Concept*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

CON.1.A3 Encryption of Communication Links (S)

It SHOULD be determined whether communication links can be encrypted in a feasible manner with a reasonable amount of resources. If this is the case, communication links SHOULD be encrypted appropriately.

CON.1.A4 Appropriate Key Management (S)

Cryptographic keys SHOULD always be created with appropriate key generators in a secure environment. If possible, cryptographic keys SHOULD be used for one purpose only. In particular, different keys SHOULD be used for encryption and signature creation. The exchange of cryptographic keys SHOULD be carried out using a method that is considered secure.

If keys are used, the authenticity of the origin and integrity of the key data SHOULD be checked.

All cryptographic keys SHOULD be changed at a sufficient frequency. There SHOULD be a defined procedure for scenarios in which a key has been revealed. All created cryptographic keys SHOULD be stored and managed securely.

CON.1.A5 Secure Deletion and Destruction of Cryptographic Keys [IT Operation Department] (S)

Keys and certificates that are no longer needed SHOULD be deleted and destroyed securely.

CON.1.A6 Identifying the Need for Cryptographic Methods and Products [IT Operation Department, Process Owner] (S)

The business processes or specialised procedures that require cryptographic methods SHOULD be defined. The applications, IT systems, and communication links necessary to fulfil the tasks at hand SHOULD then be identified. The IT Operation Department SHOULD use suitable cryptographic mechanisms to secure these elements.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module CON.1 *Crypto Concept* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

CON.1.A7 Drawing Up a Security Policy for the Use of Cryptographic Methods and Products (H)

Based on its general security policy, an organisation SHOULD draw up a specific policy for the use of crypto products. In this security policy, the person responsible for the secure operation of cryptographic products SHOULD be specified. There SHOULD be deputising rules in connection with the crypto products used.

Necessary training and awareness safeguards SHOULD be defined for users, along with codes of conduct and reporting channels for potential problems or security incidents. Furthermore, the policy SHOULD define the methods used to ensure that crypto modules are configured securely, used properly, and maintained at regular intervals.

The policy SHOULD be known to all the relevant employees and SHOULD be integral to their work. If the policy is changed or deviations prove necessary, this SHOULD be coordinated with the CISO and documented accordingly. There SHOULD be regular checks on whether the policy is still being properly implemented. The results SHOULD be appropriately documented.

CON.1.A8 Determining the Factors That Influence Cryptographic Methods and Products (H)

Before a decision can be taken on which cryptographic methods and products will be used in the event of high protection requirements, the following influencing factors SHOULD be determined, among other considerations:

- security aspects (see CON.1.A6 *Identifying the Need for Cryptographic Methods and Products*)
- technical aspects
- personnel and organisational aspects
- economic aspects
- the lifecycles of cryptographic methods and the key lengths used
- approval of cryptographic products
- legal framework conditions

CON.1.A9 Selecting an Appropriate Cryptographic Product [IT Operation Department, Process Owner] (H)

Before selecting a cryptographic product, an organisation SHOULD define the requirements to be met by the product. Here, aspects such as the scope of functions, interoperability, efficiency, and protection against incorrect operation and malfunction SHOULD be considered. It SHOULD be checked whether certified products should be given priority. The selection process SHOULD also consider the future deployment locations due to the export and import restrictions on cryptographic products, for example.

As a general rule, products that do not make it possible to control the storage of keys SHOULD NOT be used.

CON.1.A10 Developing a Crypto Concept (H)

A crypto concept SHOULD be developed that is integrated into the security concept of the organisation in question. The concept SHOULD describe all the technical and organisational specifications for the cryptographic products used. Additionally, all the relevant applications, IT systems, and communication links SHOULD be listed. The created crypto concept SHOULD be updated at regular intervals.

CON.1.A11 Secure Configuration of Crypto Modules [IT Operation Department] (H)

Crypto modules SHOULD be installed and configured securely. All preset keys SHOULD be changed. Afterwards, whether the crypto modules work properly and can actually be operated by users SHOULD be tested.

Furthermore, the requirements for the operational environment SHOULD be defined. If an IT system is changed, whether the cryptographic methods used are still effective SHOULD be tested. The configuration of the crypto modules SHOULD be documented and checked at regular intervals.

CON.1.A12 Secure Separation of Roles When Using Crypto Modules [IT Operation Department] (H)

User roles SHOULD be defined when configuring a crypto module. Access control and authentication mechanisms SHOULD be used in order to verify whether an employee is actually allowed to use the desired service. The crypto module SHOULD be configured such that the authentication information has to be re-entered every time there is a role change or a specified period of inactivity as passed.

CON.1.A13 Operating System Security Requirements When Using Crypto Modules (H)

The interaction between the operating system and the crypto modules SHOULD ensure the following:

- the crypto modules installed cannot be disabled or circumvented without this being noticed.
- the applied or stored keys cannot be compromised.

- the data to be protected can only be stored on storage media without encryption or leave the information-processing system with the knowledge of and under the control of the user
- attempted manipulations of the crypto module will be detected.

CON.1.A14 Training of Users and Administrators [Supervisor, Process Owner, IT Operation Department] (H)

There SHOULD be training for users and administrators on handling the relevant crypto modules. The meaning of the security settings of crypto modules and why they are important SHOULD be explained in detail to the users. Furthermore, they SHOULD be made aware of the threats that result from bypassing or disabling these security settings for the sake of convenience. The training content SHOULD always be adapted to the particular operational scenarios at hand.

Administrators SHOULD also receive specific training on the administration of crypto modules. They SHOULD also be provided with an overview of basic cryptographic terms.

CON.1.A15 Reacting to the Practical Weakening of a Crypto Method (H)

A process SHOULD be established that can be used in the event of a weakened cryptographic method. In so doing, it SHOULD be ensured that the weakened cryptographic method can be secured or will be replaced with an appropriate alternative.

CON.1.A16 Physical Protection of Crypto Modules [IT Operation Department] (H)

The IT Operation Department SHOULD ensure that unauthorised physical access to the contents of a crypto module is prevented. Hardware and software products used as crypto modules SHOULD be able to perform a self-test.

CON.1.A17 Emission Security [IT Operation Department] (H)

Whether additional safeguards are necessary for emission security SHOULD be examined. In particular, this SHOULD be ensured when processing government material that is classified as VS-VERTRAULICH (VS-CONFIDENTIAL) or higher.

CON.1.A18 Cryptographic Replacement Modules [IT Operation Department] (H)

Replacement crypto modules SHOULD be kept available.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) deals with the topic of cryptography in ISO/IEC 27001:2013 (annex A.10) on the basis of two guidelines.

The BSI has produced “Leitfaden Erstellung von Kryptokonzepten” [Guidelines for Creating Crypto Concepts] and a "Musterkryptokonzept" [Crypto Concept Model], which can support organisations in creating their own crypto concepts.

The BSI Technical Directive “BSI-TR-02102: Crytographic Mechanisms: Recommendations and Key Lengths” should be observed when selecting encryption methods and key lengths.

The Information Security Forum (ISF) has developed requirements for crypto concepts in “The Standard of Good Practice for Information Security” (area TS2, "Cryptography”).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module CON.1 *Crypto Concept*.

G 0.13 Interception of Compromising Interference Signals

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

CON.2 Data Protection

1. Description

1.1. Introduction

The aim of data protection is to protect individuals so that the use of their personal data by third parties does not affect their fundamental rights. The constitution of the Federal Republic of Germany includes citizens' fundamental right to decide how their personal data is used. The federal and state data protection laws refer to this when they emphasise the protection of the right to informational self-determination. In Article 8, the EU Charter of Fundamental Rights directly describes the right to protection of personal data (paragraph 1), highlights the necessity of a legal basis for data processing (paragraph 2), and prescribes the monitoring of compliance with data protection regulations by an independent body (paragraph 3). The General Data Protection Regulation (GDPR) provides more details on the requirements of the Charter of Fundamental Rights. Article 5 of the GDPR, which states the basic principles for processing personal data (and specifies some of them as protection goals), is of central importance in this regard. The German Standard Data Protection Model (SDM) offers a method of systematically monitoring the required implementation of data protection regulations on the basis of seven data protection goals.

1.2. Objective

The aim of this module is to show how the requirements of the German Standard Data Protection Model relate to IT-Grundschutz.

1.3. Scoping and Modelling

Module CON.2 *Data Protection* is intended for users in Germany as a basic guide to identifying components that process or otherwise use personal or person-related data as part of the effort to determine protection needs. Each organisation should then assess whether the module should be applied not just to individual information domains or procedures, but to its entire undertaking.

The conference of the independent federal and state data protection agencies (also known as the Data Protection Conference, or DSK) developed the German Standard Data Protection

Model as a concept that systematises the technical and organisational safeguards stated in the German and European legal regulations on the basis of data protection goals. On the one hand, the model is used by the bodies responsible for processing to systematically plan and implement required safeguards. It thus promotes the data protection-compliant design and organisation of information technology processes and applications. On the other hand, the model offers the data protection agencies a way to render a transparent, comprehensible, and robust overall assessment of a given method and its components using a uniform system. As a method, the SDM is suitable for regularly checking and professionally evaluating the effectiveness of the technical and organisational safeguards of a given data processing system on the basis of and in accordance with the criteria of the GDPR.

For the selection of appropriate technical and organisational safeguards, the SDM adopts the perspective of data subjects in asserting their fundamental rights, which is why it differs significantly from the viewpoint of IT-Grundschutz, which focuses primarily on information security and seeks to protect data-processing organisations. In the SDM, safeguards are selected based on the impairment that data subjects must accept as a result of a given organisation's data processing activities.

Against this background, a distinction must be made between the selection of safeguards to ensure information security for organisations and the selection of safeguards to ensure data subjects' rights. The IT-Grundschutz methodology primarily promotes information security; the SDM is meant to preserve data subjects' rights.

The SDM thus seeks to fulfil the following standards:

- it transfers requirements under data protection law into a catalogue of data protection goals
- it divides the considered methods into three components: data, IT systems, and processes
- it factors in the categorisation of data into three levels of information security requirements—"normal", "high", and "very high"—and supplements this classification with corresponding considerations at the level of processes and IT systems
- it offers a catalogue with standardised protective safeguards

2. Threat Landscape

For module CON.2 *Data Protection*, the following specific threats and vulnerabilities are of particular importance:

2.1. Non-Compliance with Data Protection Laws or Use of an Incomplete Risk Model

According to the EU General Data Protection Regulation, the processing of personal data is generally prohibited. Collecting, using, and transferring such data is only permitted when allowed or ordered by a statutory provision, or if the person in question has given express advance consent (see GDPR, Article 6).

From the perspective of data protection, an organisation that collects, uses, transfers, or receives (in summary: "processes") personal data fundamentally poses a risk to individuals. This risk still exists when an organisation's data processing activities are legally compliant.

In contrast, it places individuals at an even higher risk when an organisation does not sufficiently tie its data processing to a specific purpose, interprets this purpose too liberally, or carries out data processing for no specific purpose at all. The same applies if an organisation processes personal data in a non-transparent manner or without safeguards to secure integrity and does not provide data subjects with ways to intervene.

Cases in which data is accessed by third parties in ways that do not serve the purpose of the original data processing in question also present a frequent danger in practice. Such access typically pertains to foreign parent companies, security authorities, banks and insurance companies, public service administrations, IT manufacturers and IT service providers, or research organisations. In these contexts, the justification for access is often not checked—for example, because a long-established practice is being continued. Subordinate employees may also shy away from the personal risk of questioning whether there is a sufficient legal basis for such access. Furthermore, when an organisation's legal department or data protection officer report negative findings in this regard, those in charge often decide not to take corresponding action.

Both individuals and the organisations responsible face further risk if no standard processes are provided for lawful access to IT services or the transmission of data files by third parties. The same applies if no evidence of compliance can be provided in the form of protocols and documentation.

Insufficient data security also poses a significant risk to persons/employees. Recital 75 of the GDPR describes the risks associated with the processing of personal data and the corresponding threat posed by unauthorised access as follows: “The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security safeguards; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.”

2.2. Definition of Insufficient Protection Needs

Incorrect assessments of the need to protect their personal data represent another danger to persons/employees. These protection needs, which an organisation typically determines itself

when it is responsible for processing personal data, can be inaccurate or insufficient for various reasons:

- The organisation has not considered the catalogue of data protection goals that extends beyond information security.
- When determining the protection needs, the organisation did not distinguish between the risks regarding the implementation of data subjects' fundamental rights and the risks to the organisation.
- Although the organisation did distinguish between these two protection interests, it has designed the functions of its procedure and its protective safeguards in its own favour or to the disadvantage of data subjects.

3. Requirements

The specific requirements of module CON.2 *Data Protection* are listed below. As a matter of principle, the Data Protection Officer is responsible for monitoring compliance with the requirements of the GDPR (for details and restrictions, see GDPR, Art. 39). The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Data Protection Officer
Further responsibilities	

3.1. Basic Requirements

For module CON.2 *Data Protection*, the following requirements MUST be met as a matter of priority:

CON.2.A1 Implementing the German Standard Data Protection Model (B)

Compliance with the legal provisions on data protection MUST be ensured at the EU, federal, and state levels (GDPR, BDSG, and LDSG). If the SDM methodology is not taken into account (i.e. the safeguards are not systematised on the basis of the protection goals and compared with the SDM reference safeguards catalogue), this SHOULD be justified and documented.

3.2. Standard Requirements

No standard requirements are defined for module CON.2 *Data Protection*.

3.3. Requirements in Case of Increased Protection Needs

No requirements for increased protection needs are defined for module CON.2 Data Protection.

4. Additional Information

4.1. Useful Resources

EU General Data Protection Regulation: “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”, imposes fundamental, Europe-wide legal requirements for data protection compliance.

“The Standard Data Protection Model – A method for Data Protection advising and controlling on the basis of uniform protection goals” from the technology working group (*AK Technik*) of the Independent Data Protection Supervisory Authorities at the federal and state levels provides a method for implementing the requirements of data protection law.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module CON.2 *Data Protection*.

G 0.18 Poor Planning or Lack of Adaptation

Federal Office
for Information Security

CON.3 Backup Concept

1. Description

1.1. Introduction

Organisations are storing ever increasing amounts of data and becoming increasingly dependent on it at the same time. If data is lost due to defective hardware, malware, or inadvertent deletion, for example, this may result in serious damage. Conventional IT systems such as servers or clients can be affected. However, routers, switches, and IoT devices can also store sensitive information, such as configurations. In this module, the term “IT system” therefore includes all forms of IT components that store sensitive information.

The effects of data loss can be minimised through regular data backups. A data backup is a means of ensuring that IT operations can be resumed quickly with a redundant copy of an organisation's data if some of the actively used data is lost. An organisation's data backup concept thus also plays a central role in contingency planning. The essential requirements of contingency planning, such as the maximum permissible data loss (recovery point objective, RPO), should be taken into account in backup concepts.

In addition to the creation of backups as a preventive measure, a comprehensive data protection concept should consider how completed backups will be restored on the original system. A wide variety of solutions can be used for backups, such as:

- Storage systems
- Tape drives
- Mobile removable media (USB pen drives or external hard disks)
- Optical storage media
- Online solutions

This module refers to such solutions collectively as "storage media for backups". In contrast, data mirroring via RAID systems is not considered a backup because the mirrored data is changed at the same time. This means that data mirroring via a RAID system can prevent a failure due to a hardware defect in individual storage media, but it cannot protect against unintentional overwriting or malware infections.

1.2. Objective

The aim of this module is to show how organisations can create a data protection concept and use it to adequately secure their data against loss.

1.3. Scoping and Modelling

CON.3 *Backup Concept* must be applied once for the entire information domain under consideration.

The module describes basic specifications that help ensure an appropriate backup concept. Requirements for the long-term storage and maintenance of electronic documents are not addressed. These are included in module OPS.1.2.2 *Archiving*.

This module also does not cover any system- or application-specific properties of backups. The backup concept requirements of this kind are covered in the corresponding modules of the NET *Networks and Communication*, SYS *IT Systems,* and APP *Applications* layers.

For deleting and destroying backups, module CON.6 *Deleting and Destroying Data and Devices* must be taken into account.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module CON.3 *Backup Concept*, the following specific threats and vulnerabilities are of particular importance.

2.1. Lack of Backups

If data is lost that has not been backed up beforehand, this can have consequences that threaten the existence of an organisation. Data can be lost due to malware, technical malfunctions, or a fire, for example, but also if employees delete data (whether intentionally or unintentionally).

2.2. Lack of Recovery Tests

Backing up data regularly does not automatically guarantee that it can be restored without problems. If data backups are not regularly tested to see if they can be restored, doing so may not be possible.

2.3. Unsuitable Storage of Backup Media

Regardless of whether conventional tapes or modern storage systems are involved, storage media used for backups contain a great deal of sensitive information on the respective organisation. If backup storage media are not stored in a secure location, an attacker may be able to access them and steal or manipulate sensitive information. Backup storage media can also become unusable due to unfavourable storage conditions. The information stored on them may then no longer be available.

2.4. Inadequate Documentation

If an organisation's measures regarding backups and, in particular, recovery are documented insufficiently (or not at all), this can significantly delay recovery. This in turn can result in delays in important processes (e.g. in production). It may also mean that a backup cannot be restored and the data is thus lost.

If information on recovery is only available digitally, there is a risk that it will also be lost in the event of major damage (caused by ransomware, for instance), which jeopardises the recovery process.

2.5. Non-Compliance with Statutory Regulations

If an organisation fails to comply with statutory regulations such as data protection laws, it may be required to pay fines or damages.

2.6. Using Insecure Providers for Online Backups

If an organisation outsources its backups to another provider, attacks on this provider can also affect the organisation's data. This can lead to an outflow of sensitive data.

There is also a risk that unfavourable contractual conditions will result in backups not being available at short notice. This would make it impossible to restore them within a defined period of time in an emergency.

2.7. Insufficient Storage Capacity

Insufficient capacity on storage media used for backups can result in a failure to back up the most recent data. Software used for backups may also automatically overwrite old backups that are still required. If the persons responsible are not informed (due to insufficient monitoring, for example), data could be lost completely. This could also mean that only outdated versions are available in an emergency.

2.8. Inadequate Backup Concept

If an appropriate concept is not created for backup measures, this may lead to business requirements being disregarded for the affected business processes. If the recovery time or backup intervals are not taken into account, this could mean the backups are not suitable for restoring data in the event of a loss.

In addition, the storage medium for a backup can become a preferred target for attack if valuable data from all of an organisation's business processes is stored on it in a condensed format.

Furthermore, organisational deficiencies can lead to situations in which a backup is unusable. For example, if a backup is encrypted and the key for decrypting it is also affected by a data loss, it will not be possible to restore the data. This could happen if the key is not stored separately.

2.9. Insufficient Data Backup Speed

In addition to the storage space required for backups, the time needed to perform them is also increasing. In the worst case, this can mean that a backup has not yet been completed when a new backup begins, which can lead to various problems. Under certain circumstances, the backup that has not yet been completed could be terminated, and no further complete backups would be performed as a consequence. Alternatively, the backup solution could try to perform the new backup in parallel with the previous one and the backup system could end up failing under the increasing load.

2.10. Ransomware

Ransomware is a special form of malware that encrypts data on infected IT systems. Attackers subsequently demand payment of a ransom, claiming that they will then enable the victim to decrypt the data again. In the absence of backups, the encrypted data is lost in many cases or can only be recovered by paying the ransom. Even after the ransom is paid, however, there is no guarantee that the data can be recovered.

Many forms of ransomware look for network drives with write access in order to encrypt all their data, as well. This means that all encrypted information dating back to the most recent backup can be lost, even if a ransom is paid. Along with the IT system originally infected, this may affect centrally stored information accessed by multiple IT systems.

If backup storage media are not sufficiently secured, there is also the danger that they themselves will be affected by a ransomware attack and the information stored on them (backups) may be encrypted.

3. Requirements

The specific requirements of module CON.3 *Backup Concept* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Process Owner, IT Operation Department, Employee

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For module CON.3 *Backup Concept*, the following requirements MUST be met as a matter of priority.

CON.3.A1 Determining the Factors That Influence Backups [Process Owner, IT Operation Department] (B)

The IT Operation Department MUST ascertain the framework conditions for backups of each IT system and the applications executed on them. For this purpose, the application Process Owners MUST define their requirements for data protection. At minimum, the IT Operation Department MUST agree the following framework conditions with the Process Owners:

- Data to be backed up
- Storage space
- Change volumes
- Changing times
- Availability requirements
- Confidentiality requirements
- Integrity requirements
- Legal requirements
- Requirements for deleting and destroying data
- Responsibilities for backing up data

The parameters MUST be recorded in a clear and appropriate manner. New requirements MUST be considered promptly.

CON.3.A2 Establishment of Backup Procedures [Process Owner, IT Operation Department] (B)

The IT Operation Department MUST determine the procedure for how data is to be backed up.

A backup procedure MUST define the type, frequency, and times of backups. This MUST be based on the parameters that have been determined and involve the Process Owners of the respective applications. The storage media to be used and the manner in which they are to be transported and stored MUST also be defined. Backups MUST always be stored on separate storage media. Backup storage media requiring particular protection SHOULD only be connected to the respective organisation's network or the source system during backup and restoration procedures.

For virtual environments and storage systems, checks SHOULD be carried out on whether the IT system at hand can be additionally backed up by snapshot mechanisms in order to create several quickly recoverable intermediate versions between the complete backups.

CON.3.A3 ELIMINATED (B)

This requirement has been eliminated.

CON.3.A4 Creating Backup Plans [IT Operation Department] (B)

The IT Operation Department MUST create backup plans based on the defined backup procedure at hand. These MUST define the minimum backup requirements to be met. At minimum, the backup plans MUST contain short descriptions of the following:

- The IT systems and data to be included in each backup
- The order in which IT systems and applications should be restored
- How the backups can be created and restored
- How long backups should be stored
- How backups can be protected from unauthorised access and overwriting
- The parameters to be selected
- The hardware and software to be used

CON.3.A5 Regular Backups [IT Operation Department] (B)

Regular data backups MUST be made in line with the applicable backup plans. All employees MUST be informed of their organisation's backup regulations. They MUST also be informed of the tasks they are to perform in the creation of backups.

CON.3.A12 Secure Storage of Backup Media [IT Operation Department] (B)

Backup storage media MUST be kept physically separate from the backed-up IT systems. They SHOULD be stored in a different fire zone. The storage location SHOULD be air-conditioned in such a way that the storage media can be stored for the amount of time specified in the backup concept at hand.

CON.3.A14 Protection of Backups [IT Operation Department] (B)

Created backups MUST be suitably protected against unauthorised access. In particular, it MUST be ensured that backups cannot be overwritten intentionally or unintentionally. IT systems used for data protection SHOULD only allow write access to backup storage media for authorised backup or administrative activities. Alternatively, backup media SHOULD only be connected to the corresponding IT systems for authorised backups or authorised administrative activities.

CON.3.A15 Regular Backup Testing [IT Operation Department] (B)

Tests MUST be performed regularly to determine whether the backup process is working as desired, and especially whether the backed-up data can also be restored without any problems within an appropriate period of time.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

CON.3.A6 Developing a Backup Concept [Process Owner, IT Operation Department] (S)

An organisation SHOULD prepare a backup concept that includes at least the following points:

- Definitions of essential aspects of backups (e.g. different types of backup procedures)
- Threat landscape
- Factors influencing each IT system or group of IT systems
- Backup plans for each IT system or group of IT systems
- Relevant findings from business continuity management, in particular the recovery point objective (RPO) for each IT system or group of IT systems.

The IT Operation Department SHOULD coordinate the backup concept with the Process Owners responsible for the applications affected. If a central backup system is used, it SHOULD be noted that there may be a higher need for protection due to the concentration of data. Backups SHOULD be carried out regularly in line with the backup concept.

The backup concept itself SHOULD also be included in backups. The technical information contained in the backup concept to restore systems and backups (backup plans) SHOULD be backed up in such a way that it will be available even if the backup systems themselves fail.

Employees SHOULD be informed about the parts of the backup concept that concerns them. The proper implementation of the backup concept SHOULD be checked regularly.

CON.3.A7 Procuring a Suitable Backup System [IT Operation Department] (S)

Before procuring a backup system, the IT Operation Department SHOULD create a requirements list to evaluate the products available on the market. The backup systems an organisation purchases SHOULD meet the requirements of its backup concept.

CON.3.A8 ELIMINATED (S)

This requirement has been eliminated.

CON.3.A9 Prerequisites of Online Backups [IT Operation Department] (S)

If online storage is to be used for backups, the following points SHOULD be contractually regulated at minimum:

- How the corresponding contract is formulated
- Where the data will be stored
- Service level agreements (SLAs), particularly in terms of availability
- Suitable authentication methods for access
- Encryption of data stored online
- Transport encryption

In addition, the backup system and network connection in question SHOULD offer performance that will not exceed the permissible backup or restore times.

CON.3.A10 ELIMINATED (S)

This requirement has been eliminated.

CON.3.A11 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

CON.3.A13 Using Cryptographic Methods for Backups [IT Operation Department] (H)

The IT Operation Department SHOULD encrypt all backups to ensure the confidentiality of backed-up data. It SHOULD be ensured that encrypted data can be restored even after extended periods of time. The cryptographic keys used SHOULD be protected by a separate backup.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) specifies requirements for backup concepts in ISO/IEC 27002:2013 (“12.3 Backup”).

Germany's digital association, Bitkom, has produced a guide to carrying out backups in the publication “Leitfaden Backup / Recovery / Disaster Recovery”.

Section “SY2.3 Backup” of “The Standard of Good Practice for Information Security” published by the Information Security Forum (ISF) provides guidelines for backups.

The National Institute of Standards and Technology details requirements for backups in NIST Special Publication 800-53 (“CP-9 Information System Backup”).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module CON.3 *Backup Concept*.

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

T 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.29 Violation of Laws or Regulations

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Federal Office
for Information Security

CON.6 Deleting and Destroying Data and Devices

1. Description

1.1. Introduction

The deletion and destruction of data and devices is a fundamental part of the lifecycle of information on storage media. In this module, the term "storage media" refers to analogue storage media such as paper or films, as well as digital storage media such as hard disks, SSDs, or CDs.

If storage media are discarded, the information contained on them could be disclosed if the media have not been securely deleted or completely destroyed. In addition to clients and servers, this can affect all IT systems (including IoT devices such as smart TVs) that purportedly only store insignificant information. IoT devices are often connected via a WLAN and store the access data this requires. This can be sensitive data that should not be disclosed to unauthorised persons.

Ordinary deletion processes based on operating system functions do not usually delete information in a secure way that prevents the data from being reconstructed. Special procedures are therefore required to securely delete information. However, storage media can only be deleted securely and effectively in their entirety, and this is usually only possible to a limited extent with individual files.

In addition, there are legal provisions (such as the German Commercial Code or data protection laws) that have far-reaching consequences for the deletion and destruction of documents. On the one hand, such laws call for retention periods that prohibit the early deletion of business transactions, balance sheets, or contracts, for example. On the other, legal entitlements to the secure and prompt deletion of data result from these legal provisions when, for example, personal data is affected.

1.2. Objective

This module describes how information in organisations can be securely deleted and destroyed and how a corresponding holistic concept can be created.

1.3. Scoping and Modelling

Module CON.6 *Deleting and Destroying Data and Devices* must be applied once to the entire information domain under consideration. It includes general process-related, technical, and organisational requirements for deletion and destruction. This module only covers the secure deletion and destruction of complete storage media, as the secure deletion of individual files is usually only possible to a limited extent.

2. Threat Landscape

For module CON.6 *Deleting and Destroying Data and Devices*, the following specific threats and vulnerabilities are of particular importance:

2.1. Non-Existent or Insufficiently Documented Regulations for Deletion and Destruction

If there are no secure processes and procedures for deleting and destroying information and storage media (or they are not used correctly), there is no guarantee that confidential information will be securely deleted or destroyed. It is therefore impossible to foresee where this information will end up and whether it will be accessible to third parties. This danger is particularly high in the case of digital media and IT systems that are to be discarded, as it is not always immediately apparent what (residual) information is on them. This information can be read by unauthorised third parties. If it is particularly sensitive information, such as trade secrets or sensitive personal data within the meaning of Article 9 of the GDPR, this can result in high fines.

2.2. Loss of Confidentiality due to Residual Information on Storage Media

Most standard applications and operating systems do not delete data in a secure way that is completely irreversible. Only the references to the file are removed from the administration information of the file system and the blocks that belong to the file are marked as free. However, the actual content of the blocks on the storage medium is retained and can be reconstructed with appropriate tools. This can enable attackers to access the files, such as when storage media are handed over to third parties or disposed of inappropriately. Confidential information may thus fall into the hands of unauthorised parties.

Swap files, swap partitions, and files for hibernation mode sometimes also contain confidential data such as passwords or cryptographic keys. However, this data and its contents are often not protected. They can be read, for example, if storage media are removed and reinstalled in another IT system.

The live operation of many applications also produces files not required for production environments, such as browser histories. These files can include security-relevant information, as well. If swap files or temporary files are not securely deleted, sensitive information, passwords, and keys can be misused by unauthorised parties to gain access to further IT systems and data, obtain a competitive edge on the market, or spy on the behaviour of users in a targeted manner.

2.3. Inappropriate Involvement of External Service Providers in the Deletion and Destruction Process

When storage media are deleted or destroyed by external service providers, the information on them could be exposed if there is not sufficient regulation on how the external service provider is integrated into the process of deletion and destruction.

For example, attackers could steal storage media from inadequately secured collection points or gain access to residual information if a service provider does not delete or destroy the storage media with a sufficient level of security.

2.4. Inappropriate Handling of Defective Storage Media or IT Devices

If a storage medium is defective, it does not necessarily mean that the data on it is irreversibly damaged. In many cases, the data (or at least parts of it) can be recovered with special tools. If defective storage media or IT devices are simply disposed of without deleting or destroying the data on them, this data could be disclosed during the disposal process.

The data on defective storage media could also be disclosed in the course of repairs or warranty claims. Imagine, for example, that an organisation sends a defective hard disk back to the manufacturer under a warranty claim. They detects a defect in the controller and replace the defective model with a new one for the customer. At the time the defective controller is replaced by a new one, the originally defective hard disk is only quickly and thus insecurely deleted. The hard disk is then returned to the market. In this process, sensitive information can be disclosed throughout the entire process, as it is still on the original hard disk.

3. Requirements

The specific requirements of module CON.6 *Deleting and Destroying Data and Devices* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Employee, Process Owner, Data Protection Officer, Central Administration, IT Operation Department

3.1. Basic Requirements

For module CON.6 *Deleting and Destroying Data and Devices*, the following requirements MUST be implemented as a matter of priority:

CON.6.A1 Regulations for Deleting or Destroying Information [Central Administration, Process Owner, Data Protection Officer, IT Operation Department] (B)

An organisation MUST regulate the deletion and destruction of information. In doing so, the Process Owners for each specialised procedure or business process MUST specify which information must be deleted and disposed of under which conditions.

They MUST consider legal provisions that:

- define the minimum retention periods
- guarantee the maximum retention periods and the right to the secure deletion of personal data

If personal data is involved, the regulations for deleting and destroying personal data MUST be coordinated with the Data Protection Officer.

The deletion and destruction of information MUST be regulated for specialised procedures, business processes, and IT systems before they are used productively.

CON.6.A2 Proper Deletion and Destruction of Sensitive Resources and Information (B)

Sensitive information and storage media MUST be securely deleted or destroyed prior to disposal. The process for this MUST be clearly regulated. Individual employees MUST be informed of the tasks they need to perform for secure deletion and destruction. The process for deleting and destroying storage media MUST also take account of backups when necessary.

The location of destruction facilities on an organisation's premises MUST be clearly regulated. In this regard, it MUST be considered that information and resources may be collected first and only deleted or destroyed later. A central collection point of this kind MUST be protected against unauthorised access.

CON.6.A11 Deletion and Destruction of Storage Media by External Service Providers (B)

If external service providers are commissioned, the process for deletion and destruction MUST be sufficiently secure and transparent. The procedures used by an external service provider for secure deletion and destruction MUST at least meet the corresponding organisation’s internal requirements for deletion and destruction procedures.

Those commissioned with deletion and destruction SHOULD be regularly audited to ensure that their operations are still proceeding correctly.

CON.6.A12 Minimum Requirements for Deletion and Destruction Procedures (B)

An organisation MUST implement the following minimum procedures for deleting and destroying sensitive storage media. These procedures SHOULD be reviewed and adapted as necessary, depending on the protection needs of the data being processed.

- Rewritable digital media that are not encrypted during use MUST be completely overwritten with a data stream of random values (e.g. a PRNG stream).
- If encrypted digital media are used, they MUST be erased through secure deletion of the corresponding key in compliance with the respective crypto concept.
- Optical storage media MUST be destroyed in accordance with security level O-3 (at minimum) as defined in ISO/IEC 21964-2.
- Smartphones and other smart devices SHOULD be encrypted in line with the crypto concept in question. Smartphones and other smart devices MUST be reset to factory settings. The setup process SHOULD then be carried out to complete the deletion.
- IoT devices MUST be reset to factory settings. All the credentials stored in such devices MUST then be changed.
- Paper MUST be destroyed in accordance with security level P-3 (at minimum) as defined in ISO/IEC 21964-2.
- Storage media integrated in other devices MUST be securely erased via the devices' integrated functions. If this is not possible, the mass storage components MUST be removed and either securely erased like conventional digital media from a separate IT system, or destroyed in accordance with security level E-3 or H-3 (at minimum) as specified in ISO/IEC 21964-2.

3.2. Standard Requirements

For module CON.6 *Deleting and Destroying Data and Devices*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

CON.6.A3 ELIMINATED (S)

This requirement has been eliminated.

CON.6.A4 Selecting Suitable Methods for Deleting or Destroying Storage Media (S)

An organisation SHOULD verify that the minimum requirements for deletion and destruction procedures (see CON.6.A12 *Minimum Requirements for Deletion and Destruction Procedures*) are sufficiently secure for the media and information actually used. Based on its findings, the organisation SHOULD determine appropriate procedures for deletion and destruction of each storage media.

For all the types of storage media the organisation uses and deletes or destroys itself, there SHOULD be suitable devices and tools with which the responsible employees can delete or destroy stored information. The selected procedures SHOULD be known to all the employees responsible.

The organisation SHOULD regularly check that the selected methods still correspond to the state of the art and are sufficiently secure for its purposes.

CON.6.A5 ELIMINATED (S)

This requirement has been eliminated.

CON.6.A6 ELIMINATED (S)

This requirement has been eliminated.

CON.6.A7 ELIMINATED (S)

This requirement has been eliminated.

CON.6.A8 Creating a Policy for Deleting and Destroying Information [Employee, IT Operation Department, Data Protection Officer] (S)

An organisation SHOULD document its regulations regarding deletion and destruction in a policy. The policy SHOULD be known to all the relevant employees of the organisation and represent the basis for their actions and work. In terms of its content, the policy SHOULD include all employed storage media, applications, IT systems, and other resources and information that are subject to deletion and destruction. Employee compliance with the policy SHOULD be checked regularly and at random. The policy SHOULD be updated at regular intervals.

CON.6.A9 ELIMINATED (S)

This requirement has been eliminated.

CON.6.A13 Destruction of Defective Digital Storage Media (S)

If, due to a defect, digital storage media containing sensitive information cannot be securely deleted in accordance with the applicable procedures for deleting storage media, they SHOULD be destroyed in accordance with security level 3 (at minimum) of ISO/IEC 21964-2.

In the event that defective storage media are replaced or repaired instead, it SHOULD be contractually agreed with the service provider contracted for this purpose that these media will be securely deleted or destroyed by the service provider. The service provider's procedures SHOULD at least meet the organisation's internal requirements for deletion and destruction procedures.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module CON.6 *Deleting and Destroying Data and Devices* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

CON.6.A10 ELIMINATED (H)

This requirement has been eliminated.

CON.6.A14 Destruction of Storage Media at Increased Security Levels (H)

The organisation SHOULD determine the required security level for the destruction of data media in accordance with ISO/IEC 21964-1, based on the protection needs of the data media to be destroyed. The media SHOULD be destroyed in accordance with the assigned security level outlined in ISO/IEC 21964-2.

4. Additional Information

4.1. Useful Resources

In the ISO/IEC 27001:2013 standard (annex A, “A.8.3 Media handling”), the International Organization for Standardization (ISO) provides guidelines for the handling of media and information, including on deletion and destruction.

The ISO has also produced publications on the destruction of storage media in the series of standards ISO/IEC 21964 (“Information technology – Destruction of data carriers”), which builds on the standard DIN 66399 ("Office and data technology – Destruction of data carriers”):

- Part 1: Principles and definitions
- Part 2: Requirements for equipment for destruction of data carriers
- Part 3: Process of destruction of data carriers

The National Institute of Standards and Technology provides guidelines for deletion and destruction in NIST Special Publication 800-88, “Guidelines for Media Sanitization”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module CON.6 *Deleting and Destroying Data and Devices*.

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.24 Destruction of Devices or Storage Media

Federal Office
for Information Security

CON.7 Information Security on Trips Abroad

1. Description

1.1. Introduction

Work-related travel is now part of everyday life in many organisations. To be able to continue working outside the normal work environment, people need to travel with both hard-copy documents and information technology such as laptops, smartphones, tablets, removable hard drives, or USB pen drives. For business trips, particularly those abroad, there are a multitude of threats and risks to information security that do not exist during normal business operations.

Each trip must be assessed separately since there is always a different threat level—depending on the combination of the purpose of the trip (e.g. a business meeting, conference, congress, or seminar), the duration, and the destination—which also affects the protection of business-critical information.

The threat landscape is particularly critical when travelling due to factors such as public networks that are not under the control of a given employee's organisation. This means that risks the organisation has already addressed may become relevant again. Depending on the destination country, the risks one faces on foreign trips is also often significantly higher than on domestic trips.

When employees are constantly travelling to different destinations with varying regulatory and legal requirements, it is not always easy to protect operational information. Legal requirements and border control checks can become stricter, for example, and thereby affect the preservation of data confidentiality. This leads to special information security requirements that depend on the type and duration of a given trip, as well as the destination. Specific political, societal, religious, geographical, climatic, legal, and regulatory considerations play a significant role in this regard.

1.2. Objective

This module describes ways to protect the confidentiality, integrity, and availability of all types of information which is taken on trips abroad, whether in electronic or physical form. The confidential information all travelling employees take with them in the form of knowledge is also the subject of this module. Furthermore, it outlines appropriate regulations and safeguards for handling sensitive information and data when travelling abroad. Areas to consider include basic framework conditions relating to IT, data protection and the law.

This module highlights the risks and requirements of specific scenarios that are directly related to the secure use of information technology, information, and devices when travelling abroad.

It is designed to be used by the persons in charge in an organisation as a guide to establishing appropriate security safeguards in the context of information security on such trips. It indicates the fundamental principles that should be taken into account in this regard. Many of these threats also apply when travelling domestically or, more fundamentally, when processing information in environments that are not under the control of the organisation in question.

1.3. Scoping and Modelling

Module CON.7 *Information Security on Trips Abroad* must be applied once to the information domain under consideration if employees are to carry or process sensitive information when travelling or temporarily working abroad.

The module encompasses the fundamental requirements which contribute to the appropriate protection of information on such trips. Protecting the confidentiality and integrity of sensitive information is just as important in this regard as it is at an organisation's headquarters.

Threats and requirements relating to the local information domain in question are not taken into consideration here.

Since the process-related, technical, and organisational requirements that are specific to working while travelling are the focus of module CON.7 *Information Security on Trips Abroad*, the requirements in the layers NET *Networks and Communication*, SYS *IT Systems*, and APP *Applications* are not considered. All the necessary modules, especially SYS.2.1 *General Client*, NET.3.3 *VPN* and SYS.3.2.2 *Mobile Device Management (MDM)*, must be considered separately.

The requirements of modules INF.9 *Mobile Workplace* and OPS.1.2.4 *Teleworking*, which cover similar topics, should also be considered and implemented.

The present module also overlaps with other modules and topic areas that are not taken into consideration here, including:

- fulfilment of data protection requirements
- preventive measures for the protection of information (including technical demands placed on portable IT systems with regard to emission or eavesdropping protection, for example)

- personal security

2. Threat Landscape

For module CON.7 *Information Security on Trips Abroad*, the following specific threats and vulnerabilities are of particular importance.

2.1. Eavesdropping and Spying on Information/Industrial Espionage

Espionage refers to attacks that aim to collect, evaluate, and process information about organisations, people, products, or other target objects. Particularly when travelling abroad, there are unknown sources of risk which an organisation's efforts at information security management cannot influence. As a general rule, foreign spaces and IT environments present many risks stemming from targeted eavesdropping on in-person discussions, communication lines, phone conversations and data transmissions. Particularly when abroad, this can be problematic and difficult to assess for travellers with regard to the legal options available in such cases.

Threats can affect both public spaces and rooms and circumstances in other organisations, as well as the offices of an organisation's own representatives abroad. Devices such as mobile phones can also be used to record or listen to conversations unnoticed. In addition, many IT systems come equipped with a microphone and camera, which can be accessed and then exploited.

Furthermore, there may be restrictions when entering or leaving certain countries which override or contradict the regulatory provisions of an employee's country of origin and the security requirements of the corresponding organisation. Access to data stored on notebooks and other portable IT systems can be requested, for example. This can allow confidential and personal data to be viewed and even copied and saved to some extent. Since this information may include things like strategy papers or strictly confidential drafts from an organisation, potential misuse must always be anticipated in the event of inspection (industrial espionage).

When travelling abroad, there are risks beyond information being intercepted in a technically complex manner. Sensitive data can often simply be spied on using optical, acoustic, or electronic methods since the standards one is used to with regard to information security regulations can not be expected in many cases. Among other factors, this relates to the general security level in a country and the local circumstances that a traveller cannot avoid.

2.2. Disclosure and Misuse of Sensitive Information (Electronic and Physical)

When information is exchanged, sensitive information can be unintentionally transmitted alongside what was intended. This can happen when information is sent electronically, during a telephone call, or when storage media are handed over in person. When travelling abroad, the secure exchange of information is sometimes made even more difficult by surrounding circumstances that are technically insecure. In addition, business travellers may leave

confidential documents in both physical and electronic form lying visible in public places or in hotel rooms due to carelessness.

Communicating with unknown IT systems and networks always poses a potential threat to a traveller's own end devices. This can allow confidential information to be copied, for example.

Meanwhile, foreign storage media can also contain malware. This carries the risk that important data could be stolen, manipulated, encrypted, or erased. At the same time, the integrity and availability of IT systems may also be impaired. This is exacerbated by the fact that data exchanges abroad often occur via insecure media. However, employees are not always aware of this important aspect.

2.3. Use of False Identities

Communication while travelling involves the increased risk that attackers may try to fake an identity (both in person and electronically) or assume an authorised identity, such as through disguises, spoofing methods, hijacking, or man-in-the-middle attacks. Users can be deceived about their communication partner’s identity to the point that they disclose sensitive information. Attackers can obtain a false digital identity by spying on a user ID and password, manipulating the sender field of a message, or manipulating an online address, for example.

Employees do not always know foreign business partners personally. If an employee trusts a stranger who introduces themselves as a particular business partner and has background knowledge that person would have, the employee may pass on valuable information. In reality, however, it could be a fraudster posing as the business partner.

Security requirements in terms of confidentiality and integrity can never be fully met in buildings that do not belong to an organisation, especially in foreign countries. There is always a residual risk that even equipment that would normally be classified as secure could be tampered with. This includes, for example, the use of caller ID on a telephone or the ID of a fax sender to fake an identity and obtain information.

2.4. Lack of Security Awareness and Carelessness in Handling Information

Although organisational regulations and technical security procedures for portable IT systems and mobile storage media exist in organisations, they are often not sufficiently observed and implemented by employees. Mobile storage media are frequently left unattended in meeting rooms or even on trains, for example.

In addition, gifts in the form of storage media (such as USB pen drives) can be accepted by employees and indiscriminately connected to their own laptops. This carries the risk that a laptop will be infected with malware, which could lead to sensitive data being stolen, manipulated, or encrypted.

On public transport or even during business meals, people can often be observed conducting open conversations about business-critical information. This can easily be overheard by outsiders and potentially used to seriously disadvantage the employee or their organisation.

2.5. Violation of Local Laws or Regulations

When travelling abroad, differing laws and regulations in the destination country should be given particular consideration, as they can be very different from the legal situation in one's country of origin. Relevant laws and regulations in destination countries (e.g. concerning data protection, information requirements, liability, or information access for third parties) are often unknown or incorrectly assessed by travellers. As a result, a multitude of laws can be violated not just abroad, but also at home—for example, if personal data concerning domestic customers is transmitted without protection over public networks while on a business trip abroad.

2.6. Coercion, Extortion, Hijacking, and Corruption

There are often other security risks resulting from political and social circumstances abroad. The security of information, and also of travellers themselves, can be endangered through coercion, extortion, or hijacking while travelling in foreign countries. For example, employees could be threatened with violence to force them to hand over sensitive data. In the process, they may be forced to circumvent or disregard security policies and safeguards. The focus here is often on high-level managers or employees who enjoy a particular position of trust.

Attackers predominantly aim to steal or manipulate sensitive information in order to interfere with business processes or to enrich themselves and others. Attackers are often driven by political, ideological, and financial goals.

In addition to the threat of violence, there is also the possibility of bribery or corruption: Travellers may be offered money or other benefits in order to persuade them to hand over confidential information to unauthorised persons or commit other security breaches.

In general, coercion, extortion, kidnapping, and corruption disrupt or undermine information security regulations.

2.7. Information from Unreliable Sources

While working abroad, travellers can be sent false or misleading information in order to deceive them. This deception may result in incorrect statements being incorporated into business-critical reports. Amongst other things, this may lead to business-relevant information being based on false data, calculations providing incorrect results, and wrong decisions being taken as a result.

2.8. Theft or Loss of Devices, Storage Media, and Documents

Particularly on trips abroad, mobile devices can easily be lost or stolen. The smaller and more popular these devices are, the higher the risk of theft. Alongside the purely material damage resulting from the immediate loss of a mobile device, the publication of sensitive data (e.g. e-mails, notes, or addresses from meetings) can lead to additional financial damage. This can also damage an organisation's reputation.

3. Requirements

The specific requirements of module CON.7 *Information Security on Trips Abroad* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	User, IT Operation Department, Human Resources Department

3.1. Basic Requirements

For module CON.7 *Information Security on Trips Abroad*, the following requirements MUST be implemented as a matter of priority:

CON.7.A1 Security Policy for Information Security on Trips Abroad

All aspects which are relevant to information security in connection with working abroad MUST be considered and regulated. The security safeguards taken in this regard MUST be documented in an information security policy for trips abroad. The security policy or an instruction leaflet detailing the security safeguards to be observed MUST be handed out to employees who work in different countries.

In addition, a security concept for handling portable IT systems on trips abroad MUST be established that describes all the security requirements and safeguards in sufficient detail. The implementation of the security concept MUST be checked at regular intervals.

CON.7.A2 Raising Employee Awareness of Information Security When Travelling Abroad (B)

Users MUST be made aware of and receive training in the responsible handling of information technology and portable IT systems on trips abroad. Users MUST be aware of the threats that can arise from inappropriate handling of information, improper destruction of data and storage media, or malware and insecure data exchanges. The limits of the security safeguards in use MUST also be demonstrated. Users MUST be empowered and encouraged to prevent loss or theft or to seek professional advice in case of inconsistencies. In addition, the legal requirements for individual destinations in relation to travel security SHOULD be emphasised to employees. The Chief Information Security Officer MUST keep abreast of legal requirements in the context of information security (e.g. data protection, IT security law) and raise employee awareness in this regard.

CON.7.A3 Identification of Country-Specific Regulations, Travel Conditions and Environmental Conditions [Human Resource Department]

Prior to travel, the applicable regulations of each country MUST be reviewed by the respective organisation's information security managers or Human Resources Department and communicated to the relevant staff.

The organisation MUST establish, implement, and communicate appropriate policies and safeguards that enable the adequate protection of internal data. Individual travel- and environmental conditions MUST be taken into account.

Before the beginning of a trip, employees MUST also familiarise themselves with the climatic conditions in the destination country and determine the protective safeguards they require for themselves (e.g. vaccinations) and the information technology they plan to take.

CON.7.A4 Use of Privacy Screens [User] (B)

Particularly when abroad, users MUST ensure that no sensitive information can be spied on when they are working on mobile devices. To this end, appropriate privacy screens which cover the entire screen of each device and thwart information espionage MUST be used.

CON.7.A5 Use of Screen/Code Locking [User] (B)

A screen or code lock that prevents third parties from accessing mobile device data MUST be used. The user MUST employ an appropriate code or a secure device password for this purpose. Screen locking MUST automatically activate after a short period of inactivity.

CON.7.A6 Prompt Reporting of a Loss [User]

Employees MUST report any loss or theft of information, IT systems, or storage media to their organisation immediately. To this end, there MUST be clear reporting channels and contact persons within the organisation. The organisation MUST evaluate the possible impacts of the loss and take appropriate countermeasures.

CON.7.A7 Secure Remote Access to an Organisation's Network [IT Operation Department, User] (B)

In order to allow secure remote access to an organisation’s network for employees on trips abroad, the IT Operation Department MUST set up secure remote access (e.g. via a virtual private network, VPN) in advance. VPN access MUST be cryptographically secured. In addition, users MUST have sufficiently secure access data to successfully authenticate themselves on their end devices and their organisation's network. Employees MUST use secure remote access for all communications which are possible in this context. Care MUST be taken to ensure that only authorised persons can access IT systems which have remote access. To the greatest extent possible, mobile IT systems MUST be protected against direct access to the Internet by a restrictively configured personal firewall.

CON.7.A8 Secure Use of Public WLANs [User] (B)

Whether or not mobile IT systems are allowed direct access to the Internet MUST always be specified.

To access an organisation's network via publicly accessible WLANs, the user MUST use a VPN or comparable security mechanisms (see CON.7.A7 *Secure Remote Access* and NET.2.2 *WLAN Usage*). Security safeguards MUST also be taken when using WLAN hotspots (see also INF.9 *Mobile Workplace*).

CON.7.A9 Secure Handling of Mobile Storage Media [User] (B)

If mobile storage media are used, users MUST ensure in advance that they are not infected with malware. Before passing on mobile storage media, users MUST also ensure that they do not contain any sensitive information. If a storage medium is no longer used, it MUST be securely deleted, especially if it is to be passed on to other persons. To this end, the storage medium MUST be overwritten using a sufficiently secure method specified by the organisation in question.

CON.7.A10 Encryption of Portable IT Systems and Storage Media [User, IT Operation Department] (B)

To ensure that sensitive information cannot be accessed by unauthorised third parties, employees MUST ensure that all sensitive information is secured in accordance with the applicable internal policies before travelling. Mobile storage media and clients SHOULD be encrypted by the user or the IT Operation Department prior to travel. The cryptographic keys MUST be stored separately from encrypted devices. When encrypting data, the legal regulations of the destination country SHOULD be observed. In particular, country-specific laws on the issuance of passwords and the decryption of data SHOULD be considered.

CON.7.A12 Secure Destruction of Sensitive Materials and Documents [User] (B)

Organisations MUST present employees with options for appropriately and securely destroying sensitive documents. Users MUST comply with these regulations. They MUST NOT dispose of their organisation's internal records until they have been securely destroyed. If this is not possible locally or it involves dealing with documents or storage media containing particularly sensitive information, these items MUST be kept until the employee’s return from business travel and then appropriately destroyed.

3.2. Standard Requirements

For module CON.7 *Information Security on Trips Abroad*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

CON.7.A11 Use of Anti-Theft Devices [User] (S)

To protect mobile IT systems outside their organisation, users SHOULD use anti-theft devices, particularly in places where there is increased public traffic or high user fluctuation. The procurement and usage criteria for anti-theft devices SHOULD be adapted to each organisation’s processes and documented accordingly.

CON.7.A13 Transporting Necessary Data and Storage Media [User] (S)

Before beginning a trip, employees SHOULD check what data is not absolutely required on the IT systems they are taking with them (notebook, tablet, smartphone, etc). Any data that does not need to be left on a device SHOULD be securely deleted. However, if it is necessary to take

sensitive data on trips, this SHOULD only be done in encrypted form. In addition, the mobile storage media that may be taken on trips abroad and the corresponding security measures that should be taken into account (e.g. protection against malware, encryption of business-critical data, storage of mobile storage media) SHOULD be established in writing. Employees SHOULD know and follow these regulations before beginning a trip.

These security-related requirements SHOULD vary depending on the protection needs of the data to be handled abroad and the data to be accessed.

CON.7.A14 Cryptographically Secured E-Mail Communication [User, IT Operation Department] (S)

Employees SHOULD secure e-mail-based communications cryptographically in accordance with their organisation's internal provisions. E-mails SHOULD also be suitably encrypted or digitally signed. Public IT systems, such as those in hotels or Internet cafés, SHOULD not be used for accessing e-mails.

For communication via e-mail services (e.g. webmail), organisations SHOULD clarify in advance what security mechanisms are implemented by the respective providers and whether they satisfy its internal security requirements. These include, for example, secure server operation, the establishment of an encrypted connection, and the duration of data storage.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module CON.7 *Information Security on Trips Abroad* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

CON.7.A15 Emission Security for Portable IT Systems (H)

Before the beginning of a trip, the protection needs of the particular information to be handled on the employee's mobile storage media or client while abroad SHOULD be determined. The corresponding organisation SHOULD check whether the information to be taken has a special need for protection and use low-radiation or radiation-proof storage media and clients accordingly.

CON.7.A16 Protecting Integrity Using Checksums or Digital Signatures [User] (H)

Users SHOULD use checksums to verify the integrity of data during transmission and backups. To achieve an even better level of protection in safeguarding the integrity of sensitive information, digital signatures SHOULD be used.

CON.7.A17 Use of Dedicated Travel Hardware [IT Operation Department] (H)

To ensure that an organisation's sensitive information cannot be accessed by third parties while travelling abroad, the IT Operation Department SHOULD provide employees with pre-configured travel hardware. On the basis of the minimum principle, this travel hardware SHOULD only provide the functions and information which are absolutely necessary to conduct business activities.

CON.7.A18 Restricted Authorisations on Trips Abroad [IT Operation Department] (H)

Before the beginning of a trip, the authorisations the employee in question truly needs in order to conduct their day-to-day business while abroad SHOULD be checked. To this end, the option to have the IT Operation Department withdraw the employee's access rights for the duration of the trip in order to prevent unauthorised access to information within the organisation SHOULD be considered.

4. Additional Information

4.1. Useful resources

The “Initiative Wirtschaftsschutz” information portal provides further information on security on business trips on its website (https://www.wirtschaftsschutz.info).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module CON.7 *Information Security on Trips Abroad*.

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.29 Violation of Laws or Regulations

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.35 Coercion, Blackmail or Corruption

G 0.36 Identity Theft

G 0.42 Social Engineering

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

CON.8 Software Development

1. Description

1.1. Introduction

Many organisations face challenges they cannot adequately solve with ready-to-use software products. They need software solutions that are adapted to their individual requirements. Examples include highly specific software solutions for industry specialists (such as for controlling production plants) or IT applications that are adapted to an organisation's business processes (such as content management or identity management systems). That said, legacy systems that are no longer maintained by the original manufacturer can also be custom-developed for such purposes.

This individual software can be developed by an organisation itself or a third party. Software development plays a central role in this process when program code is developed or adapted to meet an organisation's requirements. It is essential that information security be taken into account throughout the software development process and not just at a later stage. This is the only way to guarantee the long-term information security of the resulting software solutions.

Software can be developed within the framework of traditional, self-contained projects or as a continuous activity without a fixed end point. In both cases, project management tools are often used in practice to coordinate and control software development. For this reason, the term "project" is used more frequently in this module and no distinction is made between project-based and continuous development, as the associated procedures and tools are similar.

1.2. Objective

This module deals with all the relevant security aspects that organisations must consider when developing software. It covers how an organisation can prepare and execute software development while identifying corresponding hazards and formulating requirements.

1.3. Scoping and Modelling

Module CON.8 *Software Development* must be applied once to each development project in the information domain at hand.

Software is often developed in a client-contractor relationship. This is reflected in two modules of IT-Grundschutz: APP.7 *Development of Individual Software,* which deals with the client side, and CON.8 *Software Development,* which covers the contractor side. The present module therefore covers the requirements to be met by contractors. The requirements relevant to software development (functional and non-functional requirements, including for secure procedures and security profiles) are dealt with from the client perspective within the framework of module APP.7 *Development of Individual Software*.

The present module does not provide complete instructions or general procedures for software development; instead, it focuses on the relevant aspects of information security in connection with software development. The module also does not cover aspects of patch and change management. For these subjects, please refer to module OPS.1.1.3 *Patch and Change Management*.

The acceptance of software that is commissioned or developed in-house, as well as the tests associated with this process, are covered in module OPS.1.1.6 *Software Tests and Approvals*. Further aspects of testing in the context of software development are dealt with in this module, CON.8 *Software Development*.

ORP.5 *Compliance Management* must also be considered, as it describes how legal and organisation-internal requirements (and those pertaining to the customer) should be taken into account.

If a software development process includes cryptographic aspects, the relevant requirements from module CON.1 *Crypto Concept* must be considered.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module CON.8 *Software Development*, the following specific threats and vulnerabilities are of particular importance.

2.1. Selection of an Unsuitable Process Model

Process models make it possible to structure and plan software development by specifying certain steps in a particular order. If an unsuitable process model is selected for software development, the development process and the associated project can be significantly disrupted. Depending on the characteristics of the chosen model and the extent of the development project at hand, important aspects could be neglected or irrelevant aspects over-emphasised. Both issues increase the project management workload and hinder productive work.

Meanwhile, the decision to forgo a process model entirely increases the risk that relevant aspects, especially those relating to information security, will not be considered appropriately during software development. If relevant security functions are then not implemented or tested at all, this may result in developed software that does not meet the security requirements at hand.

2.2. Selection of an Unsuitable Development Environment

Urgent functions could be overlooked or implemented inadequately if an unsuitable development environment is selected or each employee selects their own. Furthermore, an unsuitable environment may present errors or weaknesses that can significantly disrupt software development.

If no particular development environment is specified and selected, various developers may work on the software using different tools of their own choosing, which could result in compatibility problems. Different compilers could cause compatibility issues, for instance.

2.3. Inadequate Quality Assurance in the Development Process

Inadequate quality assurance during software development can delay a development project or even cause it to fail altogether. Inadequate checks on the secure implementation of software developed in-house can lead to vulnerabilities when it is deployed.

If quality assurance is not made an integral part of the development process, errors and manipulations in the design or implementation of software may remain undetected. Particular attention in this regard should be paid not only to components developed in-house, but to external contributions from third parties and transferred components, as well.

2.4. Inadequate Documentation

Non-existent or insufficient software documentation in the conception or development phase can lead to delays in diagnosing and remedying possible errors (if this is possible at all). If development is inadequately documented, it also increases the work involved in updating, adapting, or expanding the respective software later on.

If the administrator or user documentation is inadequate, the software could be managed or operated incorrectly in a productive environment. This can, for example, disrupt IT operations, create errors in work results, or delay workflows.

2.5. Inadequately Secured Use of Development Environments

Inadequate security in a development environment can allow for manipulation of the software being produced. Such manipulations can then be difficult to detect afterwards.

If it is not known which users can and could access the development environment at a given point in time, the software produced can be manipulated anonymously. If manipulations in software are discovered, it may then be impossible to trace the user responsible under some circumstances.

If the source code of a given project is not subject to adequate version management, it will not be possible to track changes reliably or restore previous software versions that worked properly.

If source code is insufficiently protected against accidental or intentional changes, it may be partially or completely damaged and the work that has gone into it may be lost.

Failing to adequately protect source code and version management against data loss can lead to various threats, regardless of whether the data loss is triggered by a technical defect or human error (for example). It may not be possible to develop the software further because data is missing entirely, or it may only be possible to use an outdated (and possibly faulty) interim version at great expense.

2.6. Software Design Errors

The more extensive software becomes in terms of its range of functions, the more its program code often grows along with it. If program code is not structured using appropriate safeguards and not based on a suitable software architecture, it is usually very difficult to maintain. Vulnerabilities can then only be addressed with difficulty and obsolete program parts can only be replaced with a great deal of effort if, for example, the protection needs of the processed data change and thereby affect the security requirements of the software in question.

Software design errors not only complicate the maintenance of software; they can also lead to vulnerabilities and threats. If program code is not structured in a meaningful way and the software architecture is not documented comprehensibly, it is very difficult to identify conceptual errors in software tests. As a result, vulnerabilities can exist at almost any level of the software.

In practice, software design errors often have historical roots. For example, legacy systems may be used for tasks and environments for which they were not initially conceived. During the development of very old applications, aspects such as maintainability and modifiability may not have been considered as they would be in line with the current state of the art.

2.7. Inadequate Testing and Approval Procedures

If new software is not sufficiently tested and approved, potential errors cannot be detected. In addition to endangering the productive use and information security of the software itself, such errors may impact other applications and IT systems in the productive environment.

If security functions or basic security requirements are not tested, there is no guarantee that the developed software will meet the security requirements of the organisation using it. As a result, sensitive information could be disclosed, manipulated, or destroyed (e.g. by unauthorised third parties who can access the software due to inadequate authentication functions).

2.8. Software Testing with Production Data

If new software is tested with production data, unauthorised persons may be able to view sensitive personal data or other confidential information.

If the software is tested with original production data rather than copies (e.g. in the case of database systems), this can lead to even more extensive risks:

- In addition to confidentiality, software malfunctions during testing can lead to the integrity or availability of the production data being compromised.

- Unintentional changes in production data can also result from software being tested or operated incorrectly. These changes may not be identified quickly. Such errors can also affect other IT applications that access the same data sets.

These circumstances are very often exacerbated because the focus lies not on protecting the test data, but on whether the software behaves as intended during testing and meets the requirements defined.

3. Requirements

The specific requirements of module CON.8 *Software Development* are listed below. The Process Owner is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	Process Owner
Further responsibilities	Tester, Central Administration, IT Operation Department, Developer

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

CON.8.A2 Selection of a Process Model (B)

A suitable process model MUST be defined for software development. Based on the process model selected, a flow chart for software development MUST be created. In cases involving commissioned development, the client's security requirements for the process MUST be integrated into the process model.

The selected process model, including the specified security requirements, MUST be followed.

Staff SHOULD be trained in the methodology of the selected process model.

CON.8.A3 Selection of a Development Environment (B)

A list of required and optional selection criteria for a development environment MUST be provided by the Process Owner for software development. The development environment MUST be selected based on the criteria specified.

CON.8.A4 ELIMINATED (B)

This requirement has been eliminated.

CON.8.A5 Secure System Design (B)

The following basic rules of secure system design MUST be considered in the software to be developed:

- All input data MUST be checked and validated before further processing takes place.
- For client-server applications, the data MUST be validated on the server side.
- The software's default settings MUST be set to facilitate secure operation.
- In the event of errors in or failures of system components, sensitive information MUST NOT be disclosed.
- It MUST be possible to run the software with as few privileges as possible.
- Sensitive data MUST be transmitted and stored in encrypted form according to the specifications of the crypto concept at hand.
- Trusted mechanisms that meet the security requirements of the application in question MUST be used for user authentication and access.
- If passwords are stored for authentication, they MUST be stored using a secure hash procedure.
- Security-relevant events MUST be logged in such a way that they can be evaluated afterwards.
- Information that is not relevant for productive operation (e.g. comments with access data for the development environment) SHOULD be removed in delivered program code and configuration files.

The system design MUST be documented. It MUST be verified that the system design meets all the relevant security requirements.

CON.8.A6 Use of External Libraries from Trusted Sources (B)

If external libraries are used as part of the development and implementation process, they MUST be obtained from trusted sources. Before external libraries are used, their integrity MUST be ensured.

CON.8.A7 Conducting Software Tests During Development [Tester, Developer] (B)

Even before software is tested and approved in a corresponding process, software tests MUST be performed and the source code checked for errors during development. The Process Owner of the client or department that has commissioned the development SHOULD be involved.

The tests carried out during development MUST cover the functional and non-functional requirements of the software. The software tests MUST include negative tests, as well. In addition, all critical limits on input and data types MUST be checked.

Test data SHOULD be carefully selected and protected for this purpose. Furthermore, automatic static-code analysis SHOULD be performed.

The software MUST be tested in a test and development environment that is separate from the production environment. Furthermore, tests MUST be carried out to determine whether the system requirements are sufficiently sized for the intended software.

CON.8.A8 Provision of Patches, Updates, and Changes [Developer] (B)

It MUST be ensured that security-critical patches and updates for developed software are provided in a timely manner by the Developers. If security-critical updates are released for external libraries in use, the Developers MUST adapt their software accordingly and provide corresponding patches and updates.

The Developers MUST provide checksums or digital signatures for installation, update, and patch files.

CON.8.A9 ELIMINATED (B)

This requirement has been eliminated.

CON.8.A10 Source Code Version Management [Developer] (B)

Development project source code MUST be managed by an appropriate version management system. An organisation MUST regulate access to its version management system and define when changes made to source code by Developers are to be stored as a separate version in the system. It MUST be ensured that all changes to source code can be tracked and reversed by means of the version management system.

Version management MUST be included in the organisation's backup concept. Version management MUST NOT take place without data backups.

CON.8.A20 Checking External Components (B)

Unknown external components (or program libraries) whose security cannot be ensured by established and recognised peer reviews or comparable means MUST be checked for vulnerabilities. All external components MUST be checked for potential conflicts.

The integrity of external components MUST be verified by checksums or cryptographic certificates.

Furthermore, obsolete versions of external components SHOULD NOT be used in current development projects.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

CON.8.A1 Definition of Roles and Responsibilities [Central Administration] (S)

One person SHOULD be assigned responsibility for the software development process. In addition, the roles and responsibilities for all software development activities SHOULD be defined. The roles SHOULD cover the following topics:

- Compliance management and change management
- Software design and architecture
- Information security in software development
- Software implementation in the areas relevant to the development project at hand

- Software testing

One person SHOULD be assigned responsibility for information security for each development project.

CON.8.A11 Drawing Up a Policy for Software Development (S)

A software development policy SHOULD be created and kept up to date. In addition to naming conventions, the policy SHOULD contain specifications for elements that may or may not be used. The relevant requirements from this module SHOULD be included in the policy. The policy SHOULD be binding for Developers.

CON.8.A12 Detailed Documentation (S)

Sufficient project, function, and interface documentation SHOULD be created and kept up to date. Operational documentation SHOULD include specific security instructions for administrators on the installation, configuration, and use of the product in question.

Software development SHOULD be documented in a manner that will enable a technical expert to understand and develop the corresponding program code further. The documentation SHOULD also include the software architecture and threat modelling.

Aspects related to documentation SHOULD be considered in the process models used for software development.

CON.8.A13 ELIMINATED (S)

This requirement has been eliminated.

CON.8.A14 Training Development Teams on Information Security (S)

Developers and other members of a development team SHOULD be trained on general information security aspects and the aspects specifically relevant to them, including:

- Requirements analysis
- Project management in general, as well as with regard to software development in particular
- Risk management and threat modelling in software development
- Quality management and quality assurance
- Models and methods of software development
- Software architecture
- Software testing
- Change management
- Information security, the security policies of the organisation in question, and security aspects in special areas

CON.8.A15 ELIMINATED (S)

This requirement has been eliminated.

CON.8.A16 Appropriate Control of Software Development (S)

Software development SHOULD follow a suitable control or project management model based on the selected process model. The control or project management model SHOULD be integrated into the software development policy in question. In this regard, the required personnel qualifications and the coverage of all relevant phases during the lifecycle of the software SHOULD be considered in particular. A suitable system of risk management SHOULD be established for the process model. Appropriate quality objectives SHOULD also be defined for each development project.

CON.8.A21 Threat Modelling (S)

Threat modelling SHOULD be undertaken during the design phase of software development. For this purpose, potential threats SHOULD be identified on the basis of the relevant security profile, the catalogue of requirements, and the planned operational environment or operational scenario. The threats SHOULD be assessed in terms of their probability and impact.

CON.8.A22 Secure Software Design (S)

Software design SHOULD take into account the applicable requirements catalogue, the security profile, and the results of threat modelling. As part of secure software design, a secure software architecture SHOULD be assembled as the basis for developing the source code of the application in question. Future standards and attack techniques SHOULD be taken into account as far as possible so that the software to be developed can also be easily maintained in the future.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

CON.8.A17 Selection of Trusted Development Tools (H)

Only tools with proven security properties SHOULD be used to develop software. Sufficient requirements SHOULD be imposed on hardware or software manufacturers with regard to the security of their tools.

CON.8.A18 Periodic Security Audits of the Development Environment (H)

Regular security audits SHOULD be performed on environments used for software development and testing.

CON.8.A19 Regular Integrity Audits of the Development Environment [IT Operation Department] (H)

The integrity of a development environment SHOULD be checked regularly with cryptographic mechanisms in line with the current state of the art. The deployed test program itself and its checksum files SHOULD be adequately protected against manipulation. A large

number of false positives SHOULD NOT be allowed to obscure important information that indicates a loss of integrity.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) sets requirements for software development in the following standards, among others:

- ISO/IEC 27001:2013, appendix A.14.2, “Security in Development and Support Processes”
- ISO/IEC 25000:2014, “Systems and Software Quality Requirements and Evaluation – Guide to SQuaRE” (a general overview of the SQuaRE series of standards)
- ISO/IEC 25001:2014, “Planning and Management”
- ISO/IEC 25010:2011 "System and Software Quality Models" (requirements and guidelines)

The Information Security Forum (ISF) sets out requirements for secure software development in "The Standard of Good Practice for Information Security" (section "SD System Development").

The National Institute of Standards and Technology provides requirements for secure system design in Special Publication 800-160, "Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems".

The Special Interest Group "Process Models for Operational Application Development” of the German Informatics Society provides an overview of current information on application development in its publications.

Further information on threat modelling can be found in the scientific article "Threat Modelling in Software Development". This article was published for the conference “Sicherheit 2010: Sicherheit, Schutz und Zuverlässigkeit” [Security 2010: Safety, Security, and Reliability] of the German Informatics Society.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security

objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module CON.8 *Software Development*.

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.40 Denial of Service

G 0.41 Sabotage

G 0.46 Loss of Integrity of Sensitive Information

CON.9 Information Exchange

1. Description

1.1. Introduction

Information is transmitted between senders and recipients through communication channels as various as personal conversations, telephone calls, letters, removable media, and data networks. Rules on the exchange of information ensure that confidential information is only passed on to authorised persons. Such rules are particularly necessary when information is transmitted via external data networks.

1.2. Objective

The objective of this module is to secure the exchange of information between various communication partners. This module can help establish a concept for secure information exchange.

1.3. Scoping and Modelling

Module CON.9 *Information Exchange* must be applied once to the entire information domain under consideration if information is to be exchanged with communication partners outside of the information domain.

The protection of network connections is dealt with in other modules of the IT-Grundschutz Compendium; see layer NET *Networks and Communication*. Requirements for removable media (see module SYS.4.5 *Removable Media*) and further processing in IT systems outside of an information domain are not considered in this module.

2. Threat Landscape

For module CON.9 *Information Exchange*, the following specific threats and vulnerabilities are of particular importance.

2.1. Delayed Availability of Information

The exchange of information can be disrupted, delayed, or interrupted.

If the technology used generates transmission errors, the transfer of information can be delayed, incomplete, or processed too slowly. Under certain circumstances, the exchange of information can come to a complete halt because interfaces or operating resources are not powerful enough or fail for some other reason.

Business processes can be significantly impaired if required deadlines for the delivery of information are not met. In extreme cases, contractually agreed deadlines can be violated if a data transmission fails due to technical outages or human error.

2.2. Unregulated Forwarding of information

Sensitive information can fall into the hands of unauthorised persons.

If a confidentiality agreement is not concluded before information is exchanged, for example, it will not be possible to control who receives and uses the information. The risk of data misuse also increases if a confidentiality agreement is formulated in an imprecise or incomplete way.

2.3. Sharing False or Internal Information

Sensitive information can be sent to unauthorised recipients.

Such sensitive information can inadvertently fall into the hands of unauthorised users if employees are not sufficiently made aware of this danger and trained accordingly. For example, storage media can be passed on that contain residual information such as insufficiently deleted legacy data. Other residual information includes undeleted internal comments that may be inadvertently transmitted to an external recipient in an electronic document (e.g. as an e-mail attachment). In other cases, confidential documents can be accidentally sent to the wrong recipient because there are no clear guidelines for handling them.

2.4. Unauthorised Copying and Modification of Information

Attackers can intercept or influence information and data without being noticed.

They can also steal information if it is not sufficiently protected. For example, an attacker can intercept storage media in the mail or read the contents of unprotected e-mails without being noticed. An attacker can also modify unprotected information while it is being transmitted in order to inject malware into files (for example).

2.5. Inadequate Application of Encryption Procedures

The protection of information during transmission using cryptographic procedures can be undermined by attackers.

An attacker who knows the cryptographic method in use can intercept encrypted data and the associated key if employees do not use the encryption method properly. Employees who have not been sufficiently trained could, for example, send the key and data on the same data medium. Keys that are too easy to guess are also often used.

3. Requirements

The specific requirements of module CON.9 *Information Exchange* are listed below. As a matter of principle, the Chief Information Security officer (CISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Process Owner, User, Central Administration

3.1. Basic Requirements

For module CON.9 *Information Exchange*, the following requirements MUST be met as a matter of priority:

CON.9.A1 Definition of Authorised Recipients [Central Administration, Users] (B)

The Central Administration MUST ensure that the disclosure of information does not violate any related legal frameworks.

The Central Administration MUST define which recipients are allowed to receive and share which information. The channels through which the respective information may be exchanged MUST be defined. Before exchanging information, each employee MUST ensure that the recipient has the necessary authorisations to receive and process the information.

CON.9.A2 Regulating the Exchange of Information [Central Administration, User] (B)

Before information is exchanged, the information owner MUST determine its level of sensitivity. The information owner MUST determine how to protect the information during transmission.

If sensitive information is being transmitted, the information owner MUST inform the recipient about its level of sensitivity. If the information is sensitive, the information owner MUST also inform the recipient that they may only use the information for the purpose for which it was transmitted.

CON.9.A3 Instruction of Personnel on Exchanges of Information [Process Owner] (B)

The Process Owner MUST inform all the relevant employees about the framework conditions for each information exchange. The Process Owner MUST ensure that the employees know what information they can pass on, as well as when, where, and how.

3.2. Standard Requirements

For module CON.9 *Information Exchange*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

CON.9.A4 Agreements on Exchanging Information with External Parties [Central Administration] (S)

If information is regularly exchanged with other organisations, the organisation in question SHOULD formally agree on a corresponding framework. This information exchange agreement SHOULD include information on the protection of all confidential information.

CON.9.A5 Removal of Residual Information Prior to Sharing [User] (S)

In addition to general training, an organisation SHOULD inform its users about the dangers of residual and additional information in documents and files. The users SHOULD be taught how to avoid residual and additional information in documents and files.

The organisation SHOULD instruct each user on how to exclude unwanted residual information from exchanges of information.

Users SHOULD check each file and document for undesired information before transferring files. Users SHOULD remove unwanted residual information from documents and files.

CON.9.A6 Compatibility Checks on Sender and Recipient Systems (S)

Before exchanging information, the compatibility of the sender and receiver IT systems and products SHOULD be checked.

CON.9.A7 Backup Copies of Transferred Data [User] (S)

Users SHOULD make a backup copy of transmitted information in case the information cannot be restored from other sources.

CON.9.A8 Encryption and Digital Signatures (S)

An organisation SHOULD check whether information can be cryptographically secured during an exchange. If information is to be cryptographically secured, sufficiently secure procedures SHOULD be used for this purpose.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module CON.9 *Information Exchange* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into

account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

CON.9.A9 Confidentiality Agreements [Central Administration, User] (H)

Before disclosing confidential information to external parties, the user SHOULD inform the Central Administration. The Central Administration SHOULD conclude a confidentiality agreement with the recipients in question. The confidentiality agreement SHOULD regulate how the information may be kept on the receiving side. The confidentiality agreement SHOULD specify who on the receiving side may have access to which transmitted information.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) describes requirements for the exchange of information in its standard *ISO/IEC 27001:2013*, section 13.2.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module CON.9 *Information Exchange*.

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.45 Data Loss

CON.10 Development of Web Applications

1. Description

1.1. Introduction

Web applications provide users with particular functions and dynamic (changing) content. For this purpose, web applications make documents and user interfaces available on a server (e.g. in the form of input masks) and deliver them on request to corresponding programs on clients such as web browsers. Web applications are usually developed on the basis of frameworks. Frameworks are reusable program templates for frequently recurring tasks. Frameworks are also available for security components.

Web applications must implement security mechanisms that ensure the protection of the information they process and prevent it from being misused. Some typical security components or mechanisms include authentication, authorisation, input validation, output encoding, session management, error handling, and logging.

Developers must be familiar with the relevant security mechanisms of their web applications. For this reason, the development process has a crucial influence on the security of software.

1.2. Objective

The aim of this module is to ensure the secure development of web applications and protect the information they process.

1.3. Scoping and Modelling

This module must be applied to any development project involving web applications in a given information domain.

It considers the specific hazards and requirements relevant to the development of web applications. Requirements for the secure use of web applications are not considered here. These can be found in module APP.3.1 *Web Applications*. General requirements for secure

software development are also not covered here. These are addressed in module CON.8 *Software Development*.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module CON.10 *Development of Web Applications*, the following specific threats and vulnerabilities are of particular importance.

2.1. Bypassing Authorisations in Web Applications

Attackers often try to access functions or data of web applications which are only available to a limited group of users. If authorisation is implemented improperly, in some circumstances an attacker could obtain the authorisations of another user with more comprehensive rights and thereby access protected areas and data. This can occur when an attacker deliberately manipulates their own input data, for example.

2.2. Insufficient Input Validation and Output Encoding

If a web application processes unchecked input data, protection mechanisms could be bypassed. This risk increases if the output data of the web application is transmitted at the same time directly to the user's web browser, to the application calling the web application, or to downstream IT systems without sufficient encoding. Such output data may contain malicious code that will be interpreted or executed on the target systems. For example, an attacker could enter JavaScript code as form data. This malicious code may then be unintentionally executed by another user's IT system.

2.3. Insufficient Error Handling by Web Applications

If errors occur during the operation of a web application that are not handled correctly, this can hinder both the operation of the application and the protection of its functions and data. For example, an error can result in the web application no longer running correctly and no longer being accessible to clients. In addition, tasks may not be completed fully, cached actions and data may be lost, and security mechanisms may fail.

2.4. Insufficient Logging of Security-Relevant Events

If security-relevant events are insufficiently logged by a web application, security incidents can be difficult to trace at a later date. This may make it impossible to ascertain the cause of a given incident. For example, configuration errors can be overlooked if corresponding error messages are not recorded in the log files. If logging is inadequate, vulnerabilities are also difficult or impossible to detect and rectify.

2.5. Disclosure of Security-Relevant Information Through Web Applications

Websites and data generated and delivered by a web application can contain information on related background systems such as IT components and versions of frameworks. This information can make it easier for an attacker to target the web application.

2.6. Misuse of a Web Application Due to Automated Use

If attackers use the functions of a web application in an automated way, they can perform numerous processes in a short time. Using a repeated login process, an attacker can, for example, attempt to determine valid combinations of user names and passwords (brute force) or generate lists of valid user names (enumeration) if the web application returns information about existing users. In addition, repeatedly calling up resource-intensive functions (e.g. complex database queries) can be misused for denial-of-service attacks at the application level.

2.7. Inadequate Session Management in Web Applications

Inadequate session management can allow an attacker without special access rights to determine the session ID of a user with extensive access rights. The attacker can then use this ID to access protected functions and resources of the web application, such as in the form of a session fixation attack. Here, the attacker first has the web application assign them a session ID with restricted user rights. This ID is then transmitted to a legitimate user with higher access rights (e.g. via a link in an e-mail). If the user with higher rights follows this link and authenticates themselves to the web application under the attacker's session ID, the attacker can then use the application with the full access rights of the legitimate user.

3. Requirements

The specific requirements of module CON.10 *Development of Web Applications* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	Developer
Further responsibilities	None

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For module CON.10 *Development of Web Applications*, the following requirements MUST be met as a matter of priority.

CON.10.A1 Authentication for Web Applications (B)

Developers MUST ensure that users securely and appropriately authenticate themselves to a web application before they can access protected functions or content. An appropriate authentication method MUST be selected. The selection process MUST be documented.

A central authentication component MUST be used. The central authentication component SHOULD be used with established standard components (e.g. from frameworks or program libraries). If a web application stores authentication data on a client, the user MUST be explicitly informed about the risks of this function and consent to it ("opt-in").

The web application MUST offer the option to set limits for failed login attempts. The web application MUST inform users immediately if their password has been reset.

CON.10.A2 Access Control for Web Applications (B)

An authorisation component MUST be used by Developers to ensure that users can only perform actions for which they are authorised. Every attempt to access protected content and functions MUST be checked before being allowed.

The authorisation component MUST consider all the resources and content administered by a web application. If the corresponding access control system is defective, access MUST be denied. Access control MUST also be in place for URL calls and object references.

CON.10.A3 Secure Session Management (B)

Developers MUST ensure that session IDs are protected appropriately. Session IDs MUST be generated randomly and with sufficient entropy. If the web application framework in use can generate secure session IDs, the Developers MUST use this feature. The security-relevant configuration options of the framework MUST be considered. If session IDs are transmitted and stored by the clients, they MUST be transmitted with sufficient protection.

A web application MUST provide users with the option to expressly terminate an active session. After a user has logged in, any existing session ID MUST be replaced by a new one. Sessions MUST have a maximum validity period (timeout). Inactive sessions MUST automatically expire after a specified period of time. After a session has become invalid, all the session data MUST be rendered invalid and deleted.

CON.10.A4 Controlled Integration of Content in Web Applications (B)

Developers MUST ensure that a web application only integrates the intended content for delivery to the user.

The destinations of the redirection function of a web application MUST be restricted sufficiently so that users are only redirected to trustworthy websites. If a user is leaving a trustworthy domain, the web application MUST inform them of this.

CON.10.A5 Upload Functions (B)

Developers MUST ensure that a user can only save files under the specified path. Developers MUST ensure that a user cannot influence the storage location for uploads. Developers MUST integrate functions into their web applications that allow operators of the applications to configure uploads.

CON.10.A6 Protection Against Unauthorised Automated Use of Web Applications (B)

Developers MUST implement security mechanisms that protect their web applications from automated access. When implementing the security mechanisms, Developers MUST consider how they affect the options available to authorised users.

CON.10.A7 Protection of Confidential Data (B)

Developers MUST ensure that confidential data is transferred from clients to servers using only the HTTP post method.

Developers MUST use directives in web applications to ensure that no sensitive data is cached on the client side. Developers MUST ensure that no confidential form data is displayed in plain text in forms. A web application SHOULD prevent confidential data from being stored unexpectedly by the web browser. All web application access data MUST be protected against unauthorised access on the server side with the help of cryptographic algorithms (salted hash). The files containing the source code of a web application MUST be protected against unauthorised retrieval.

CON.10.A8 Comprehensive Input Validation and Output Encoding (B)

Developers MUST treat all data passed to a web application as potentially dangerous and filter it appropriately. All input data, as well as data streams and secondary data (such as session IDs), MUST be validated on the server side.

The automatic handling of erroneous input SHOULD be minimised (through sanitising) to the greatest extent possible. If it is unavoidable, sanitising MUST be implemented securely.

Output data MUST be encoded so that malicious code is not interpreted or executed on the target system.

CON.10.A9 Protection Against SQL Injections (B)

If data is passed to a database management system (DBMS), Developers MUST use stored procedures or prepared SQL statements. If data is passed to a DBMS and neither stored procedures nor prepared SQL statements are supported by the operational environment, SQL queries MUST be secured separately.

CON.10.A10 Restrictive Disclosure of Security-Related Information (B)

Developers MUST ensure that webpages, responses, and error messages from web applications do not contain information that would provide an attacker with insights into how to bypass corresponding security mechanisms.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

CON.10.A11 Software Architecture of a Web Application (S)

Developers SHOULD document the software architecture of their web applications along with all their components and dependencies. The documentation SHOULD be updated and adapted during the development process. The documentation SHOULD be designed so that it can be used in the development phase and the decisions taken will be comprehensible. The documentation SHOULD identify all the components necessary for operation that are not part of the respective web application. The documentation SHOULD also describe which components implement which security mechanisms, how the web application is to be integrated into an existing infrastructure, and which cryptographic functions and procedures are used.

CON.10.A12 Verification of Essential Changes (S)

If important settings are to be changed with an application, the Developers SHOULD ensure that the changes are verified again by entering a password. If this is not possible, the web application SHOULD ensure that users authenticate themselves by other appropriate means. Users SHOULD be informed of changes via communication channels outside the web application.

CON.10.A13 Error Handling (S)

If errors occur during the runtime of a web application, the Developers SHOULD ensure that the application handles them in a way that enables it to remain in a consistent state.

The web application SHOULD log error messages. If an initiated action causes an error, the web application SHOULD cancel that action. If an error occurs, the web application SHOULD deny access to the resource or function being requested.

Previously reserved resources SHOULD be released within the framework of error handling. Errors SHOULD be handled by the web application itself whenever possible.

CON.10.A14 Secure HTTP Configuration of Web Applications (S)

To protect against clickjacking, cross-site scripting, and other attacks, Developers SHOULD set appropriate HTTP response headers. The following HTTP headers SHOULD be used at minimum: Content-Security-Policy, Strict-Transport-Security, Content-Type, X-Content-Type-Options, and Cache-Control. The HTTP headers used SHOULD be adapted to the web application at hand. The HTTP headers used SHOULD be as restrictive as possible.

Cookies SHOULD always be set with the attributes *secure*, *SameSite*, and *httponly*.

CON.10.A15 Prevention of Cross-Site Request Forgery (S)

Developers SHOULD equip web applications with the security mechanisms required to distinguish between users' intended page requests and unintentionally forwarded third-party commands. At minimum, whether a secret token is required in addition to the session ID for access to protected resources and functions SHOULD be checked.

CON.10.A16 Multi-Factor Authentication (S)

Developers SHOULD implement multi-factor authentication.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

CON.10.A17 Preventing Resources from Being Blocked (H)

As protection against denial-of-service (DoS) attacks, resource-intensive operations SHOULD be avoided. Where resource-intensive operations are necessary, a particular effort SHOULD be made to secure them. For web applications, potential overflows of log data SHOULD be monitored and prevented.

CON.10.A18 Cryptographic Protection of Confidential Data (H)

Developers SHOULD ensure that a web application's confidential data is protected by secure cryptographic algorithms.

4. Additional Information

4.1. Useful Resources

On its website, the Open Web Application Security Project provides guidance on securing web applications.

The Federal Office for Information Security (BSI) provides guidance on the use of cryptographic procedures in the document “Cryptographic Mechanisms: Recommendations and Key Lengths: BSI TR-02102”.

The Federal Office for Information Security (BSI) provides guidance on developing secure web applications in the document “Entwicklung sicherer Webanwendungen” [Development of Secure Web Applications].

The Federal Office for Information Security (BSI) provides companies with guidance on developing secure web applications in “Leitfaden zur Entwicklung sicherer Webanwendungen” [BSI Guide for the Development of Secure Web Applications].

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the

issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module CON.10 *Development of Web Applications*.

G 0.18 Poor Planning or Lack of Adaptation

G 0.28 Software Vulnerabilities or Errors

OPS.1.1.2 Proper IT Administration

1. Description

1.1. Introduction

The ongoing administration of IT systems and components is fundamental to IT operations. System administrators configure IT systems and applications, monitor operations, and take measures in response to maintain the functionality and capability of their IT landscapes. They also adapt IT systems to changed needs. In so doing, system administrators fulfil some tasks in the field of security. Besides ensuring that IT systems remain available, they implement security safeguards and monitor their effectiveness. To this end, they have comprehensive authorisations, which is why it is very important for the security of an information domain that system administration itself be protected against unauthorised access.

1.2. Objective

The objective of this module is to show how the security requirements of IT applications, systems, and networks can be met by means of proper IT administration.

By implementing this module, an organisation can ensure that the activities required to secure its information domain are performed properly and systematically in system administration. At the same time, the organisation can react to the special threats that inevitably result from working with administrative privileges and being able to access sensitive areas of the organisation.

1.3. Scoping and Modelling

Module OPS.1.1.2 *Proper IT Administration* must be applied once to the entire information domain under consideration.

This module covers the overarching requirements that the administration process itself must fulfil. For the remote administration of IT systems using external interfaces, as well as for remote maintenance performed by the respective manufacturers or suppliers on devices and components, module OPS.1.2.5 *Remote Maintenance* should also be used.

The other modules of the OPS.1.1 *Core IT Operation* layer describe aspects of IT operations that are also relevant alongside this module. They should thus also be considered and modelled as a complement to this module.

The proper administration of users and rights is of particular relevance to the security of an organisation. As a consequence, this subject is also addressed in a separate module (see ORP.4 *Identity and Access Management*).

The requirements described in this module must also be applied if administrative tasks are performed on IT systems, applications, or platforms by third parties. Particular requirements for such cases are also described in the modules OPS.2.1 *Outsourcing for Customers* and OPS.3.1 *Outsourcing for Service Providers*.

Module OPS.1.1.2 *Proper IT Administration* refers to normal operations. In exceptional situations, particularly in the event of a possible IT attack and compromised IT systems, deviating requirements must be observed that are described in the corresponding modules of DER.2 *Security Incident Management*.

Aspects of patch and change management are not covered in this module either; they can be found in module OPS.1.1.3 *Patch and Change Management*.

2. Threat Landscape

For module OPS.1.1.2 *Proper IT Administration*, the following specific threats and vulnerabilities are of particular importance:

2.1. Failures Caused by Unspecified Responsibilities

If an IT operation department has not clearly regulated administrative responsibilities in areas like planning, installation, documentation, or monitoring, it will not be possible to carry out security-relevant tasks from these areas systematically (or at all). This is also the case if the regulations are not known and understood by the employees involved. Some typical examples involve the unclear delimitation of responsibilities between IT and telecommunications technology, between office IT and production systems, or between application and platform operations.

2.2. Shortage of Personnel with Core Competencies

Even administrators may be unexpectedly absent for extended periods of time. If they do not have trained deputies, the continued orderly operation of the IT systems and applications they support will not be guaranteed. Administrators sometimes build up very extensive detailed knowledge about the IT systems and applications they oversee. This includes not only the products and solutions used, but special features of their operational environment and the specific configurations at hand. This knowledge enables administrators to quickly identify errors and implement requirements more easily. However, it often also means that complex IT systems and applications are administered by an individual person. If this person is absent, their knowledge is no longer available to the respective organisation.

2.3. Misuse of Administrative Authorisations

Administrative authorisations allow for comprehensive access to confidential information like documents, communications, and databases. Besides performing the tasks assigned to them, administrators could use these comprehensive authorisations for their own purposes (or for third parties). They might access personnel documents or colleagues' communication threads, for example. Furthermore, third parties could pressure administrators or use other incentives to enlist their help in accessing and misusing data or IT systems.

2.4. Inadequate Consideration of Administrative Tasks

The privileged system access granted to administrators is frequently the focus of attackers. If administrative tasks are not performed properly, it becomes much easier to attack the corresponding information domain. Negligence may cause errors in configuration, lead to specified protective safeguards not being implemented sufficiently (if at all), or result in failures to follow up on suspicious events. The reasons for this may include a lack of security awareness, high time pressure, or a lack of processes and approaches, for example. This may result in vulnerabilities that may be exploited by attackers.

2.5. Operational Disruptions

Administrative activities directly influence the operation of IT systems and applications. For example, active user sessions may be interrupted when IT systems are restarted, or authorised access may be prevented while firewall rules are being adapted. If such processes are performed without taking into account the possible effects on users or coordinating the processes with them, operations may be disrupted significantly.

2.6. Lack of Options for Investigating Incidents

Shortcomings regarding the documentation of IT operations or missing records may make it impossible to investigate or clear up security incidents. Since it is often not immediately apparent how an attack was carried out, how extensive it was, or how systems were manipulated, appropriate investigations are first required to answer such questions. To make this possible, however, the target state of IT systems prior to the security incident in question must be documented and verifiable. It must also be possible to distinguish between proper and unauthorised changes to IT systems on the basis of suitable records. If corresponding information is not available, incidents can only be investigated with some degree of difficulty, if doing so is feasible at all. In such cases, it is also not possible to provide any legally valid evidence against the attackers.

3. Requirements

The specific requirements of module OPS.1.1.2 *Proper IT Administration* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified

according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	Human Resources Department

3.1. Basic Requirements

For module OPS.1.1.2 *Proper IT Administration*, the following requirements MUST be met as a matter of priority:

OPS.1.1.2.A1 ELIMINATED (B)

This requirement has been eliminated.

OPS.1.1.2.A2 Deputising Rules and Contingency Planning (B)

It MUST be ensured that only appointed deputies can access the IT systems to be supported. Emergency users with administrative rights should be set up for emergencies.

OPS.1.1.2.A3 Controlled Hiring of IT Administrators (B)

If employees assume administrative tasks within an IT environment, they MUST be trained, particularly in terms of the IT architecture and the IT systems and applications for which they are responsible. Administrators MUST be made familiar with the security provisions that apply in their organisation and are relevant to their work.

OPS.1.1.2.A4 Termination of IT Administration Duties [Human Resources Department] (B)

If administrators are relieved of their tasks, all their assigned personal administration credentials MUST be withdrawn. The passwords still known to employees who are being relieved of duties MUST be checked and these passwords MUST be changed.

Furthermore, whether employees being relieved of their duties have been appointed as contact persons for third parties (e.g. in contracts or as an Admin-C entry for Internet domains) MUST be checked. If this is the case, new contact persons MUST be specified and the third parties advised. The users of the IT systems and applications concerned MUST be informed that the previous administrator has left.

OPS.1.1.2.A5 Verifying Administrative Tasks (B)

An organisation MUST be able to prove which administrator has carried out which administrative activities at any time. For this purpose, each administrator SHOULD have their own user ID. Administrator deputies SHOULD also receive their own user IDs.

Each login by an administrator ID MUST be logged.

OPS.1.1.2.A6 Protecting Administrative Tasks (B)

Administrators MUST authenticate themselves through appropriate procedures before performing actions with administrative privileges.

Actions and activities that do not require elevated privileges MUST NOT be performed with administrative privileges.

Organisations MUST ensure that only administrators have access to administrative interfaces and functions. In particular, organisations MUST ensure that only administrators can make security-relevant changes to IT systems and applications.

Administration MUST be performed using secure protocols. The option to set up a separate administration network SHOULD be considered.

3.2. Standard Requirements

For module OPS.1.1.2 *Proper IT Administration*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

OPS.1.1.2.A7 Regulation of IT Administration Tasks (S)

The competencies, tasks, and obligations of administrators SHOULD be defined in a binding manner in a work instruction or policy. The tasks allocated to different administrators SHOULD be distributed in such a way that overlapping responsibilities are avoided, but all the tasks to be performed are still assigned. These regulations SHOULD be updated at regular intervals. In particular, their specifications SHOULD prevent administrators from making unauthorised changes within the information domain in question, provided that the changes go beyond the tasks explicitly assigned to them and are not necessary to prevent a security incident or failure.

OPS.1.1.2.A8 Administration of Specialised Applications (S)

The basic requirements mentioned in this module SHOULD also be implemented consistently for employees with administrative tasks for individual specialised applications. The division of tasks between application and system administration SHOULD be clearly defined and documented in writing. Interfaces SHOULD be defined between the persons in charge of system administration and those in charge of specialised application administration.

If there is an administrative intervention in the operation of an application, this SHOULD be coordinated in advance with the department in question. The needs of the department SHOULD be taken into account.

OPS.1.1.2.A9 Sufficient Resources for the IT Operation Department (S)

Sufficient personnel and material resources SHOULD be provided in order to properly handle the administrative tasks at hand. This SHOULD take into account the fact that appropriate capacities must also be available for unforeseeable tasks.

Resource planning SHOULD be reviewed regularly and adapted to the current requirements.

OPS.1.1.2.A10 Further Education and Information (S)

Administrators SHOULD take part in training and further education measures. This SHOULD also consider technical developments that are not currently used, but may become important to a given organisation in the foreseeable future. Training activities SHOULD be supported by a training plan. This training plan SHOULD take into account the whole team in question so that all the necessary qualifications are covered by multiple members.

Administrators SHOULD regularly obtain information regarding the security of the applications, IT systems, services, and protocols they support, especially in connection with current threats and security safeguards.

OPS.1.1.2.A11 Documentation of IT Administration Tasks (S)

System changes SHOULD be documented in an appropriate and transparent form. This documentation SHOULD include:

- which changes have been performed
- when the changes were performed
- who performed the changes
- the basis and reasons for the changes

Security-relevant aspects SHOULD be explained and highlighted in a transparent way.

OPS.1.1.2.A12 Provisions for Maintenance and Repairs (S)

IT systems SHOULD be maintained at regular intervals. The security aspects to be observed during maintenance and repair work SHOULD be regulated. The persons responsible for the maintenance or repair of equipment SHOULD also be specified. The maintenance tasks carried out SHOULD be documented.

OPS.1.1.2.A13 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.1.2.A20 Administration and Commissioning of Devices (S)

There SHOULD be an overview of all the devices in use at a given organisation that could have an impact on information security. In addition to IT systems and ICS components, devices pertaining to the Internet of Things (IoT) SHOULD also be considered. Appropriate testing and approval procedures SHOULD be carried out before the devices are put into operation for the first time. The overview SHOULD be kept up to date and correspond with the documentation of administrative activities.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.1.2 *Proper IT Administration* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

OPS.1.1.2.A14 Security Vetting of Administrators [Human Resources Department] (H)

In situations involving increased protection needs, administrators SHOULD be subject to additional security vetting.

OPS.1.1.2.A15 Division of Administrative Activities (H)

Different administration roles SHOULD be created for partial tasks. When differentiating among tasks, the type of data involved and the system architecture in place SHOULD be taken into consideration.

OPS.1.1.2.A16 Access Restrictions for Administrative Access (H)

Access to administrative interfaces SHOULD be technically restricted with filtering and separation measures. Interfaces SHOULD not be accessible to persons outside the responsible administration teams. Administrative access to IT systems in other protection zones SHOULD only be established via a jump server in the respective administrator's current security zone. Access attempts from other systems or other security zones SHOULD be rejected.

OPS.1.1.2.A17 Dual Control in IT Administration (H)

For particularly security-critical IT systems, access to credentials with administrative authorisations SHOULD be implemented in a way that always requires two employees. In other words, one administrator SHOULD perform the administrative tasks at hand under the supervision of a second administrator.

OPS.1.1.2.A18 Consistent Logging of Administrative Activities (H)

Administrative activities SHOULD be logged. For particularly security-critical IT systems, all administrative access attempts SHOULD be logged consistently and completely. Executing administrators SHOULD not have authorisation to change or delete the recorded log files. The log files SHOULD be retained for an appropriate period of time.

OPS.1.1.2.A19 Consideration of High-Availability Requirements (H)

Administrators SHOULD analyse which of the IT systems and networks they support are subject to high-availability requirements. For these areas, they SHOULD make sure that the components and architectures used, as well as the related operating processes, are appropriate for fulfilling these requirements.

4. Additional Information

4.1. Useful Resources

In the ISO/IEC 27001:2013 standard, the International Organization for Standardization (ISO) provides specifications for proper IT administration, particularly in the SY System Management area.

The BSI has published the four-volume High Availability Compendium.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module OPS.1.1.2 *Proper IT Administration*.

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.35 Coercion, Blackmail or Corruption

G 0.37 Repudiation of Actions

G 0.42 Social Engineering

OPS.1.1.3 Patch and Change Management

1. Description

1.1. Introduction

Updating an organisation's information technology components in a proper and timely manner poses a major challenge. In practice, existing vulnerabilities or operational disruptions are often traced back to inadequate patches and changes (or a lack thereof). Neglecting the subject of patch and change management therefore quickly leads to potential points of attack.

In general, the task of patch and change management is to design all the changes made to applications, infrastructure, documentation, processes, and procedures so that they are manageable and controllable.

1.2. Objective

This module shows how to design functional patch management in an organisation and how the corresponding process can be controlled and optimised.

Beyond patch management, however, the module also includes some core aspects of change management that are relevant to information security. Change management refers to the task of planning and controlling changes.

1.3. Scoping and Modelling

Module OPS.1.1.3 *Patch and Change Management* must be applied to the entire information domain under consideration.

The descriptions in this module focus on IT operations, and in particular on patch management, which is used to update software. The individual modules of the SYS *IT Systems* and APP *Applications* layers contain more specific requirements related to patch and change management.

Rather than addressing the entire subject of change management, this module only deals with the core aspects that pertain to information security. In larger organisations, it makes sense to structure change management systematically. Standards such as the change management process of the IT Infrastructure Library (ITIL) can be used for this purpose. Change management such as this need not be limited to IT; it can also encompass business processes and specialised tasks.

Requirements for testing and releasing patches and software are also not dealt with in detail in this module. They can be found in OPS.1.1.6 *Software Tests and Approvals*.

2. Threat Landscape

For module OPS.1.1.3 *Patch and Change Management*, the following specific threats and vulnerabilities are of particular importance.

2.1. Poorly Defined Responsibilities

Poorly defined, overlapping, or unclear responsibilities can, for example, slow down the categorisation and prioritisation of change requests. This can delay the overall distribution of patches and changes. It can also have a serious effect on security if patches and changes are released rashly without performing a test run or considering all the (technical) aspects at hand.

In extreme cases, poorly defined responsibilities may adversely affect an entire organisation or large parts of it. Disruptions in operations have a negative effect on availability. If security-relevant patches are distributed late or not at all, confidentiality and integrity may be threatened.

2.2. Poor Communication in Change Management

If patch and change management is poorly accepted within an organisation or if the people involved communicate poorly, this can lead to processing delays and incorrect decisions related to change requests. This may reduce the organisation's security level and seriously impair its IT operations. In any case, poor communication results in inefficient change processes because they require an excessive amount of time and resources. This has adverse effects on an organisation's ability to react and may, in extreme cases, result in vulnerabilities or the inability to attain important business objectives.

2.3. Poor Consideration of Business Processes and Specialised Tasks

Inappropriate changes may, amongst other things, impair the smooth handling of business processes or specialised tasks, or even cause the IT systems involved to fail completely. Even when using the most comprehensive testing procedure, it cannot be ruled out that a change will turn out to be faulty during later production operations.

If, in the course of the change process, the impact, category, or priority of a submitted change request is assessed incorrectly in terms of the business processes or specialised tasks involved, the organisation in question may fall short of its desired security level. Such misjudgements

predominantly occur when there is a lack of coordination between the persons responsible for IT and the responsible specialised departments.

2.4. Insufficient resources for patch and change management

Effective patch and change management requires adequate resources in terms of personnel, time, and funding. If suitable employees are not available, for example, the required roles could be staffed with unqualified personnel. This can also prevent interfaces for specific information being created—for example, between IT and the corresponding contacts in specialised departments. In addition, it may be impossible to provide the required capacities for the infrastructure of test and distribution environments. While it is often possible to compensate for shortages of personnel, time, and finances during normal operations, these shortages become even more apparent under serious time pressure, such as when emergency patches are being installed.

2.5. Problems in Automating the Distribution of Patches and Changes

In many cases, patches and changes are not distributed manually, but centrally with software support. If such software is used, incorrect patches and changes can be distributed automatically throughout an entire information domain, which can result in major security problems. This can be particularly severe if software with vulnerabilities is installed simultaneously on many systems.

If errors only occur occasionally, they can often be remedied manually. However, problems can arise if IT systems are not available for an extended time. Employees in the field who only connect their IT systems to an organisation's LAN sporadically are one such example. If a corresponding tool is configured in such a way that updates are only distributed within a certain period of time and not all IT systems are available in that window, these systems will not be updated.

2.6. Poor Recovery Options in Patch and Change Management

If patches or changes are distributed without a recovery option or the recovery routines of the software used are not suitable and effective, it will not be possible to remedy incorrectly updated software in good time. This may result in the failure of important IT systems and significant consequential damage. Alongside the potential loss of data, this especially threatens the availability and integrity of the data of the IT systems affected.

2.7. Misjudging the Relevance of Patches and Changes

If changes are prioritised incorrectly, unimportant patches could be installed first, for example. Important patches could then be installed too late and allow vulnerabilities to remain open for longer. Patch and change management is often supported by software-based tools. These tools may also contain software errors and therefore provide insufficient or incorrect information on a change. If the change information provided by a tool of this kind is not verified and checked for plausibility, the actual implementation of changes may differ from an organisation's assumptions.

2.8. Manipulation of Data and Tools in Change Management

Patch and change management often takes place from a central location. Its exposed position means it is particularly threatened. Should attackers manage to take over the servers involved, they will be able to distribute manipulated software versions simultaneously to a large number of IT systems via this central location. Further points of attack are often created by the fact that these systems are operated by external partners (outsourcing). Maintenance access maybe also be available that allows attackers to access a central server for distributing changes.

3. Requirements

The specific requirements of module OPS.1.1.3 *Patch and Change Management* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner

3.1. Basic Requirements

For module OPS.1.1.3 *Patch and Change Management* the following requirements MUST be implemented as a matter of priority:

OPS.1.1.3.A1 Concept for Patch and Change Management [Process Owner] (B)

If IT components, software, or configuration data are changed, there MUST be specifications that also consider security aspects. These MUST be defined in a concept for patch and change management and followed accordingly. All patches and changes MUST be suitably planned, approved, and documented. Patches and changes SHOULD be suitably tested in advance (see also OPS.1.1.6 *Software Tests and Approvals* in this regard). If patches are installed and changes carried out, fallback solutions MUST be available. If there are major changes, the Chief Information Security Officer MUST also be involved. Overall, it MUST be ensured that the desired security level is maintained during and after the implementation of changes. In particular, the desired security settings SHOULD also be maintained.

OPS.1.1.3.A2 Definition of Responsibilities (B)

Persons in charge of patch and change management MUST be specified for all organisational areas. The defined responsibilities MUST also be reflected in an organisation's access control policy.

OPS.1.1.3.A3 Configuration of Auto-Update Mechanisms (B)

The handling of integrated auto-update mechanisms of the software used MUST be defined within a strategy for patch and change management. In particular, it MUST be specified how these mechanisms are to be safeguarded and appropriately configured. Moreover, the type of update mechanisms of new components SHOULD be checked.

OPS.1.1.3.A15 Regular Updating of IT Systems and Software (B)

IT systems and software SHOULD be updated regularly.

In principle, patches SHOULD be applied promptly after release. Based on the patch and change management concept at hand, patches must be assessed promptly after release and prioritised accordingly. Decisions MUST be taken as to whether patches should be applied. When a patch is applied, it SHOULD be checked whether it has been successfully applied on all relevant systems in a timely manner. If a patch is not applied, this decision and the reasons for it MUST be documented.

OPS.1.1.3.A16 Regular Search for Information on Patches and Vulnerabilities (B)

The IT Operation Department MUST ensure it is regularly informed about vulnerabilities which become known in the firmware, operating systems, applications, and services used. The identified vulnerabilities MUST be rectified as soon as possible.

As long as no appropriate patches are available, other appropriate safeguards to protect the systems affected MUST be implemented depending on the severity of the vulnerabilities and basic threats. If this is not possible, it SHOULD be ensured that the corresponding hardware, relevant operating systems, and applications and services are no longer used.

3.2. Standard Requirements

For module OPS.1.1.3 *Patch and Change Management*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

OPS.1.1.3.A4 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.1.3.A5 Handling Change Requests [Process Owner] (S)

All requests for changes SHOULD be recorded and documented. Change requests SHOULD be checked by the person responsible for patch and change management to ensure that the information security aspects have been sufficiently taken into account.

OPS.1.1.3.A6 Coordination of Change Requests (S)

The coordination process associated with a change SHOULD take into account all the relevant target groups and the impact on information security. The target groups affected by the change SHOULD be able to comment on the change in a verifiable manner. There SHOULD be a defined procedure to speed up the handling of important requests for changes.

OPS.1.1.3.A7 Integration of Change Management into Business Processes (S)

The change management process SHOULD be integrated into business processes or specialised tasks. In cases involving planned changes, the current situation of the affected business processes SHOULD be considered. All relevant departments SHOULD be informed of upcoming changes. There SHOULD also be an escalation level that includes members of the corresponding organisation's Top Management. In case of doubt, these members SHOULD decide on the priority and scheduling of a given hardware or software change.

OPS.1.1.3.A8 Secure Use of Tools for Patch and Change Management (S)

Requirements and framework conditions SHOULD be defined for selecting tools for patch and change management. Furthermore, a specific security policy SHOULD be drawn up for the tools used.

OPS.1.1.3.A9 Testing and Acceptance Procedures for New Hardware (S)

When new hardware is selected, it SHOULD be checked that the software used, and in particular the relevant operating systems, are compatible with the hardware and its driver software. New hardware SHOULD be tested before it is used. It SHOULD be tested exclusively in an isolated environment.

There SHOULD be an acceptance procedure and a declaration of release for IT systems. The person in charge SHOULD file the declaration of release in a suitable place in writing. If errors are detected during live operations despite the acceptance and release procedures, there SHOULD be a procedure for troubleshooting.

OPS.1.1.3.A10 Assuring the Integrity and Authenticity of Software Packages (S)

The authenticity and integrity of software packages SHOULD be ensured throughout the patch or change process. To this end, it SHOULD be checked whether checksums or digital signatures are available for the software packages used. If there are, these SHOULD be checked before a package is installed. Furthermore, it SHOULD be ensured that the programs required for checking are available.

As a matter of principle, software and updates SHOULD only be obtained from trustworthy sources.

OPS.1.1.3.A11 Continuous Documentation of Information Processing (S)

Changes SHOULD be documented in all phases, applications, and systems. Corresponding rules SHOULD be developed for this purpose.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.1.3 *Patch and Change Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

OPS.1.1.3.A12 Use of Tools in Change Management (H)

Before using a change management tool, it SHOULD be checked whether it can distribute changes appropriately in the information domain in question. It SHOULD also be possible to define break points for stopping the distribution of incorrect changes.

OPS.1.1.3.A13 Measuring the Success of Change Requests [Process Owner] (H)

The Process Owner for patch and change management SHOULD perform follow-up tests to verify that a given change has been successful. For this, the Process Owner SHOULD select suitable reference systems as quality assurance systems. The results of follow-up tests SHOULD be documented within the scope of the change process.

OPS.1.1.3.A14 Synchronisation Within Change Management (H)

In the change management process, appropriate mechanisms SHOULD ensure that devices that cannot be reached temporarily or for a longer period of time also receive patches and changes.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides specifications relevant to patch and change management in the ISO/IEC 27001:2013 standard (section 12.1.2, "Change Management").

The IT Infrastructure Library (ITIL) provides guidance on setting up a change management process.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module OPS.1.1.3 *Patch and Change Management*.

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.39 Malware

G 0.46 Loss of Integrity of Sensitive Information

OPS.1.1.4 Protection Against Malware

1. Description

1.1. Introduction

Malware refers to programs that perform harmful functions on an IT system, usually without the knowledge or consent of the user. These harmful functions can have a wide range of purposes, ranging from potential espionage and extortion (using ransomware) to the sabotage and destruction of information, or even devices.

In principle, malware can be implemented on all operating systems and IT systems. In addition to traditional IT systems such as clients and servers, this includes mobile devices such as smartphones. Today, network components like routers and industrial control systems—and even IoT devices such as networked cameras—are also frequently threatened by malware.

On classic IT systems, malware is distributed mainly via e-mail attachments, manipulated web pages (drive-by downloads), or storage media. Smartphones are usually infected via the installation of malicious apps, but drive-by downloads are also possible. Furthermore, open network interfaces, incorrect configurations, and software vulnerabilities are frequent points of entry on all IT systems.

This module uses the term “virus protection program”. Here, “viruses” are a synonym for all types of malware. A virus protection program therefore refers to a program for protecting against any type of malware.

1.2. Objective

This module describes the requirements that must be met and implemented to protect an organisation effectively against malware.

1.3. Scoping and Modelling

Module OPS.1.1.4 *Protection Against Malware* must be applied once to the entire information domain under consideration.

This module describes the general requirements for protection against malware. Specific requirements for protecting particular IT systems in an organisation against malware are included in the relevant modules, particularly in the SYS layer *IT Systems.* If identified malware results in a security incident, the requirements of module DER.2.1 *Security Incident Handling* should be considered. The requirements of module DER.2.3 *Clean-Up of Extensive Security Incidents* help in removing identified malware and re-establishing a cleaned state.

The virus protection programs used within the framework of this module should also be taken into account in patch and change management (OPS.1.1.3 *Patch and Change Management*). Furthermore, the topic of protection against malware should be taken into account in the context of the modules ORP.3 *Information Security Awareness and Training* and CON.3 *Backup Concept*.

2. Threat Landscape

For module OPS.1.1.4 *Protection Against Malware*, the following specific threats and vulnerabilities are of particular importance.

2.1. Software Vulnerabilities and Drive-By Downloads

If IT systems are not sufficiently protected against malware, software vulnerabilities can be exploited by attackers to execute malicious code. Among other situations, this can happen if patches are not applied promptly and the protective mechanisms of application programs (such as browsers) are not configured correctly. In the case of drive-by downloads, it may be enough to visit a website infected with malicious code, for example. A vulnerability in a browser or in an installed plug-in such as Java or Adobe Flash can then be exploited to infect the IT system in question and provide the attacker with comprehensive control, as well as access to the corresponding organisation's network. IT systems that are not updated regularly, such as many smartphones, are at particular risk in this regard.

2.2. Extortion through Ransomware

Ransomware is a widespread type of malware. It encrypts the data of an infected IT system and, in many cases, further data it manages to access (e.g. through network shares). In most cases, attackers use encryption methods that cannot be reversed without the corresponding key as a means of extorting large sums of money from their victims. If there is no effective protection against malware and no supplementary precautions (such as data backups) are taken, the availability of information can be considerably restricted, data can be lost, and massive financial and reputational damage can occur.

2.3. Targeted Attacks and Social Engineering

Organisations are often attacked by customised malware. In such cases, supervisors (for example) are tricked into opening harmful e-mail attachments through social engineering. Customised malware often cannot be detected immediately by virus protection programs. The human resources department of an organisation can also be the target—for example, if it is sent electronic job application documents that are infected with malware. If an attacker manages to infect an IT system using such methods, they may infiltrate other areas of the corresponding organisation and view, manipulate, or destroy information.

2.4. Botnets

Malware may recruit the IT systems of an organisation into botnets. Attackers, who often control thousands of systems in a botnet, can use them to send spam or start distributed denial-of-service (DDoS) attacks on third parties. Even though the affected organisation itself may not be damaged directly, this may have negative effects regarding the availability and integrity of its own services and IT systems, and may even result in legal problems. For example, if an organisation's e-mail server is blacklisted, it may no longer be possible to send and receive e-mails.

2.5. Infection of Production Systems and IoT Devices

In addition to classic IT systems, devices that are not obvious targets are increasingly being attacked by malware. For example, an attacker may infect a surveillance camera accessible via the Internet to spy on an organisation. However, even a networked light bulb or a coffee machine with app control may serve as points of entry into an organisation's network or as part of a botnet unless these devices are protected sufficiently against malware. Networked production systems or industrial controls can also be manipulated or even destroyed through malware, which may result in downtime and further risks to an organisation and its employees (e.g. due to fire).

3. Requirements

The specific requirements of module OPS.1.1.4 *Protection Against Malware* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	User

3.1. Basic Requirements

For module OPS.1.1.4 *Protection Against Malware*, the following requirements MUST be met as a matter of priority:

OPS.1.1.4.A1 Creating a Malware Protection Concept (B)

A concept that describes which IT systems must be protected against malware MUST be drawn up. It MUST include IoT devices and production systems. Furthermore, it MUST be specified how protection is to be implemented. If no reliable protection is possible, the identified IT systems SHOULD NOT be operated. The concept SHOULD be documented in a comprehensible manner and kept up to date.

OPS.1.1.4.A2 Using System-Specific Protection Mechanisms (B)

The protection mechanisms provided by the IT systems used, as well as by the operating systems and applications used on them, MUST be checked. Such mechanisms MUST be used unless there is at least an equal substitute or good reasons against their use. If they are not used, this MUST be explained and documented.

OPS.1.1.4.A3 Selection of a Virus Protection Program (B)

A program MUST be selected and installed for the specific purpose of virus protection depending on the operating system used, the other protection mechanisms present, and the availability of suitable virus protection programs. A suitable virus protection program MUST be selected and installed for gateways and IT systems used for data exchange.

The products used MUST be designed for enterprise environments and include services and support that are tailored to the needs of the organisation in question. Products for purely home-based users or products without manufacturer support MUST NOT be used for professional production operations.

Cloud services designed to improve the detection performance of virus protection programs SHOULD be used. If the cloud functions of such products are used, it MUST be ensured that there are no conflicts regarding data or confidentiality protection. In addition to real-time and on-demand scans, it MUST also be possible to scan compromised and encrypted data for malware with the solution chosen.

OPS.1.1.4.A4 ELIMINATED (B)

This requirement has been eliminated.

OPS.1.1.4.A5 Operation and Configuration of Virus Protection Programs (B)

Virus protection programs MUST be configured appropriately for their operational environment. The focus SHOULD be on detection performance unless data protection or performance reasons influence this in individual cases. If the security-relevant functions of a virus protection program are not used, this SHOULD be explained and documented. In the case of protection programs that are specially optimised for desktop virtualisation, it SHOULD be transparently documented whether certain detection procedures have been omitted in

favour of performance. Care MUST be taken to ensure that users are not able to make any security-related changes to the settings of anti-virus programs.

OPS.1.1.4.A6 Regular Updating of Virus Protection Programs and Signatures (B)

The scan engines and malware signatures of virus protection programs MUST be updated regularly and promptly on the corresponding IT systems.

OPS.1.1.4.A7 User Awareness and Obligations [User] (B)

Users MUST be informed regularly of the threats posed by malware. They MUST comply with the basic codes of conduct at hand to reduce the risk of malware infection. Files, e-mails, websites, and other content from untrusted sources SHOULD NOT be opened. Users MUST be aware of the appropriate persons to contact in the event of a suspected malware infection. Users MUST inform their designated contacts if they suspect an infection involving a malicious program.

3.2. Standard Requirements

For module OPS.1.1.4 *Protection Against Malware*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

OPS.1.1.4.A8 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.1.4.A9 Reporting Malware Infections [User] (S)

The virus protection program used SHOULD block and report malware infections automatically. These automatic reports SHOULD be sent to a central location. The employees responsible SHOULD then decide how to proceed based on the current situation. The procedure to be followed in case of reports and alarms from virus protection programs SHOULD be planned, documented, and tested. In particular, the actions to be taken in case of a confirmed infection SHOULD be specified.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.1.4 *Protection Against Malware* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

OPS.1.1.4.A10 Using Special Analysis Environments (H)

Automated analyses in a special test environment (based on sandboxes, or separate virtual or physical systems) SHOULD also be used for assessing suspicious data.

OPS.1.1.4.A11 Using Several Scan Engines (H)

To improve detection performance, virus protection programs with several alternative scan engines SHOULD be used for IT systems that require special protection (e.g. gateways and IT systems for data exchange).

OPS.1.1.4.A12 Using Storage Media Locks (H)

Before connecting storage media from third parties to the IT systems of an organisation, the media SHOULD be checked in a storage media lock.

OPS.1.1.4.A13 Handling Untrusted Files (H)

If it is necessary to open untrusted files, this SHOULD only be done on an isolated IT system. In this system, the corresponding files SHOULD be converted into a secure format or printed (for example) if doing so will reduce the risk of a malware infection.

OPS.1.1.4.A14 Selecting and Using Cyber Security Products to Thwart Targeted Attacks (H)

The use and added value of products and services that offer an extended scope of protection compared to conventional anti-virus programs SHOULD be examined. Security products like these SHOULD be used against targeted attacks, such as when running files in special analysis environments, hardening clients, or encapsulating processes. Before a decision is taken to purchase a particular security product, the effectiveness of its protection and its compatibility with the IT environment of the organisation in question SHOULD be tested.

OPS.1.1.4.A15 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for protection against malware in the standard ISO/IEC 27001:2013, in particular in annex A, A.12.2 (“Protection from Malware”).

The Information Security Forum (ISF) provides guidelines for protection from malware in “The Standard of Good Practice for Information Security”, in particular in area TS1 ("Security Solutions").

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are

covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module OPS.1.1.4 *Protection Against Malware*.

G 0.14 Interception of Information / Espionage

G 0.19 Disclosure of Sensitive Information

G 0.23 Unauthorised Access to IT Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.39 Malware

G 0.42 Social Engineering

G 0.46 Loss of Integrity of Sensitive Information

OPS.1.1.5 Logging

1. Description

1.1. Introduction

To ensure reliable IT operations, IT systems and applications should automatically log all (or at least some specific) events that are relevant to operations and security and make them available for analysis. Logging is used in many organisations as a means of promptly identifying hardware and software problems and resource bottlenecks. However, security problems and attacks on network services can also be traced on the basis of log data. Through forensic examination, evidence can be secured from such data after an attack on IT systems or applications has come to light.

In each information domain, log data is locally generated by a multitude of IT systems and applications. To get a complete overview of a given information domain, the event logs generated by various IT systems and applications can be sent to a dedicated logging infrastructure for central storage. Only then can the log data be selected, filtered, and analysed systematically in one central location.

1.2. Objective

The aim of this module is to ensure the secure collection of all relevant data so that it can be stored and provided in a suitable form for evaluation. This in turn facilitates the logging of as many security-relevant events as possible.

1.3. Scoping and Modelling

OPS.1.1.5 *Logging* must be applied once to the entire information domain at hand.

This module only considers overarching aspects that are required for appropriate logging. Logging for specific IT systems or applications is not dealt with here; it is described in the relevant modules of the IT-Grundschutz Compendium.

In many operating systems or applications, logging functions are already present or can be integrated through additional products. To safeguard these functions and stored log data, the underlying operating systems must be protected. However, this is not covered in this module.

Operating-system-specific modules such as SYS.1.2.2 *Windows Server 2012* must be implemented.

Before implementing logging of security-relevant events, it is important that the related responsibilities and competencies be clearly defined and assigned. Particular attention should be paid to the principle of separation of duties. This topic is also not part of this module; it is covered in module ORP.1 *Organisation*.

In addition, this module must be distinguished from the detection of security-relevant events (see DER.1 *Detecting Security-Relevant Events*) and responses to security incidents (DER.2.1 *Security Incident Handling*). At most, these aspects are only addressed in passing in the present module.

The evaluation of log data and the secure, unchangeable, and reproducible long-term storage of such information is also described elsewhere (see DER.1 *Detecting Security-Relevant Events* or OPS.1.2.2 *Archiving*).

Finally, specifications on how to handle personal data are described in module CON.2 *Data Protection*.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module OPS.1.1.5 *Logging*, the following specific threats and vulnerabilities are of particular importance.

2.1. Insufficient Logging

Within an information domain, there are often IT systems and applications with default settings in which logging has not been enabled. Sometimes, individual IT systems or applications are not able to perform logging at all. In both cases, important information may be lost and it may be impossible to detect attacks in time. This is also possible if logging is used for individual IT systems or applications, but the log data is not collected in a central location. In information domains without centralised logging, it is difficult to ensure that the relevant logged information from all IT systems and applications will be preserved and analysed.

Furthermore, log data must contain meaningful information. The events to be logged depend, among other things, on the protection needs of the corresponding IT systems or applications. If this is disregarded—for example, by only using the default settings of IT systems and applications for logging—it may result in particularly relevant security events not being logged. Attacks may then go undetected.

2.2. Incorrect Selection of Relevant Log Data

Log data often provides important information that aids in detecting security incidents. However, filtering out relevant messages from the large amount of different log events presents a particular challenge. This is because numerous log events are only informative in

nature and divert attention from messages that are actually important. If too many log events are selected, analysing all their information will be difficult and require a great deal of time.

Furthermore, log events can be discarded or overwritten if the RAM or hard drive capacity of the IT system or logging infrastructure in question is insufficient. If this results in too few relevant log events being recorded, security-critical incidents may remain undetected.

2.3. Lack of Proper Time Synchronisation During Logging

If the time is not synchronised on all the IT systems within an information domain, the log data they produce may not correlate, and attempting to correlate it may result in erroneous statements. This is due to the lack of a common basis for the different time stamps of events. It is thus harder to assess collected log data where there is no time synchronisation, particularly if the data is stored on a central log server. Furthermore, a lack of proper time synchronisation may make it impossible to use logs in securing evidence.

2.4. Poor Planning of Logging

If logging is not sufficiently planned, IT systems or applications may not be monitored and security-relevant events may not be recognised and appropriately dealt with as a result. In addition, it will be impossible to trace data protection infringements back to their causes.

2.5. Loss of Confidentiality and Integrity in Log Data

Some IT systems in an information domain may generate log data (such as user names, IP addresses, e-mail addresses, and computer names) that can be associated with specific persons. Such information can be copied, intercepted, and manipulated if it is not encrypted and securely stored. This may result in attackers accessing confidential information or manipulated log data being used to deliberately disguise security incidents. Furthermore, if attackers obtain a large amount of log data, they may use it to ascertain the internal structure of the corresponding information domain and carry out more targeted attacks.

2.6. Incorrectly Configured Logging

If logging in IT systems is incorrectly configured, important information will be missed or not recorded properly. It is also possible that incorrect or excessive information will be logged. For example, personal data may be logged and stored without authorisation. The organisation in question could thus be in violation of related legal requirements.

Due to incorrectly configured logging, log data may also be available in inconsistent or proprietary formats. In such cases, logs may be difficult to assess and security incidents may remain undetected.

2.7. Failure of Log Data Sources

If IT systems in an information domain no longer provide the required log data, it will no longer be possible to appropriately detect security incidents. Errors in hardware and software and incorrectly administered IT systems can be the cause of such data source failures. In particular, if the failure of data sources is not detected, this may result in a false perception of

an organisation's security situation. Attackers may thus remain undetected for a long period of time and be able to intercept organisation-critical information or manipulate production systems (for example).

2.8. Insufficient Logging Infrastructure Capacity

Due to complex information domains and wide-ranging attack scenarios, the requirements logging systems need to meet are increasing because a very large amount of log data must be stored and processed. Moreover, it is customary to increase the intensity of logging when security incidents occur. However, if the corresponding logging infrastructure is not designed for this, the log data stored may be incomplete. As a result, security-relevant events will be assessed insufficiently (or not at all) and security incidents will remain undetected.

3. Requirements

The specific requirements of module OPS.1.1.5 *Logging* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

OPS.1.1.5.A1 Drawing Up a Security Policy for Logging [Process Owner] (B)

Based on an organisation's general security policy, a specific security policy SHOULD be drawn up for logging. This security policy MUST transparently describe requirements and specifications on how logging is to be planned, set up, and securely operated. The security policy MUST specify what is to be logged, as well as how and where. Here, the type and scope of logging SHOULD be based on the protection needs of the information in question.

The security policy MUST be drawn up by the CISO together with the Process Owners. It MUST be known to all employees in charge of logging and be integral to their work. If the security policy is changed or deviations from its requirements are allowed, this MUST be coordinated with the CISO and documented. The correct implementation of this specific security policy MUST be regularly reviewed. The results of these reviews MUST be documented.

OPS.1.1.5.A2 ELIMINATED (B)

This requirement has been eliminated.

OPS.1.1.5.A3 Configuring Logging at the System and Network Level (B)

All security-relevant events pertaining to IT systems and applications MUST be logged. If the IT systems and applications defined as relevant in a logging policy have a logging function, it MUST be used. When setting up logging, the manufacturer specifications for the relevant IT systems or applications MUST be considered.

Spot checks MUST be carried out at appropriate intervals to ensure that logging is still functioning correctly. The intervals of these checks MUST be defined in the logging policy at hand.

If events relevant to operations and security cannot be logged on an IT system, additional IT systems MUST be integrated for logging (e.g. for events at the network level).

OPS.1.1.5.A4 Time Synchronisation of IT Systems (B)

The system time of all IT systems and applications that generate logs MUST always be synchronous. It MUST be ensured that the date and time formats of log files are uniform.

OPS.1.1.5.A5 Complying with Legal Framework Conditions (B)

The regulations of the current laws on federal- and state-level data protection MUST be followed during logging (see CON.2 *Data Protection*).

Moreover, any personal rights and/or rights of co-determination of the Employee Representatives in question MUST be observed.

Compliance with any other relevant legal regulations MUST also be ensured.

Log data MUST be deleted in accordance with a specified process. Technical provisions MUST prevent log data being deleted or changed in an uncontrolled manner.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

OPS.1.1.5.A6 Basic Structure of a Centralised Logging Infrastructure (S)

All security-relevant logging data SHOULD be stored in a central location. To this end, a central logging infrastructure (read: a log server system) SHOULD be designed and placed in a network segment created for this purpose (see NET.1.1 *Network Architecture and Design*).

In addition to security-relevant events (see OPS.1.1.5.A3 *Configuring Logging at the System and Network Level*), a central logging infrastructure SHOULD log general operational events that indicate errors.

The logging infrastructure SHOULD have sufficient capacity. The possibility of scaling up this infrastructure to support extended logging SHOULD be considered. To this end, sufficient technical, financial, and personnel resources SHOULD be available.

OPS.1.1.5.A7 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.1.5.A8 Archiving of Log Data (S)

Log data SHOULD be archived. The relevant legal regulations SHOULD be taken into account in the process.

OPS.1.1.5.A9 Providing Log Data for Assessment (S)

Collected log data SHOULD be filtered, normalised, aggregated, and correlated. Log data processed in this way SHOULD be made available in a manner suitable for assessment.

Logging applications SHOULD have corresponding interfaces to programs capable of automatic data analysis.

It SHOULD be ensured that the evaluation of log data complies with the security requirements defined in the respective logging policy. Operational and internal agreements SHOULD also be taken into consideration when making log data available.

Log data SHOULD be stored unchanged in its original format.

OPS.1.1.5.A10 Access Protection for Log Data (S)

It SHOULD be ensured that administrators who execute logging have no authorisation to modify or delete recorded log data.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

OPS.1.1.5.A11 Increasing the Scope of Logging (H)

If applications or IT systems require increased protection, more events SHOULD be logged so that security-relevant incidents can be traced as comprehensively as possible.

To ensure that log data can be evaluated in real time, it SHOULD be stored centrally at shorter intervals by the relevant IT systems and applications. Logging SHOULD enable assessment of the entire information domain in question. Applications and IT systems that do not allow for central logging SHOULD NOT be used in case of increased protection needs.

OPS.1.1.5.A12 Encryption of Log Data (H)

Log data SHOULD be encrypted for secure transfer. All saved logs SHOULD be digitally signed. Archived log data and log data stored outside the corresponding logging infrastructure SHOULD also always be stored in an encrypted manner.

OPS.1.1.5.A13 Highly Available Logging Infrastructure (H)

A highly available logging infrastructure SHOULD be created.

4. Additional Information

4.1. Useful Resources

The Federal Office for Information Security (BSI) regulates the logging and detection of security-relevant events in “Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen” [BSI Minimum Standard for Logging and Detection of Cyber Attacks].

The International Organization for Standardization (ISO) specifies logging requirements in the ISO/IEC 27001:2013 standard (section A.12.4, “Logging and Monitoring”).

The Information Security Forum (ISF) provides guidelines for logging in “The Standard of Good Practice for Information Security” (section TM1.2, "Security Event Logging").

The National Institute of Standards and Technology (NIST) describes how logging can be used securely in Special Publication 800-92, “Guide to Computer Security Log Management”.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module OPS.1.1.5 *Logging*:

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.32 Misuse of Authorisation

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.46 Loss of Integrity of Sensitive Information

OPS.1.1.6 Software Tests and Approvals

1. Description

1.1. Introduction

The use of IT in organisations requires computerised data processing to be as error-free as possible, as the individual results can no longer be checked in most cases. Software of any kind must therefore be tested before it is put into operation. These tests must prove that software reliably provides the required functions and does not have any undesired side effects. When software is subsequently approved by the relevant organisational unit, basic permission is granted to use it in the respective organisation's production environment. At the same time, this organisational unit assumes responsibility for the IT process supported by the software.

Software can be tested at different stages of its lifecycle. For example, software tests can even become necessary during development, before approval for production operation, or within the scope of patch and change management. This applies to both custom and standardised software. Regression tests play a special role here because even if only minor aspects of software are changed, this can impact completely different characteristics and functions of the software. These effects are precisely what regression tests are designed to identify.

This module describes the testing and approval process for all types of software. The testing and approval process is characterised by the fact that it can be performed several times depending on the result.

1.2. Objective

This module is designed to ensure that software meets the technical and organisational requirements and the present protection needs of the entire organisation in question, or individual organisational units thereof. An essential aspect here involves systematically and methodically checking security-critical software for existing vulnerabilities.

1.3. Scoping and Modelling

OPS.1.1.6 *Software Tests and Approvals* must be applied once to the entire information domain under consideration.

Whilst module CON.8 *Software Development* refers to the software development process and the software tests it requires, this module describes the special requirements of test and approval management. In this context, test and approval management does not refer exclusively to software developed in-house or on behalf of a customer; it also includes the testing and approval of all the types of software described in APP.6 *General Software*, as well as all other software products covered by the APP *Applications* layer.

Software testing can also become part of patch or change management or software development. Corresponding requirements are specified in more detail in the modules OPS.1.1.3 *Patch and Change Management* and CON.8 *Software Development*.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module OPS.1.1.6 *Software Tests and Approvals*, the following specific threats and vulnerabilities are of particular importance.

2.1. Software Testing with Production Data

If software tests are carried out with production data, this may result in security problems. In particular, confidential production data may be accessed by unauthorised employees or third parties commissioned to perform software tests. If “original” production data (rather than copies thereof) is used for testing, it could be inadvertently changed or deleted.

Software tests conducted during production operations could severely disrupt the entire operation because malfunctions of the software to be tested could impact other applications and IT systems. In addition, software testers deliberately test software at its limits in order to uncover possible errors. This in turn increases the risk that the entire operation in question will be disrupted.

2.2. Insufficient Testing Procedures

If new software is tested insufficiently (or not at all) and approved without installation specifications, errors in the software may remain undetected. Moreover, it is possible that mandatory installation parameters will not be detected or considered as a result.

Software and installation errors that are not detected due to inadequate software testing procedures can significantly threaten an organisation's IT operations. For example, important data could be lost if a software update is installed.

2.3. Insufficient Approval Procedures

An insufficient approval procedure may result in the use of software that has not been technically approved. The software may thus lack necessary functions or include some that are not required or do not work as intended. Furthermore, the software may be incompatible with other applications.

2.4. Inadequate Documentation of Tests and Test Results

Software can usually be approved as soon as all tests have been performed and no deviations have been detected. However, if the documentation of the software tests is incomplete, it will not be possible later on to verify what was tested. If detected software errors or missing functions were insufficiently documented and thus not taken into account during release, these deviations can unintentionally delete or change the productive data to be processed. This may also disrupt other IT systems and applications.

2.5. Inadequate Documentation of Approval Criteria

If corresponding criteria are not clearly communicated, this may result in software approval being granted prematurely or not being granted even though it could be. On the one hand, this could lead to the approval of versions with undetected software errors, which may disrupt production operations. On the other, inadequate documentation of approval criteria can lead to project delays and financial losses.

3. Requirements

The specific requirements of module OPS.1.1.6 *Software Tests and Approvals* are listed below. The IT Operation Department is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Tester, Process Owner, Data Protection Officer, Human Resources Department

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

OPS.1.1.6.A1 Planning of Software Tests (B)

Before software tests are carried out, corresponding framework conditions MUST be specified within an organisation in accordance with the protection needs, organisational units, technical options, and test environments at hand. Software MUST be tested on the basis of a software requirements catalogue. If there is also a requirements specification, it MUST be taken into account as well.

Test cases MUST be selected in such a way that they test all the software functions at hand in the most representative way possible. In addition, negative tests SHOULD be included to ensure software does not contain any unwanted functions.

The test environment MUST be selected to be as representative as possible of all the device models and operating system environments used in the organisation in question. Testing SHOULD also determine whether software is compatible with and functional on the operating systems used in their present configurations.

OPS.1.1.6.A2 Performing Functional Software Tests [Tester] (B)

Functional software tests MUST verify the proper and complete functioning of software. Functional software tests MUST be performed in a manner that will not impact production operations.

OPS.1.1.6.A3 Assessing Test Results [Tester] (B)

The results of software tests MUST be assessed. A gap analysis SHOULD be performed using the defined specifications. Such assessments MUST be documented.

OPS.1.1.6.A4 Software Approval [Process Owner] (B)

The technical organisational unit responsible MUST approve software as soon as it has passed corresponding tests. The approval MUST be documented by means of an approval confirmation.

The approving organisational unit MUST verify whether the software has been tested in accordance with the relevant requirements. The results of the software tests MUST match the previously specified expectations. It MUST also be verified that the legal and organisational requirements at hand have been met.

OPS.1.1.6.A5 Performing Software Tests for Non-Functional Requirements [Tester] (B)

Software tests MUST be performed to verify that all essential non-functional requirements are met. In particular, security-specific software tests MUST be performed if the application in question includes security-critical functions. The test cases carried out MUST be documented along with their results.

OPS.1.1.6.A11 Using Anonymised or Pseudonymised Test Data [Data Protection Officer, Tester] (B)

If production data containing sensitive information is used for software tests, it MUST be appropriately protected during the testing. If this data contains personal information, it must be anonymised at minimum. Personal test data SHOULD be completely anonymised if

possible. If references to persons could be derived from the test data, the Data Protection Officer and (if applicable) the Employee Representatives MUST be consulted.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

OPS.1.1.6.A6 Orderly Instruction of Software Testers [Process Owner] (S)

The Process Owner SHOULD inform software testers of the test types to be performed and the software areas to be tested. Furthermore, the software testers SHOULD be informed of the use cases and possible further requirements of the software.

OPS.1.1.6.A7 Selecting Software Testers [Human Resources Department, Process Owner] (S)

Particular criteria SHOULD be considered when selecting software testers. Software testers SHOULD have the required professional qualifications.

If custom software is to be reviewed at the source code level, the testers SHOULD have sufficient expertise in the programming language and development environment to be tested. The source code SHOULD NOT be reviewed exclusively by testers who were also involved in the creation of the source code.

OPS.1.1.6.A8 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.1.6.A9 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.1.6.A10 Drawing Up an Acceptance Plan (S)

An acceptance plan SHOULD document the test types to be performed, the test cases considered, and the expected results. Furthermore, the acceptance plan SHOULD include the corresponding approval criteria. A procedure SHOULD be defined for the possibility of approval being denied.

OPS.1.1.6.A12 Performing Regression Tests [Tester] (S)

Regression testing SHOULD be performed when software has been changed. It SHOULD check whether previously existing security mechanisms and settings have been unintentionally changed by the update. Regression tests SHOULD be performed in full and include extensions and auxiliary resources. If test cases are omitted, this SHOULD be justified and documented. The test cases carried out SHOULD be documented along with their results.

OPS.1.1.6.A13 Separating the Test Environment from the Production Environment (S)

Software SHOULD only be tested in a test environment intended for this purpose. The test environment SHOULD be operated separately from the production environment. The architectures and mechanisms used in the test environment SHOULD be documented. The

documentation SHOULD also specify what is to be done with the test environment once the software tests are complete.

OPS.1.1.6.A15 Verification of Installation and Related Documentation [Tester] (S)

Software installations SHOULD be checked according to the rules for the installation and configuration of software (see module APP.6 *General Software*). If available, the installation and configuration documentation SHOULD also be checked.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

OPS.1.1.6.A14 Performing Penetration Tests [Tester] (H)

Penetration tests SHOULD be performed on applications and/or IT systems with increased protection needs. A concept for penetration tests SHOULD be created. In addition to the deployed test methods, the concept for penetration tests SHOULD document corresponding success criteria.

Penetration tests SHOULD be performed in accordance with the framework conditions of the penetration test concept. The vulnerabilities detected during penetration tests SHOULD be classified and documented.

OPS.1.1.6.A16 Security Vetting of Testers (H)

If testers require access to particularly sensitive information, the organisation in question SHOULD obtain evidence of their integrity and reputation. When dealing with classified material, software testers SHOULD be subjected to security vetting in line with the German Security Screening Act (SÜG). The CISO SHOULD involve the organisation's Confidentiality Officer or Security Representative in this regard.

4. Additional Information

4.1. Useful Resources

In ISO/IEC 27001:2013 (annex A.14, “System Acquisition, Development, and Maintenance”), the International Organization for Standardization (ISO) specifies requirements for secure system development (which also requires a test and approval process) and for test data. In addition, the ISO has published the standard ISO/IEC 29119-2:2013, “Software and Systems Engineering – Software Testing – Part 2: Test Processes”, which deals in detail with requirements for software testing.

The BSI has published the study “Durchführungskonzept für Penetrationstests” [Implementation Concept for Penetration Tests], which can be used as a basis for penetration tests, as well as the “BSI-Leitfäden zur Entwicklung sicherer Webanwendungen” [BSI

Guidelines for the Development of Secure Web Applications], which also includes software tests.

In “The Standard of Good Practice for Information Security”, the Information Security Forum (ISF) lists aspects of testing and approval for all relevant requirements (areas).

The National Institute of Standards and Technology provides guidelines for software testing in NIST Publication 800-53, SA 11 ("Developer Security Testing and Evaluation").

The book *The Art of Software Testing* by Glenford J. Myers, Corey Sandler, and Tom Badgett can be consulted on the subject of software testing.

The Common Vulnerability Scoring System can be used as a scoring system to classify the severity of a vulnerability and thus present the results of software testing in terms of information security.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module OPS.1.1.6 *Software Tests and Approvals*.

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.32 Misuse of Authorisation

G 0.38 Misuse of Personal Information

G 0.41 Sabotage

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

OPS.1.1.7 System Management

1. Description

1.1. Introduction

Reliable system management is a basic requirement for operating state-of-the-art networked systems in a secure and efficient manner. To that end, system management activities must fully integrate all the relevant systems at hand. Appropriate safeguards must also be implemented to protect system management communication and infrastructure.

System management includes many important functions, such as system monitoring, system configuration, event handling, and logging. Another important function is reporting, which may be designed as a common platform for IT systems and network components. Alternatively, it may be implemented in a dedicated manner as a uniform platform or as part of individual system management components.

A system management solution consists of various system management components, such as agents that are operated on an underlying system management infrastructure. This solution is used to control the integrated systems to be managed via the corresponding interfaces of the respective information domain. Overall, system management consists of the combination of the solution, the underlying infrastructure, the systems to be managed, and corresponding operations.

1.2. Objective

The objective of this module is to establish information security as an integral part of system management. The module describes how system management can be set up and secured and how the associated communication can be protected.

1.3. Scoping and Modelling

OPS.1.1.7 *System Management* must be applied to the system management solution that is used in the information domain in question.

In order to create an IT-Grundschutz model for a specific information domain, all the modules must be considered in their entirety. As a rule, several modules must be applied to the topic or target object.

Among other topics, this module covers the following:

- The necessary system management components
- The conceptual tasks related to system management
- Logging from the point of view of system management
- Updating a system management solution

The following content is also significant, but dealt with elsewhere:

- Network management requirements (see NET.1.2 *Network Management*)
- Details regarding the protection of the underlying infrastructure and of IT systems to be managed, in particular their management interfaces (see SYS.2 *Desktop Systems*)
- Logging and archiving concepts (see OPS.1.1.5 *Logging*, OPS.1.2.2 *Archiving*)
- Updates (e.g. with additional software) and agents (see OPS.1.1.3 *Patch and Change Management*)
- User access to system management solutions (see ORP.4 *Identity and Access Management*, as well as OPS.1.2.5 *Remote Maintenance* and OPS.1.1.2 *Proper IT Administration*).

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module OPS.1.1.7 *System Management*, the following specific threats and vulnerabilities are of particular importance.

2.1. Unauthorised Access to the System Management Solution

System management solutions are prime targets for attackers because they have a central position and the required access rights to all the systems to be managed.

If attackers manage to access system management solutions, (e.g. through unpatched security vulnerabilities), they can then control and reconfigure all the systems managed. They could thus access sensitive information or disrupt services or managed systems. For example, a company could centrally deploy configuration servers for a system management solution. An unpatched vulnerability is then exploited in order to modify the configuration files so that the managed systems install ransomware. As a result, all the systems managed by the system management solution are encrypted.

2.2. Errors in Automation Functions for System Management

All the security objectives of the information systems being managed can be compromised by faulty automated processes.

Errors in one or more automation functions, such as scripts, can render the systems being managed inoperable or compromised. Because of the automated processes, a large number of IT systems can quickly be compromised. Particularly critical IT systems can also be compromised in short order in this way.

2.3. Unauthorised Interference in System Management Communication

Accidental interference or targeted attacks on system management communications can violate the integrity of managed IT systems and limit the availability of services or IT systems.

If system management communications are intercepted and manipulated, active systems can be controlled in this way. Furthermore, the data transmitted to and from the systems may be intercepted and viewed.

2.4. Insufficient Time Synchronisation of System Management Components

Errors in time synchronisation can mask problems and events, making it difficult to detect security incidents and data leaks, for example.

If the system time of system management components is insufficiently synchronised, protocols that use time stamps to evaluate communication validity (for example) may be disrupted by the differences in system time between the system management components and the systems being managed.

In addition, it may not be possible to correlate system management logging data. Correlation may also result in erroneous statements if time stamps only appear to match or differ due to faulty synchronisation.

2.5. Incompatibility Between the Systems to Be Managed and the System Management Solution

A system management solution that is not fully compatible can trigger malfunctions of the IT systems to be managed and restrict their availability.

If the system management solution does not fully support the IT systems to be managed, certain actions cannot be performed as planned. This risk can also arise when systems are updated and management interfaces are changed.

2.6. Loss of Connection Between Users and the System Management Solution

Lost connections can limit the availability of a system management solution.

If the connection between an administrator and the system management solution is disrupted, IT systems may fail. In addition, troubleshooting and managing IT systems may become difficult.

If a connection is lost or disrupted, cost-intensive security-related and time-critical work cannot be carried out on time. It may not be possible to apply security updates or respond appropriately to security incidents, for example.

2.7. Loss of Connection Between the System Management Solution and Systems to be Managed

Lost connections to the systems to be managed can, in particular, impair the availability or integrity of services in the corresponding information domain.

The extent and constellation of a lost connection determine whether services are impaired and what damage can occur. It may be difficult to analyse the resulting error patterns or correct the errors that occur.

2.8. Insufficient Coordination Between System Management and Network Management

Uncoordinated actions in network management can have a negative impact on system management. This can lead to inconsistencies in configuration between IT systems and connecting networks. For example, lost connections in a network can trigger a large number of subsequent events in the area of system management. These events can extend to misconfigurations.

3. Requirements

The specific requirements of module OPS.1.1.7 *System Management* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	None

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

OPS.1.1.7.A1 Specification of System Management Requirements (B)

Requirements for system management infrastructure and processes MUST be specified. In so doing, all the essential elements of system management MUST be taken into account. The security aspects of system management MUST also be considered from the start.

In addition, the interfaces of the IT systems to be managed MUST be documented, in part to ensure the compatibility of the system management solution at hand and the system(s) to be managed.

OPS.1.1.7.A2 System Management Planning (B)

A system management solution and its underlying infrastructure MUST be planned appropriately. At minimum, planning MUST include the following:

- A detailed requirements analysis
- A meaningful rough concept
- A comprehensive implementation plan
- Milestones for quality assurance and acceptance

All the issues mentioned in the corresponding requirements specification and role and access control policy MUST be considered. The following aspects MUST be considered at minimum:

- Separation into appropriate areas for system management
- Access options to and by the system management solution
- System management authorisations on the systems to be managed
- Network connections for access to and by the system management solution
- Protocols for user access to the system management solution
- Protocols for communication between the system management solution and the systems to be managed
- Requirements that management systems tools must fulfil
- Interfaces for forwarding collected event or alarm messages
- Logging (including the required interfaces to a centralised logging solution)
- Vendor and developer support over the planned deployment period
- The option to apply patches to the system management solution and the systems to be managed
- Reporting and interfaces to overarching solutions
- Corresponding requirements to be fulfilled by the systems to be managed

OPS.1.1.7.A3 Time Synchronisation for System Management (B)

All the components of a system management solution, including the systems to be managed, MUST be synchronised. System time MUST be synchronised for each system to be managed and for the system management solution via appropriate protocols.

OPS.1.1.7.A4 Protection of System Management Communication (B)

As soon as a system management solution and the systems to be managed communicate via productive infrastructure, secure protocols MUST be used for this purpose. If this is not possible, a dedicated administration network (out-of-band management) MUST be used (see NET.1.1 *Network Architecture and Design*). If this is also not possible, complementary security mechanisms MUST be used at another level (e.g. tunnel mechanisms via encrypted VPN or comparable solutions).

OPS.1.1.7.A5 Mutual Authentication Between the System Management Solution and Systems to be Managed (B)

Authentication between a system management solution and the systems to be managed MUST be two-way in nature. Authentication MUST be integrated into an overarching authentication concept. Authentication MUST be performed using secure protocols.

OPS.1.1.7.A6 Securing Access to the System Management Solution (B)

User access to a system management solution MUST be secured through:

- Secure and appropriate authentication and authorisation of the user
- Secure encryption of transmitted data

An appropriate authentication method MUST be selected. The selection process MUST be documented. The strength of the cryptographic methods and keys used MUST be regularly reviewed and adjusted as needed.

The system management solution MUST use an authorisation component to ensure that users can only perform actions for which they are authorised.

3.2. Standard Requirements

For module OPS.1.1.7 *System Management*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

OPS.1.1.7.A7 Definition of a Security Policy for System Management (S)

For system management, a security policy SHOULD be drawn up and continuously maintained. All persons involved in system management SHOULD be familiar with the policy. The security policy SHOULD be integral to their work. Regular and transparent reviews SHOULD be conducted to ensure that the policy requirements are being implemented. The results SHOULD be documented.

At minimum, the security policy SHOULD specify the following:

- The areas of system management that are to be realised via central management tools and services
- The system management tasks that are to be realised in an automated manner
- Configuration management for the data managed by the system management solution, e.g. versioning of configurations

- Specifications for network separation
- Specifications for access control
- Logging specifications
- Quality assurance specifications for the use of automation functions, e.g. scripts
- Specifications for protecting communication
- The basic operational rules for system management
- Specifications for coordination with network management, e.g. assignment of IP addresses or DNS names

OPS.1.1.7.A8 Drawing Up a System Management Concept (S)

Based on the security policy drawn up for system management, a system management concept SHOULD be established and continually maintained. In doing so, the following minimum aspects SHOULD be taken into account as required:

- Methods, techniques, and tools for system management
- Protection of access and communication
- Protection at the network level, in particular the assignment of system management components to security zones
- Scope of monitoring and alerting for each system to be managed
- Logging
- Automation, in particular the central distribution of configuration files to the systems to be managed
- Specifications for the development and testing of automation functions
- Reporting chains in the event of malfunctions and security incidents
- Provisioning of system management information for other areas of the organisation in question
- Integration of system management into contingency planning
- Required network transmission capacity of the system management solution

OPS.1.1.7.A9 Detailed and Implementation Planning for System Management (S)

Detailed and implementation planning SHOULD be drawn up for system management solutions. It SHOULD consider all the items addressed in the respective security policy and system management concept.

OPS.1.1.7.A10 Concept for Secure Operation of the System Management Solution (S)

Based on the security policies and the system management concept at hand, a concept SHOULD be drawn up for the secure operation of the system management solution and the underlying infrastructure.

The manner in which the performance of other operative units can be integrated and controlled SHOULD also be checked.

OPS.1.1.7.A11 Regular Gap Analysis Within the Framework of System Management (S)

The IT Operation Department SHOULD regularly check the extent to which the data, configurations, and scripts managed by the system management solution correspond to the target state. At minimum, the following aspects SHOULD be checked in the gap analysis:

- The configuration of the system management solution
- The configuration of the systems to be managed
- The automation functions or scripts used

In the process, whether the aspects listed still meet the security policy and requirements specification SHOULD be reviewed. A comparison SHOULD also be made to determine whether the software version of the system management solution is up to date.

OPS.1.1.7.A12 Triggering Actions by the Central Components of the System Management Solution (S)

Actions performed by a system management solution on the systems managed SHOULD be triggered exclusively by the system management solution. For this purpose, only those management functions of the system management solution and the systems to be managed that are actually needed SHOULD be activated.

OPS.1.1.7.A13 Commitment to the Use of Designated Interfaces for System Management (S)

Management access to systems to be managed SHOULD only be obtained through the designated interfaces of the respective system management solution. If direct access is necessary to the systems to be managed (e.g. after a failure of one of these systems), both the direct access and all changes made in this context SHOULD be documented and entered into the system management solution to the extent necessary.

OPS.1.1.7.A14 Central Configuration Management for Systems to be Managed (S)

Software and configuration data for systems to be managed SHOULD be consistently managed in a configuration management system that provides versioning and change tracking. The associated documentation for configuration management SHOULD be complete and up to date at all times. The documentation required for this SHOULD be securely available from a central point and integrated into backup processes. The central configuration management used for this purpose SHOULD be maintained continuously and audited regularly.

All interfaces between the system management solution and other applications and services SHOULD be documented and fully managed in a configuration management solution. Functional changes to the interfaces SHOULD be coordinated between the relevant operational areas at an early stage and documented accordingly.

Configuration data for the systems being managed SHOULD be automatically distributed across the network, and it SHOULD be possible to install and activate it without interrupting operations.

OPS.1.1.7.A15 Status Monitoring, Logging, and Alerting of Relevant Events in the System Management Solution and the Systems to be Managed (S)

The basic performance and availability parameters of a system management solution and the systems to be managed SHOULD be continuously monitored. For this purpose, the respective threshold values SHOULD be determined in advance (baselining). If defined threshold values are exceeded, the responsible personnel SHOULD be notified automatically.

For better error analysis, information from the status monitoring of other areas (e.g. from a separate “Networks” area) SHOULD also be considered to find the exact cause of disruptions.

Important events on systems to be managed and on the system management solution SHOULD be automatically transmitted to a central logging infrastructure and logged there (see OPS.1.1.5 *Logging*).

Important events SHOULD be defined for the following aspects at minimum:

- Failure or inaccessibility of systems to be managed
- Failure or inaccessibility of system management components
- Hardware malfunctions
- Login attempts on the system management solution
- Login attempts on systems to be managed
- Critical states or overload of the system management solution
- Critical states or overloads of systems to be managed

Event messages and logging data SHOULD be transmitted to a central logging system. Alarm messages SHOULD be transmitted as soon as they occur.

OPS.1.1.7.A16 Integration of System Management into Contingency Planning (S)

A system management solution SHOULD be integrated into its organisation’s contingency planning. To accomplish this, both the system management solution and the configurations of the systems being managed SHOULD be secured and integrated into restoration of service plans.

OPS.1.1.7.A17 Control of System Management Communication (S)

Communications between users and a systems management solution, as well as between the system management solution and the IT systems being managed, SHOULD be limited to strictly necessary connections using appropriate filtering techniques.

OPS.1.1.7.A18 System State Verification (S)

The consistency between a system's actual state and the state assumed by the corresponding system management solution SHOULD be checked regularly. If discrepancies are found, the state assumed by the system management solution SHOULD be restored.

OPS.1.1.7.A19 Securing System Management Communications Between the System Management Solution and the Systems Being Managed (S)

System management communications between a system management solution and the systems to be managed SHOULD always be encrypted. The strength of the cryptographic procedures and keys used SHOULD be checked at regular intervals and adjusted as necessary.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

OPS.1.1.7.A20 Implementing System Management Solutions for High Availability (H)

A central system management solution SHOULD be operated in a manner that ensures high availability. To this end, the servers and tools used for the system management solution (including their network connections) SHOULD be designed redundantly.

OPS.1.1.7.A21 Physical Separation of the Central System Management Network (H)

An organisation's management network for system management SHOULD be physically separated from its functional (and especially its productive) networks.

OPS.1.1.7.A22 Integration of System Management into Automated Detection Systems (S)

The logging of security-relevant events in system management SHOULD be integrated into a security information and event management (SIEM). The events to be forwarded to the SIEM SHOULD be comprehensibly defined.

The requirements catalogue for selecting a system management solution SHOULD specify the necessary interfaces and transfer formats.

A system management solution SHOULD be monitored in an automated manner by a security vulnerability detection system.

OPS.1.1.7.A23 Cross-Site Time Synchronisation for System Management (H)

Time synchronisation SHOULD be ensured for both an organisation's system management solution and the systems being managed across all its sites. A common reference time SHOULD be used for this purpose.

OPS.1.1.7.A24 Automated Checking of Security-Relevant Configurations by Suitable Detection Systems (H)

Security-relevant configurations of a system management solution and the systems to be managed SHOULD be regularly checked by suitable detection systems for deviations from the target state and for potential vulnerabilities.

OPS.1.1.7.A25 Logging and Regulation of System Management Meetings (H)

Session content, particularly user activity on a system management solution and all instances of direct access to systems to be managed, SHOULD be continuously logged and regulated by a technical solution. Command-level activities (i.e. manual and automated commands) SHOULD be monitored and prevented if necessary.

During monitoring, alerts SHOULD be raised not only in the event of specific rule violations, but also in case of anomalies in user behaviour.

OPS.1.1.7.A26 Decoupling of Access to the System Management Solution (H)

All administrative access to a system management solution SHOULD be secured through the use of jump servers.

4. Additional Information

4.1. Useful Resources

No further information is available for module OPS.1.1.7 *System Management*.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module OPS.1.1.7 *System Management*:

G 0.9 Failure or Disruption of Communication Networks

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.37 Repudiation of Actions

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

OPS.1.2.2 Archiving

1. Description

1.1. Introduction

Archiving plays a special role in the document management process. On the one hand, digital documents are expected to be available until the end of a specified retention period. On the other, their confidentiality and integrity need to be preserved. In addition, the context must be maintained so that the respective stored sequence can be reconstructed.

For the entire duration of long-term storage, corresponding safeguards for information maintenance and, if required, measures for maintaining evidence must therefore be implemented.

The German IT terms for “electronic archiving” and “electronic long-term storage” are sometimes used synonymously. For better clarity, the terms “archiving” and “digital long-term archive” are used in this module. An IT process for storing electronic documents is referred to as an “archive system”, “digital archive”, or “long-term storage”. The retention period of documents depends on the applicable legal regulations and other requirements, as well as on the purpose of the data involved.

In this module, the term “documents” includes data and digital documents unless these are expressly used with a differing meaning.

From a German legal perspective, the term “archiving” is substantiated and documented by the federal and state archiving laws. "Archiving" in the legally correct sense refers solely to government documents. It refers to how the documents of an authority are to be segregated and preserved by a competent governmental facility (Federal Archive) for an unlimited period of time as soon as they are no longer needed for the purposes of that authority (see Articles 1 and 2 of the German Federal Archives Act (BArchG)). This type of archiving should distinguished from the time-limited retention considered in this module.

1.2. Objective

This module describes how digital documents can be securely archived for the long term such that they are reproducible and cannot be changed. To this end, it defines requirements that can be used to securely plan, implement, and operate an archive system.

The storage of paper documents is not considered in this module, but requirements are made as to how these can be digitised and archived.

1.3. Scoping and Modelling

Module OPS.1.2.2 *Archiving* must be applied once to any information domain that involves long-term archiving of electronic documents. Long-term archiving may be necessary due to external or internal requirements, or a system for long-term archiving of electronic documents may already be in operation.

This module does not deal with archiving for an unlimited period of time in the sense of Germany's federal and state archive laws.

It describes security safeguards with which electronic documents can be stored and preserved for the long term within the framework of the applicable retention periods. Safeguards for operative backups are not addressed in this module. Requirements in this regard are covered in CON.3 *Backup Concept*.

Long-term digital storage consists of individual components, such as a database. Detailed descriptions of how such components can be operated securely are not covered in this module. The requirements of the corresponding modules, such as APP.4.3 *Relational Database Systems*, SYS.1.1 *General Server*, and SYS.1.8 *Storage Systems* should be considered in this regard.

2. Threat Landscape

For module OPS.1.2.2 *Archiving*, the following specific threats and vulnerabilities are of particular importance:

2.1. Obsolescence of Archive Systems

Archived data should typically remain stored over a very long period of time. During this period, the underlying technical system components, storage media, and data formats may age physically or technically and become useless. Compatibility issues with the data formats used can arise over the course of time, for example.

If there is no response to the ageing process, it should be assumed that archived raw data will be no longer readable from archive media in the long term. Archived data can also be changed due to physical errors in archive systems and archiving media.

2.2. Inadequate Indexing Keys for Archives

Electronic archives may contain very large amounts of data. In such cases, the individual datasets are stored in accordance with certain indexing keys, which is where a distinction must be made between business application index data and archive system index data. If unsuitable classification criteria are used, it may be difficult or impossible to search for archived documents. It may also be impossible to clearly determine the semantics of documents. Furthermore, an unsuitable or limited selection of classification criteria could thwart the objectives of preservation (e.g. the ability to provide evidence to third parties).

2.3. Unauthorised Archive Access due to Insufficient Logging

Unauthorised archive access is normally discovered with the help of log files. If logging is not performed to the required extent, such access attempts may not be detected. As a consequence, attackers might obtain stored information without this being noticed and copy or change the information, for example.

2.4. Inadequate Transfer of Paper-Based Data to an Electronic Archive

When scanning documents, the appearance or semantics of the data recorded may be compromised or documents may even be lost. As a result, the information in a document could be misinterpreted and miscalculated, such as if important parts of the document or the document batch are forgotten during scanning.

2.5. Insufficient Renewal of Cryptographic Procedures During Archiving

Cryptographic methods used for signatures, seals, time stamps, technical evidence records, or encryptions, for example, must be regularly adapted to the current state of the art in order to retain their protective effect. If this is neglected, the integrity of documents can no longer be guaranteed (e.g. due to an outdated and insecure signature). Furthermore, a file may not be admitted as evidence in court even if the document itself is still completely correct. The confidentiality of an encrypted document can also be lost this way.

2.6. Insufficient Archiving Audits

If the archiving process is audited too infrequently or inaccurately, malfunctions may not be detected. The integrity of the archived documents themselves may thus be called into question. This may result in legal and economic disadvantages for the organisation in question. A file might not be admissible as evidence in court, for example, because it cannot be ruled out that the file has been manipulated.

2.7. Violation of Legal Framework Conditions Regarding the Use of Archive Systems

When archiving electronic documents, different legal framework conditions must be observed. If these are not met, this may have civil or criminal consequences–for example, in

cases involving minimum retention periods pertaining to tax-related or budgetary requirements.

3. Requirements

The specific requirements of module OPS.1.2.2 *Archiving* are listed below. As a matter of principle, the Process Owner is responsible for compliance with the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Process Owner
Further responsibilities	User, IT Operation Department

3.1. Basic Requirements

For module OPS.1.2.2 *Archiving*, the following requirements MUST be met as a matter of priority:

OPS.1.2.2.A1 Determining Parameters for Electronic Archiving (B)

Before methods and products for electronic archiving are chosen, the technical, legal and organisational influencing factors MUST be determined and documented. The results MUST be incorporated into the archiving concept in question.

OPS.1.2.2.A2 Drawing up an Archiving Concept (B)

The aims to be achieved through archiving MUST be defined. In particular, this MUST take into consideration the rules to be followed, the employees who will be responsible, and the desired scope of functions and services.

The results MUST be documented in an archiving concept. The Top Management MUST be involved in this process. The archiving concept MUST be adapted to the current circumstances at regular intervals.

OPS.1.2.2.A3 Appropriate Installation of Archive Systems and Storage of Archive Media [IT Operation Department] (B)

The IT components of an archive system MUST be installed in secured rooms. It MUST be ensured that only authorised persons may access the rooms. Archive storage media MUST be stored appropriately.

OPS.1.2.2.A4 Consistent Indexing of Data During Archiving [IT Operation Department, User] (B)

All the data, documents, and records stored in an archive MUST be uniquely indexed. To this end, the desired structure and extent of an archive's index information MUST be defined in the design phase.

OPS.1.2.2.A5 Regular Regeneration of Archived Data [IT Operation Department] (B)

The following MUST be ensured over the entire archiving period in question:

- the data format used can be processed by the applications used
- the data stored can be read and reproduced in the future in such a way that semantics and significance can be maintained
- the file system used on the storage medium can be processed by all the components involved
- the storage media can be read at any time without technical issues
- the cryptographic methods used for encryption and the preservation of legal relevance by means of digital signatures, seals, time stamps, or technical evidence records correspond to the state of the art

OPS.1.2.2.A6 Protection of the Integrity of the Index Database of Archive Systems [IT Operation Department] (B)

The integrity of index databases MUST be safeguarded and verifiable. In addition, index databases MUST be backed up regularly. It MUST be possible to restore the backups. Medium-sized and large archives SHOULD have redundant index databases.

OPS.1.2.2.A7 Regular Backups of System and Archive Data [IT Operation Department] (B)

All archive data, the related index databases, and the system data MUST be backed up at regular intervals (see CON.3 *Backup Concept*).

OPS.1.2.2.A8 Logging Archival Access [IT Operation Department] (B)

All attempts to access electronic archives MUST be logged. To this end, dates, times, users, client systems, the actions performed, and any error messages SHOULD be recorded. The archiving concept in question SHOULD specify how long the log data should be retained.

The log data for archive access SHOULD be evaluated regularly. In so doing, the internal specifications of the organisation at hand SHOULD be taken into account.

The specific staff members to whom specific events (e.g. system errors, timeouts, and the copying of records) should be displayed SHOULD also be defined. Critical events SHOULD be evaluated and, if required, escalated immediately once they are detected.

OPS.1.2.2.A9 Selection of Suitable Data Formats for Archiving Documents [IT Operation Department] (B)

A suitable data format MUST be selected for archiving. It MUST ensure that archived data and selected features of the initial document medium can be reproduced in the long term in a format that is true to the original.

It MUST be possible to unambiguously interpret and electronically process the document structure of the selected data format. The syntax and semantics of the data formats used SHOULD be documented and published by a standardisation organisation. A loss-free image compression method SHOULD be used for evidential and audit-compliant archiving.

3.2. Standard Requirements

For module OPS.1.2.2 *Archiving*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

OPS.1.2.2.A10 Drawing Up a Policy for Using Archive Systems [IT Operation Department] (S)

It SHOULD be ensured that employees use archive systems as prescribed in the applicable archiving concept. To this end, an administration and user policy SHOULD be drawn up. The administration policy SHOULD cover the following items:

- assignment of responsibility for operation and administration
- agreements regarding performance parameters during operation (including service level agreements)
- terms regarding the assignment of site and data access rights
- terms regarding the assignment of access rights to the services provided by the archive
- regulations regarding the handling of archived data and archive media
- monitoring of the archive system and the related environmental conditions
- rules on backups
- rules on logging
- separation of producers and consumers (OAIS model)

OPS.1.2.2.A11 Instruction Regarding the Administration and Operation of the Archive System [IT Operation Department, User] (S)

Users and the responsible employees in the IT Operation Department SHOULD be trained in their areas of responsibility.

The training of IT Operation Department employees SHOULD cover the following subjects:

- system architecture and security mechanisms of the archive system used and the underlying operating system
- installation and operation of the archive system and handling of archive media
- documentation of administrative activities

- escalation procedures

The user training SHOULD cover the following subjects:

- handling the archive system
- operating the archive system
- legal framework conditions of archiving

The completion of these training courses and the names of those who attend SHOULD be documented.

OPS.1.2.2.A12 Monitoring of Storage Resources for Archive Media [IT Operation Department] (S)

The capacity available in archive media SHOULD be monitored continuously. Once it has fallen below a defined threshold, a responsible employee MUST be alerted automatically. The alert SHOULD be role-based. A sufficient number of empty archive media MUST be available on short notice at any point in time to prevent storage bottlenecks.

OPS.1.2.2.A13 Regular Auditing of Archiving Processes (S)

Whether archiving processes are still working correctly and properly SHOULD be checked regularly. A checklist SHOULD be drawn up for this that includes questions regarding responsibilities, organisational processes, use of archiving, the redundancy of archived data, administration, and technical assessment of the archive system. The audit results SHOULD be documented transparently and compared against the target condition. Deviations SHOULD be investigated.

OPS.1.2.2.A14 Regular Observation of the Market for Archive Systems [IT Operation Department] (S)

The market for archive systems SHOULD be observed regularly and systematically. Among other aspects, the following criteria SHOULD be taken into account:

- changes in standards
- instances in which hardware and software manufacturers move to different technologies
- published security gaps or vulnerabilities
- cases in which the security of cryptographic algorithms becomes compromised

OPS.1.2.2.A15 Regular Processing of Cryptographically Secured Data During Archiving [IT Operation Department] (S)

Developments in the field of cryptography should be continuously monitored to assess the ongoing reliability and security of a given algorithm (see also OPS.1.2.2.A20 *Appropriate Use of Cryptographic Procedures During Archiving*).

Archive data that has been secured using cryptographic procedures that will no longer be suitable for securing in the foreseeable future SHOULD be re-secured in good time using suitable procedures.

OPS.1.2.2.A16 Regular Renewal of Technical Archive System Components [IT Operation Department] (S)

Archive systems SHOULD be kept in line with the current state of the art over long periods of time. New hardware and software SHOULD be tested comprehensively before being installed in a running archive system. When commissioning new components or introducing new file formats, a migration concept SHOULD be drawn up. This concept SHOULD describe all changes, tests, and expected test results. Conversion of the individual data sets SHOULD be documented (using a transfer note).

When converting archive data to new formats, it SHOULD be checked whether the data must also be archived in its initial format as a consequence of legal requirements.

OPS.1.2.2.A17 Selecting a Suitable Archiving System [IT Operation Department] (S)

A new archive system SHOULD always be selected on the basis of the specifications mentioned in the archiving concept in question. It SHOULD meet the requirements formulated in this concept.

OPS.1.2.2.A18 Using Appropriate Archive Media [IT Operation Department] (S)

Appropriate media SHOULD be selected and used for archiving. In doing so, the following aspects should be considered:

- the data volumes to be archived
- the average access times
- the average number of simultaneous users accessing the archive system

The archive media SHOULD also meet the requirements of long-term archiving with regard to audit compliance and useful life.

OPS.1.2.2.A19 Regular Function and Recovery Tests for Archiving [IT Operation Department] (S)

Regular function and recovery tests SHOULD be performed for archiving. The readability and integrity of archived storage media SHOULD be checked at least once a year. Appropriate processes SHOULD be defined for troubleshooting.

Furthermore, the hardware components of archive systems SHOULD be checked for sound functionality at regular intervals. Whether all archiving processes work without any errors SHOULD also be checked regularly.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.2.2 *Archiving* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

OPS.1.2.2.A20 Appropriate Use of Cryptographic Methods for Archiving [IT Operation Department] (H)

To cover long retention periods, archive data SHOULD only be secured with cryptographic procedures that are based on current standards.

OPS.1.2.2.A21 Transfer of Paper-based Data to Electronic Archives (H)

If documents on paper are digitised and transferred to an electronic archive, it SHOULD be ensured that the digital copy matches the original document in terms of its images and content.

4. Additional Information

4.1. Useful resources

In its publication “Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung: Auflistung geeigneter Algorithmen und Parameter” [Announcement on Electronic Signatures Under the Digital Signature Act and the Digital Signature Ordinance: List of Suitable Algorithms and Parameters], the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (BnetzA) lists algorithms and parameters that have been classified as suitable.

The German Institute for Standardisation (DIN) defines criteria for trustworthy digital long-term archives in DIN 31644:2012-04, “Information and Documentation – Criteria for Trustworthy Digital Archives”. DIN 31647:2015-05, “Information and Documentation – Preservation of Evidence in Cryptographically Signed Documents”, defines technical and security requirements for the long-term storage of digitally signed documents while preserving the legal force of digital signatures.

In its technical guideline BSI TR-03138, "RESISCAN: Replacement Scanning”, the BSI has compiled the security-relevant technical and organisational measures that must be taken into account for replacement scanning.

In the technical guideline BSI TR-03125, "TR-ESOR: Preservation of Evidence in Cryptographically Signed Documents” (including its annexes), the BSI provides a guideline that describes how electronically signed data and documents can be stored in a trustworthy manner—that is, in the sense of the legally effective preservation of evidential value—over long periods of time until the end of the respective retention periods.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the

requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module OPS.1.2.2 *Archiving*.

G 0.2 Unfavourable Climatic Conditions

G 0.4 Pollution, Dust, Corrosion

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.37 Repudiation of Actions

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

OPS.1.2.4 Teleworking

1. Description

1.1. Introduction

Teleworking is understood to refer to all tasks that are performed in part or entirely outside of the business premises and buildings of an employer using information and communication technology. In home-based teleworking, employees regularly alternate between a home office and the workplace of their employer on a daily or hourly basis.

1.2. Objective

The objective of this module is to protect information that is stored, processed, and transmitted during teleworking. To this end, it presents typical threats and defines special requirements for secure teleworking.

1.3. Scoping and Modelling

Module OPS.1.2.4 *Teleworking* must be applied to every teleworking location.

This module concentrates on the form of teleworking that occurs in the home environment (home-based teleworking). It is assumed that a secure telecommunication link is available between a given home workstation and the corresponding organisation to allow suitable information to be exchanged and data to be accessed on the organisation's servers. The requirements of this module cover the following three areas:

- the organisation of teleworking
- the employee's workstation computer
- the communication link between the teleworking computer and the organisation in question

Security requirements for the infrastructure of teleworking locations are not included in this module; these are described in module INF.8 *Working from Home*. Requirements for non-fixed workplaces can be found in module INF.9 *Mobile Workplace*.

Detailed recommendations on how to configure and secure IT systems are not covered by this module. Information on this is included in SYS.2.1 *General Client*, as well as in the operating-system-specific modules. Other security aspects relevant to teleworking, such as for WLAN, are considered in the modules of the sublayers NET.2 *Radio Networks* and NET.4 *Telecommunication*.

If data modified during telework is not stored directly on the organisation's IT systems, the requirements for carrying out backups must be specified. Corresponding requirements are included in module CON.3 *Backup Concept*.

2. Threat Landscape

For module OPS.1.2.4 *Teleworking*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Rules for Teleworking Locations

The use of teleworking locations requires supplementary organisational agreements between employees and supervisors. In addition, employees and supervisors need to know what to do should security-relevant incidents occur in teleworking locations. If, for example, confidential information falls into the hands of third parties, an organisation can incur serious damage.

2.2. Unauthorised Private Use of Teleworking Computers

It is easier to use untested and unapproved hardware or software in the home environment. Doing so carelessly can, however, allow malware to access a teleworking computer (for example). This could compromise confidential information.

2.3. Delays Caused by Temporarily Restricted Availability of Employees

If an employee does not have fixed working hours when teleworking and no fixed times have been agreed when they must be available, this can cause delays in work processes.

2.4. Poor Integration of Employees into the Information Flow

Since teleworking employees do not work at their organisation every day, they have fewer opportunities to participate in direct exchanges of information with supervisors and work colleagues. Information that is passed on verbally may be delayed or may not reach teleworkers at all. This can disrupt workflows and operational processes and limit these employees' productivity.

2.5. Non-Compliance with Security Safeguards

In teleworking locations, a lack of monitoring capabilities (for example) may result in employees failing to implement some or all of the recommended or required security

safeguards. This can result in confidential information falling into the hands of third parties, for instance.

3. Requirements

The specific requirements of module OPS.1.2.4 *Teleworking* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Employee, IT Operation Department, Supervisor, Human Resources Department

3.1. Basic Requirements

For module OPS.1.2.4 *Teleworking*, the following requirements MUST be met as a matter of priority:

OPS.1.2.4.A1 Rules on Teleworking [Supervisor, Human Resources Department] (B)

All the relevant aspects of teleworking MUST be specified. The applicable rules or a corresponding leaflet explaining the security safeguards to be considered MUST be provided to teleworkers. Contentious points MUST be clarified in employment agreements or separate agreements between the employee and employer as a supplement to their employment contract. The rules MUST be updated at regular intervals.

OPS.1.2.4.A2 Security-Related Requirements for Teleworking Computers (B)

Security-related requirements MUST be defined that IT systems must meet for teleworking.

It MUST be ensured that only authorised persons have access to teleworking computers. Moreover, teleworking computers MUST be protected so that they can be used only for authorised purposes.

OPS.1.2.4.A3 ELIMINATED (B)

This requirement has been eliminated.

OPS.1.2.4.A4 ELIMINATED (B)

This requirement has been eliminated.

OPS.1.2.4.A5 Employee Awareness and Training (B)

Employees MUST be made aware of the risks connected to teleworking by means of a guide. Furthermore, they MUST be instructed in the corresponding security safeguards of their

organisation and trained in how to deal with them. Training and awareness safeguards for employees SHOULD be repeated at regular intervals.

3.2. Standard Requirements

For module OPS.1.2.4 *Teleworking*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

OPS.1.2.4.A6 Creating a Security Concept for Teleworking (S)

A security concept for teleworking that describes the security objectives, protection needs, security requirements, and risks involved SHOULD be drawn up. The concept SHOULD be reviewed and updated regularly. The security concept for teleworking SHOULD be coordinated with the overall security concept of the organisation in question.

OPS.1.2.4.A7 Regulations on Using Communication Capabilities for Teleworking [IT Operation Department, Employee] (S)

Clear rules SHOULD be specified regarding which communication capabilities may be used under which general framework conditions for the purpose of teleworking. There SHOULD be rules regarding the professional and private use of Internet services when teleworking. Here, it SHOULD also be clarified whether private use is generally allowed or prevented.

OPS.1.2.4.A8 Flow of Information Between Employees and Organisations [Supervisor, Employee] (S)

A regular in-house exchange of information SHOULD be ensured between teleworking employees and organisations. All employees SHOULD be informed about changed security requirements and other security-relevant aspects in a timely manner. All the colleagues of teleworking employees SHOULD know when and where these employees can be contacted. Technical and organisational teleworking rules on the performance of tasks, security incidents, and other problems SHOULD be specified and communicated to employees.

OPS.1.2.4.A9 Support and Maintenance Concept for Teleworking Locations [IT Operation Department, Employee] (S)

A special support and maintenance concept SHOULD be drawn up for teleworking locations. This concept SHOULD specify the following aspects: contact persons for user services, maintenance dates, remote maintenance, transport of IT devices, and the introduction of standard teleworking computers. Contact persons for hardware and software problems SHOULD be named to help ensure that employees can continue to work.

OPS.1.2.4.A10 Analysis of Teleworking Location Requirements [IT Operation Department] (S)

A requirements analysis SHOULD be performed before setting up a teleworking location. It SHOULD include the hardware and software components required for teleworking locations. The requirements for each teleworking location SHOULD be agreed with the persons in charge of IT. The protection needs of the information processed at teleworking locations SHOULD always be determined and documented.

3.3. Requirements in Case of Increased Protection Needs

No requirements with increased protection needs are defined for module OPS.1.2.4 *Teleworking*.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides information on how to deal with teleworking in the standard ISO/IEC 27001:2013, especially in annex A, A.6.2.1 (“Mobile Device Policy”) and A.11.2.6 (“Security of Equipment and Assets Off-Premises”.

The Information Security Forum (ISF) also provides guidelines on teleworking in “The Standard of Good Practice for Information Security”, especially in Area PA2 ("Mobile Computing").

The National Institute of Standards and Technology (NIST) has published NIST Special Publication 800-46, “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module OPS.1.2.4 Teleworking.

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.40 Denial of Service

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

OPS.1.2.5 Remote Maintenance

1. Description

1.1. Introduction

The term remote maintenance refers to when an external IT system is used to access IT systems and the applications running on them. This access can facilitate configuration, maintenance, or repair work, for example.

There are different ways to carry out remote maintenance. Remote client maintenance often involves transmitting the keyboard and mouse signals from an administrator's IT system to a remote IT system. The remote IT system then transmits its screen output back to the administrator's IT system. The administrator can thus perform actions on the remote IT system as if they were on site (active remote maintenance). In the case of remote server maintenance, the input and output of a console is often transmitted.

In passive remote maintenance, only the screen contents of an IT system are transmitted to an administrator. The administrator gives instructions to a user on site, who carries them out under the administrator's supervision. However, this approach usually proves to be very time-consuming and cumbersome in practice, which is why IT departments are often granted full access to IT systems.

Since many IT systems are located beyond the reach of their administrators (e.g. in remote data centres, industrial facilities, or an off-site location without IT staff), remote maintenance is used in many organisations. Remote maintenance often involves accessing an organisation's internal IT systems and applications through insecure networks. Because of the far-reaching possibilities for intervention in these IT systems and applications, securing remote maintenance components is particularly important.

1.2. Objective

The aim of this module is to protect information that is stored, processed, and transmitted during remote maintenance, along with the remote maintenance interfaces of IT systems. For this purpose, it presents requirements that relate equally to the functions of active and passive remote maintenance.

1.3. Scoping and Modelling

This module must be applied to all the target objects for which remote maintenance is used in the information domain under consideration.

It covers remote maintenance mainly from the point of view of an IT department and provides advice for administrators on how remote maintenance may be used. It is important that information security be guaranteed holistically in all lifecycle phases. The security aspects of the communication links and the authentication mechanisms used, along with the protection of remote maintenance access, are important components of the module. Nevertheless, it does not cover all the relevant aspects of the business processes associated with remote maintenance. In particular, the modules OPS.1.1.3 *Patch and Change Management*, ORP.3 *Awareness and Training in Information Security*, CON.1 *Crypto Concept*, and CON.3 *Backup Concept* should also be considered. The requirements of the NET *Networks and Communication* module layer must also be implemented in areas where they relate directly to remote maintenance.

If remote maintenance is carried out by an external service provider, module OPS.2.1 *Outsourcing for Customers* must also be observed. If cloud-based remote maintenance products are used, the general requirements from OPS.2.2 *Cloud Usage* must also be met.

Requirements for protecting remote maintenance using firewalls are not part of this module. These are included in module NET.3.2 *Firewall*.

Fundamental aspects of IT administration are also not included in this module. These can be found in module OPS.1.1.2 *Proper IT Administration*.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module OPS.1.2.5 *Remote Maintenance*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inadequate Knowledge of Remote Maintenance Regulations

Administrators who set up and use remote maintenance depend on regulations that define how remote maintenance is to be used. For example, it is necessary to determine how applications are to be configured for remote maintenance. Otherwise, remote maintenance can create additional risks for the respective internal network. If the parties involved are not informed of the regulations on remote maintenance, this poses risks to IT operations. For example, an administrator could set up a remote maintenance interface and allow an authentication procedure with an insecure password instead of a secure, certificate-based procedure.

2.2. Inadequate Planning and Rules for Remote Maintenance

If an organisation does not plan, set up, and control its remote maintenance with care, the security of all its IT systems may be impaired. If, for example, insecure communication

protocols, encryption algorithms, or authentication mechanisms are used, vulnerabilities can arise. Inadequately secured remote maintenance interfaces may also compromise an adjacent third-party network.

2.3. Inappropriate Use of Authentication During Remote Maintenance

Different authentication mechanisms can be used for remote maintenance. If an insecure authentication procedure is used, unauthorised third parties may obtain administrative authorisation on remote maintenance systems or for remote maintenance tools. This could allow them to access an organisation's IT systems and cause extensive damage.

An example of this is a login procedure that uses a short password. An attacker can quickly guess this password and thus gain access to an organisation's IT systems.

2.4. Improper Remote Maintenance

Professional and regular remote maintenance is required to ensure the security and proper functioning of IT systems and applications than can only be accessed remotely. If IT systems and applications are not properly configured and maintained via remote maintenance, they will (in the worst case) no longer be usable. If remote maintenance processes do not run correctly, this can lead to malfunctions of individual operating system components. Moreover, vulnerabilities may occur because of IT system maintenance work that is carried out too late or improperly.

2.5. Use of Insecure Protocols in Remote Maintenance

Communication via public and internal networks by means of insecure protocols constitutes a potential threat. If, for example, outdated versions of IPSec, SSH, or SSL/TLS are used to establish a tunnel between two networks or endpoints, it cannot be guaranteed that this tunnel is sufficiently secure and the information transmitted in it is adequately protected. Attackers may exploit vulnerabilities of these protocols in order to inject their own contents into protected connections. Protocols in which information is transmitted in plain text are generally considered insecure.

2.6. Insecure and Uncontrolled Use of Remote Maintenance Access by Third Parties

If IT systems are maintained remotely by third parties without a contractual basis, the responsibilities for remote maintenance may not be clearly defined. As a result, role separation can be circumvented, for example, or open remote maintenance access may not be documented.

2.7. Use of Online Services for Remote Maintenance

In addition to cases in which an administrator establishes a direct data connection to a given organisation for remote maintenance purposes, online services may be used. Here, the IT systems to be administered establish a connection to the servers of a third-party provider and the administrators use a web browser or similar means to access the systems.

If this communication is not subject to end-to-end encryption, the online service provider could read the data exchanged. In addition, the IT systems may also be administered by unauthorised persons if the data connection is manipulated. If the IT systems automatically establish a data connection to the online service upon starting up, they could be accessed directly without the users of the systems or the responsible administrator noticing.

2.8. Unknown Remote Maintenance Components

Many IT systems contain components that offer integrated functions for remote maintenance. However, these functions are often poorly documented and not taken into account during the procurement and operation of IT systems.

Integrated remote maintenance components have far-reaching access to the IT systems in which they are installed. This access often directly affects other components of the IT system and can thus bypass the security mechanisms of the underlying operating system. In addition, integrated remote maintenance functions can contain vulnerabilities that facilitate unauthorised access to IT systems.

3. Requirements

The specific requirements of module OPS.1.2.5 *Remote Maintenance* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	User

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

The following requirements MUST be met for this module as a matter of priority.

OPS.1.2.5.A1 Planning the Use of Remote Maintenance (B)

The use of remote maintenance MUST be adapted to each individual organisation. Remote maintenance MUST be planned in a needs-based manner with regard to technical and organisational aspects. At minimum, consideration MUST be given to the IT systems that should be maintained remotely and the persons responsible for this.

OPS.1.2.5.A2 Establishing a Secure Connection for Remote Maintenance of Clients [User] (B)

If desktop environments of clients are accessed via remote maintenance, the users of these IT systems MUST explicitly consent to this access.

OPS.1.2.5.A3 Securing Interfaces for Remote Maintenance (B)

The possible access and communication connections for remote maintenance MUST be restricted to those required. All remote maintenance connections MUST be disconnected after remote access.

It MUST be ensured that remote maintenance software is only installed on IT systems where it is needed.

Remote maintenance connections via untrusted networks MUST be encrypted. All other remote maintenance connections SHOULD be encrypted.

OPS.1.2.5.A4 ELIMINATED (B)

This requirement has been eliminated.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

OPS.1.2.5.A5 Use of Online Services (S)

Organisations SHOULD define the circumstances in which online services for remote maintenance may be used where the connection is established via an external service provider. The use of such services SHOULD generally be limited to as few cases as possible. IT systems SHOULD not establish automated connections to the online service. It SHOULD be ensured that the online service used performs end-to-end encryption on the transmitted information.

OPS.1.2.5.A6 Drawing Up a Policy for Remote Maintenance (S)

Organisations SHOULD draw up a policy on remote maintenance in which all the relevant regulations are documented. The policy SHOULD be known to all persons in charge who are involved the conception, setup, and performance of remote maintenance.

OPS.1.2.5.A7 Documentation During Remote Maintenance (S)

Remote maintenance SHOULD be documented appropriately. The documentation SHOULD include the remote maintenance access points that exist and whether they are activated. The documents SHOULD be stored in suitable locations and protected from unauthorised access. The documents SHOULD be available within the framework of business continuity management.

OPS.1.2.5.A8 Secure Protocols for Remote Maintenance (S)

Only communication protocols classified as secure SHOULD be used. Secure cryptographic procedures SHOULD be used for this purpose. The strength of the cryptographic procedures and keys used SHOULD be checked at regular intervals and adjusted as necessary.

If the remote maintenance access points of IT systems in an internal network are accessed via a public data network, a secured virtual private network (VPN) SHOULD be used.

OPS.1.2.5.A9 Selection and Acquisition of Suitable Remote Maintenance Tools (S)

Suitable remote maintenance tools SHOULD be selected based on the operational, security-related, and data protection requirements of the organisation in question. All procurement decisions SHOULD be coordinated with the persons in charge of the systems and applications and the Chief Information Security Officer.

OPS.1.2.5.A10 Management of Remote Maintenance Tools (S)

Organisational management processes describing how to handle the selected tools SHOULD be established. Operating instructions describing how to use these remote maintenance tools SHOULD be available. In addition to general training, model procedures for passive and active remote maintenance SHOULD be established and communicated. In addition to general training, the IT Operation Department SHOULD be made specifically aware of and trained in using remote maintenance tools. A contact person SHOULD be appointed for all technical issues related to remote maintenance tools.

OPS.1.2.5.A11 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.2.5.A12 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.2.5.A13 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.2.5.A15 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.2.5.A16 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.2.5.A17 Authentication Mechanisms for Remote Maintenance (S)

For remote maintenance, multi-factor methods SHOULD be used for authentication. The selection of the authentication method and the reasons on which this selection was based SHOULD be documented. Remote maintenance access SHOULD be considered in an organisation's identity and authorisation management efforts.

OPS.1.2.5.A18 ELIMINATED (S)

This requirement has been eliminated.

OPS.1.2.5.A19 Remote Maintenance by Third Parties (S)

If remote maintenance is carried out by external parties, all related activities SHOULD be supervised by internal staff. All remote maintenance processes performed by third parties SHOULD be recorded. Contractual arrangements MUST be made with external maintenance

personnel regarding the security of the IT systems and information concerned. If a service provider performs remote maintenance for several clients, it MUST be ensured that the networks of its clients are not connected. The duties and qualifications of external maintenance personnel SHOULD be specified in a contract.

Remote maintenance interfaces SHOULD be configured in such a way that it is only possible for the service provider to access the IT systems and network segments needed for their work.

OPS.1.2.5.A20 Remote Maintenance Operations (S)

A reporting process for support and remote maintenance concerns SHOULD be established.

Mechanisms for detecting and thwarting high-volume attacks, TCP state exhaustion attacks, and attacks at the application level SHOULD be implemented.

All remote maintenance processes SHOULD be logged.

OPS.1.2.5.A21 Creation of a Business Continuity Plan in Case of Remote Maintenance Failure (S)

A plan SHOULD be developed to minimise the consequences of a failure of remote maintenance components. This SHOULD specify how to react in case of a failure. The contingency plan SHOULD ensure that disruptions and damage (both immediate and consequential) are minimised. It SHOULD also specify how normal operations can be resumed in a timely manner.

OPS.1.2.5.A24 Securing Integrated Remote Maintenance Systems (S)

When procuring new IT systems, it SHOULD be checked whether these IT systems or their individual components have functions for remote maintenance. If these functions are not used, they SHOULD be disabled. The functions SHOULD also be disabled if they are compromised by known security vulnerabilities.

If remote maintenance functions integrated into the firmware of individual components are used, their functions and access to them SHOULD be restricted to the greatest extent possible. The remote maintenance functions SHOULD only be accessible from a separate management network.

OPS.1.2.5.A25 Decoupling of Communication During Remote Maintenance (S)

Direct remote maintenance access to an IT system by an administrator from a remote maintenance client outside the corresponding management networks SHOULD be avoided. If such access is necessary, the communication SHOULD be decoupled. Jump servers SHOULD be used for this purpose. Access to jump servers SHOULD only be possible from trusted IT systems.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

OPS.1.2.5.A14 Dedicated Clients for Remote Maintenance (H)

For remote maintenance, IT systems SHOULD be used which are designed exclusively for the administration of other IT systems. All other functions on these IT systems SHOULD be disabled. The network communication of the administration systems SHOULD be restricted in such a way that only connections to IT systems that are to be administered are possible.

OPS.1.2.5.A22 Redundant Communication Links (H)

Redundant communication links SHOULD be established for remote maintenance access. Organisations SHOULD provide connections for out-of-band management.

OPS.1.2.5.A23 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

In its publication “Grundregeln zur Absicherung von Fernwartungszugängen” [Basic Rules for Securing Remote Maintenance Access], the Federal Office for Information Security describes how remote maintenance access can be kept secure.

In its publication “Fernwartung im industriellen Umfeld” [Remote Maintenance in Industrial Environments], the Federal Office for Information Security describes how remote maintenance access can be kept secure in an industrial environment.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module OPS.1.2.5 *Remote Maintenance*.

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.40 Denial of Service

OPS.1.2.6 NTP Time Synchronisation

1. Description

1.1. Introduction

Networked IT systems often require synchronous states. In most cases, the time serves as a reference. However, the internal clocks of IT systems can deviate from the actual time. The Network Time Protocol (NTP) is used to regularly determine a reference time of central timers via network connections and to adjust internal clocks accordingly.

In networks, precise time synchronisation makes it possible to apply uniform time stamps to information—in order to arrange data chronologically, compare data, or limit access rights, for example. This is the only way to achieve things like correlating time sequences from log data of different IT systems. Accurate time information is also important in the field of cryptographic protocols. Furthermore, synchronising all timers accurately is essential in OT networks.

NTP clients obtain time information from NTP servers. NTP servers can in turn obtain time information from other NTP servers as NTP clients. This creates a hierarchical time distribution (in “strata”). At the top are NTP servers that obtain their time from precise sources (e.g. an atomic clock or a GPS or DCF77 receiver). These NTP servers are called stratum-1.

The NTP service uses methods to determine the deviation of a system clock from external time sources even in the case of deviating responses from different time sources. For example, it ignores time information from a source that suddenly deviates significantly from its own system time.

Control messages allow clients to request status information or change the behaviour of an NTP server, including across the respective network.

NTP messages are usually transmitted in an unsecured form. NTP does, however, offer the option to protect a message with cryptographic keys so that the message cannot be changed without authorisation.

1.2. Objective

The aim of this module is to secure NTP servers and clients in such a way that the IT systems in a given information domain can reliably determine the time and adjust their clocks accordingly.

1.3. Scoping and Modelling

OPS.1.2.6 *NTP Time Synchronisation* must be applied to every IT system that uses NTP in the information domain at hand.

In order to create an IT-Grundschutz model for a specific information domain, all the modules must be considered in their entirety. As a rule, several modules must be applied to a given topic or target object.

This module covers:

- Planning for the use of the NTP protocol
- Operation of NTP servers
- Operation of NTP clients

The following content is also significant, but dealt with elsewhere:

- General requirements for the operation of servers (see SYS.1.1 *General Server*)
- General requirements for the operation of clients (see SYS.2.1 *General Client*)

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module OPS.1.2.6 *NTP Time Synchronisation,* the following specific threats and vulnerabilities are of particular importance.

2.1. Insufficient Planning of the Use of NTP

As a result of insufficient planning, all IT systems may not receive a sufficiently accurate system time.

If the manner in which IT systems can adjust their system time is not properly planned, faulty time information can arise in applications. In particular, time-critical applications may enter faulty states or fail as a result.

In one example, a network may be segmented in such a way that NTP servers and clients can no longer communicate with each other. In addition, insufficient planning of time synchronisation can lead to automated processes being executed at the wrong time (for instance).

2.2. Missing or Incorrect Time Information

NTP servers can fail or transmit incorrect time information.

If an IT system can no longer reach its NTP servers because they have failed or are unreachable, it will no longer be able to adjust its system time. As a result, the system's internal clock time can become inaccurate.

If an NTP server transmits faulty time information to NTP clients, they may adjust their system clocks incorrectly. As a result, incorrect time information may be used in applications—for example, in log data.

Incorrect time information can also cause certificate-based services or services that use one-time passwords to stop working. This will prevent users from logging into affected IT systems or network services.

2.3. Conflicting Time Information

Time information from different sources may be inconsistent.

If an IT system uses multiple NTP servers to adjust its system clock, the time information from these servers may be different. As soon as the time information deviates beyond the corresponding tolerance, the IT system may no longer be able to determine which time information is correct. This may result in the system time being adjusted incorrectly.

2.4. Manipulation of NTP Communication

Network packets with time information can be manipulated.

The NTP protocol is vulnerable to various attacks. For example, an attacker can manipulate time information as it is being transmitted or redirect NTP requests to the attacker's own server. The attacker can thereby manipulate the system time of NTP clients—for example, to use time-restricted access rights even though they have expired.

3. Requirements

The specific requirements of module OPS.1.2.6 *NTP Time Synchronisation* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	None

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

OPS.1.2.6.A1 Planning the Use of NTPs (B)

The IT Operation Department MUST plan where and how NTP is used. This SHOULD be documented fully. In the process, the applications that rely on accurate time information MUST be identified. The requirements of the information domain at hand regarding the accurate time of IT systems MUST be defined and documented.

The IT Operation Department MUST define which NTP servers are to be used by which NTP clients.

Whether the NTP servers are to operate in client-server or broadcast mode MUST be defined.

OPS.1.2.6.A2 Secure Use of External Time Sources (B)

If time information is obtained from an NTP server outside the network of the organisation in question, the IT Operation Department MUST assess whether the operator's NTP server is sufficiently reliable. The IT Operation Department MUST ensure that only NTP servers classified as reliable are used. The IT Operation Department MUST know and observe the operator's usage regulations.

OPS.1.2.6.A3 Secure Configuration of NTP Servers (B)

The IT Operation Department MUST configure the NTP server in such a way that clients can only change NTP server settings if this is explicitly intended. Furthermore, it MUST be ensured that only trusted clients can request status information.

If the respective organisation's internal NTP servers do not use sufficiently accurate time sources themselves, the IT Operation Department MUST configure these NTP servers to regularly request accurate time information from external NTP servers.

OPS.1.2.6.A4 Failure to Account for Unsolicited Time Information (B)

The IT Operation Department MUST configure all NTP clients to discard unsolicited time information received from other IT systems.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

OPS.1.2.6.A5 Use of Client-Server Mode for NTP (S)

The IT Operation Department SHOULD configure all IT systems to use the NTP service in client-server mode. NTP servers SHOULD only send time information to clients when they actively request it.

OPS.1.2.6.A6 Monitoring of IT Systems Using NTP (S)

The IT Operation Department SHOULD monitor the availability, capacity, and system time of internal NTP servers.

The IT Operation Department SHOULD configure IT systems that synchronise their time via NTP to log the following events:

- Unexpected restarts of the IT system
- Unexpected restarts of the NTP service
- Errors related to the NTP service
- Unusual time information

If an NTP server regularly sends time information on its own (broadcast mode), the IT Operation Department SHOULD monitor the NTP clients to see if they receive unusual time information.

OPS.1.2.6.A7 Secure Configuration of NTP Clients (S)

The IT Operation Department SHOULD define which time information an IT system should use when it has been restarted. The IT Operation Department SHOULD define which time information an IT system should use when its NTP service has been restarted.

The IT Operation Department SHOULD determine how NTP clients will react to significantly deviating time information. In particular, a decision SHOULD be taken as to whether strongly deviating time information will be accepted by NTP servers after a system restart. The IT Operation Department SHOULD set limits for time information that deviates significantly.

The IT Operation Department SHOULD ensure that NTP clients will still receive sufficient time information even if an NTP server asks them to send fewer requests (or none at all).

OPS.1.2.6.A8 Use of Secure Time Synchronisation Protocols (S)

The IT Operation Department SHOULD check whether secure protocols can be used for time synchronisation (e.g. Network Time Security, NTS). Secure protocols SHOULD be used whenever possible.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

OPS.1.2.6.A9 Sufficient Availability of Accurate Time Sources (H)

If accurate system times are of significant importance, an organisation SHOULD have multiple stratum-1 NTP servers on its network. The IT systems of an information domain with an NTP service SHOULD use stratum-1 NTP servers directly or indirectly as a time reference. The stratum-1 servers SHOULD each have different time sources.

OPS.1.2.6.A10 Internal NTP Servers Only (H)

Each IT system in an information domain with an NTP service SHOULD receive its time information exclusively from NTP servers within the respective organisation's network.

OPS.1.2.6.A11 Redundant NTP Servers (H)

IT systems for which the accuracy of the system time is of significant importance SHOULD obtain their time information from at least four independent NTP servers.

OPS.1.2.6.A12 NTP Servers with Authenticated Information (H)

NTP servers SHOULD authenticate themselves to clients when communicating. This SHOULD also apply to the servers from which NTP servers receive their own time information. NTP clients SHOULD only accept authenticated NTP data.

4. Additional Information

4.1. Useful Resources

No further information is available for module OPS.1.2.6 *NTP Time Synchronisation*.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module OPS.1.2.6 *NTP Time Synchronisation*:

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.40 Denial of Service

G 0.46 Loss of Integrity of Sensitive Information

OPS.2.1 Outsourcing for Customers

1. Description

1.1. Introduction

Within the framework of outsourcing, organisations (outsourcing customers) outsource business processes and services entirely or partially to external service providers (outsourcing service providers). Outsourcing can involve the use and operation of hardware and software. A service can be provided on the customer's premises or at an external operating facility of the outsourcing service provider. Typical examples involve the operation of a data centre, an application, or a web site. Outsourcing is a generic term that is often supplemented by other terms such as "hosting", "housing", or "colocation".

Regardless of what is outsourced, every outsourcing arrangement binds the customer to the external service provider and the quantity and quality of its services. For the customer in particular, this relationship is associated not only with opportunities, but also with considerable risks. These include a high degree of dependency and the loss of in-house knowledge, as well as of ways to control and guide operations. Information security aspects must therefore be taken into consideration appropriately at every stage of an outsourcing arrangement.

1.2. Objective

This module seeks to ensure that all the security objectives of a given outsourcing customer are still met after its business processes or services have been handed over to an outsourcing service provider. The agreed security level should be consistently maintained or improved regardless of outsourcing. Outsourcing must not result in any uncontrollable risks for the outsourcing organisation with regard to information security. The focus of this module consists of requirements that outsourcing customers should consider and meet during every phase of an outsourcing project.

1.3. Scoping and Modelling

Module OPS.2.1 *Outsourcing for Customers* must be applied separately from the user perspective to each outsourcing service provider that provides services to one or more of a given customer's target objects.

This module includes threats and security requirements from the outsourcing customers' point of view and is limited to the requirements regarding the protection of information on the part of the outsourcing organisation.

Transmission paths to outsourcing service providers are not covered here.

The use of cloud services is dealt with in module OPS.2.2 *Cloud Usage*. Module OPS.2.1 *Outsourcing for Customers* module is not applicable to such cases.

Module OPS.2.1 *Outsourcing for Customers* also does not apply to service providers (such as porter services or cleaning staff) that perform tasks on behalf of a customer without assuming responsibility for a target object. Since these service providers nevertheless have access to target objects, they must be integrated into the customer's security concept in line with IT-Grundschutz. This integration is to be carried out at the requirement level—that is, via the requirements for third-party personnel, gatekeepers, security services, and cleaning staff as found in modules ORP.2 *Personnel* and INF.1 *Generic Building*, for example.

2. Threat Landscape

For module OPS.2.1 *Outsourcing for Customers*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Rules Regarding Information Security

Within the framework of an outsourcing project, large amounts of information are typically transmitted between the customer and the outsourcing service provider. Depending on the protection needs of the information to be processed, insufficient rules on information security may result in security issues. The spectrum of inadequate rules ranges from unclear responsibilities and control functions to guidelines that are incomprehensible, incoherently formulated, or simply not in place.

2.2. Incorrect Administration of Site, System and Data Access Rights

Depending on the outsourcing project in question, an outsourcing service provider's employees may require site, system, and data access rights for IT systems, information, buildings, or rooms on the customer side. These rights may be inappropriately assigned, managed, and controlled, and in extreme cases may even result in rights being granted without authorisation. In addition, the necessary protection of the outsourcing customer's information can no longer be guaranteed. For example, it is a serious security risk to grant uncontrolled administrative authorisations to employees of an outsourcing service provider. These employees may exploit the authorisations and copy or manipulate sensitive information.

2.3. Inadequate testing and approval procedures

If an outsourcing customer has not defined any appropriate requirements regarding testing and approval procedures for its outsourcing service provider, existing errors in hardware and software or vulnerabilities in configurations might not be detected in time (or at all). This shortcoming may make it impossible to guarantee the necessary protection of the outsourcing customer's information. Testing may reveal that new components or updates will significantly change workflows or require more resources (such as increased main memory or processor capacity) to achieve an acceptable processing speed. If the customer is not informed of this in good time, it can lead to a significant waste of investment or the need to make a significant additional investment.

2.4. Inadequate contractual arrangements with outsourcing service providers

Inadequate contractual arrangements with an outsourcing service provider may result in multiple and even severe security issues. If tasks, performance parameters or efforts have been described insufficiently or ambiguously, security safeguards may not be implemented due to ignorance or lack of resources. This can lead to multiple negative consequences—for example, if regulatory requirements and duties are not fulfilled or information obligations and laws are not observed.

2.5. Insufficient terms for the end of an outsourcing project

Problems can arise if there are insufficient and inappropriate arrangements for the termination of an outsourcing contract by the outsourcing customer. There is thus a risk that the outsourcing customer will find it difficult to break away from its outsourcing service provider. This can also happen the other way around, where the customer is forced to select an unsuitable new outsourcing service provider because the previous service provider had the option to terminate their agreement on short notice. In both cases, it may be difficult or impossible to transfer the outsourced area to another service provider or reintegrate it into the customer’s own organisation. Attempting to do so can create a wide variety of security problems. During the termination process, for example, data and systems might be considered “legacy systems” and no longer be protected adequately. If inadequate regulations are established on deleting data files and data backups, confidential data could be leaked to third parties.

2.6. Dependency on an Outsourcing Service Provider

If an organisation decides to outsource part of its operations, it makes itself dependent on its outsourcing service provider. This dependency entails the risk that knowledge may be lost and the outsourced processes and components can no longer be fully controlled. In addition, the protection needs of outsourced business processes and information could be assessed differently. This can lead to the implementation of security safeguards that are inappropriate for the protection needs at hand. Outsourcing customers often entrust entire business processes to outsourcing service providers. An outsourcing service provider can thereby gain complete control of business processes involving sensitive information, resources and IT

systems. At the same time, the outsourcing customer's knowledge of these areas decreases. As a consequence, it is possible that the outsourcing customer will no longer notice deficits in information security. This situation could be exploited by the outsourcing service provider in the form of drastically increased prices or a lower quality of service.

2.7. Disruption of the Office Atmosphere due to an Outsourcing Project

Employees of an outsourcing organisation frequently see outsourcing projects as a negative change. This often results in a poor working atmosphere. The outsourcing customer's employees may fear, for example, that their tasks will change to their disadvantage or that internal jobs will be cut as a result of the outsourcing. If employees have a negative attitude towards an outsourcing project, they may unintentionally or wilfully neglect security safeguards, boycott the project, or even commit acts of revenge. In addition, this could prompt those with specific expertise (such as the head of IT or the IT Operation Department) to give notice during the introduction phase so that the outsourcing project cannot be implemented as planned.

2.8. Inadequate Information Security in the Early Stages of Outsourcing

The introduction phase of outsourcing projects is frequently characterised by tight schedules and budgets. This can mean that security checks and audits are not carried out. Reviews and other quality assurance measures, such as the creation of a security concept, may also be skipped. Transitional safeguards with security shortcomings may become routine over the course of time and are then often maintained for many years due to resource bottlenecks. This comes with the risk that an overall project atmosphere could set in that will give rise to serious additional security shortcomings.

2.9. Failure of an Outsourcing Service Provider’s Systems

If an outsourcing service provider's IT systems and processes fail partially or completely, this will also impact its customers. Problems may also arise if clients are not sufficiently separated on the provider side. Under some circumstances, the failure of a system not assigned to a given outsourcing customer may nonetheless prevent that customer from using a contractually stipulated service. Similar problems arise when the connection between an outsourcing service provider and one of its customers fails.

2.10. Vulnerabilities in the Connection to an Outsourcing Service Provider

If, within the framework of an outsourcing project, the IT connection between the outsourcing service provider and the outsourcing customer is insufficiently secured, the confidentiality and integrity of the data transmitted may be threatened. Open or poorly secured interfaces can allow external unauthorised access to the systems of the organisations involved.

2.11. Lack of Multi-Client Capability with the Outsourcing Service Provider

Outsourcing service providers normally have numerous different customers that rely on the same resources, such as IT systems, networks, or personnel. If the IT systems and data of the different customers are not separated with a sufficient level of security, there is the risk that a customer may access the area of another. In addition, conflicts of interest could arise for the outsourcing service provider if it has to fulfil comparable demands on its resources in parallel. If the respective customers are also competitors, this can be particularly problematic.

3. Requirements

The specific requirements of module OPS.2.1 *Outsourcing for Customers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner, Procurement Department, Central Administration, BCM Officer, Human Resources Department

3.1. Basic Requirements

For module OPS.2.1 *Outsourcing for Customers*, the following requirements MUST be met as a matter of priority:

OPS.2.1.A1 Specification of Security Requirements for Outsourcing Projects (B)

All the security requirements for an outsourcing project MUST be defined on the basis of an outsourcing strategy. Both outsourcing parties MUST contractually commit to comply with IT-Grundschutz or a comparable level of protection. All interfaces between the outsourcing service provider and the outsourcing customer MUST be identified and corresponding security requirements defined in this regard. The security requirements MUST specify the authorisations (e.g. site, system, and data access rights) that the two parties are to grant to one another.

3.2. Standard Requirements

For module OPS.2.1 *Outsourcing for Customers*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

OPS.2.1.A2 Timely Involvement of Employee Representatives [Central Administration] (S)

Employee Representatives SHOULD be informed of an outsourcing project in good time. Employee Representatives SHOULD be involved from the tender phase onwards. Depending on the outsourcing project in question, the statutory rights of co-determination SHOULD be taken into consideration.

OPS.2.1.A3 Selection of a Suitable Outsourcing Service Provider (S)

A requirements profile containing the security requirements for a given outsourcing project SHOULD be created for selecting an outsourcing service provider. Assessment criteria for the outsourcing service provider and its staff SHOULD also exist. These SHOULD be based on the requirements profile.

OPS.2.1.A4 Contractual Arrangements with the Outsourcing Service Provider (S)

All aspects of an outsourcing project SHOULD be agreed in writing with the outsourcing service provider in question. In addition, all roles and duties of cooperation for the creation, review, and modification of a security concept SHOULD be regulated with the outsourcing service provider (e.g. if personnel changes occur). The rights and obligations of the contractual parties SHOULD be agreed in writing. For the purpose of checking compliance with the requirements at hand on a regular basis, the outsourcing service provider SHOULD enable the outsourcing customer to conduct audits.

OPS.2.1.A5 Establishing an Outsourcing Strategy (S)

A strategy for outsourcing SHOULD be defined. This SHOULD take into account the economic, technical, organisational, and legal framework conditions, as well as the relevant aspects of information security. The business processes, tasks, or applications generally associated with outsourcing SHOULD be clarified. An outsourcing customer SHOULD retain sufficient skills, competencies, and resources to be able to determine and control the information security requirements for each outsourcing project on its own. An outsourcing strategy SHOULD describe the goals, opportunities, and risks of the corresponding outsourcing project.

OPS.2.1.A6 Drawing up a Security Concept for the Outsourcing Project [Process Owner] (S)

An outsourcing customer SHOULD draw up an information security concept based on the associated security requirements for each of its outsourcing projects. Every outsourcing service provider SHOULD also provide an individual security concept for the respective outsourcing project. The two security concepts SHOULD be coordinated. The outsourcing service provider's security concept and its implementation SHOULD be merged into an overall security concept. The outsourcing customer or independent third parties SHOULD regularly check the effectiveness of the security concept.

OPS.2.1.A7 Definition of Possible Communication Partners [Central Administration] (S)

The internal and external communication partners who may transmit and receive specific information about a given outsourcing project SHOULD be defined. There SHOULD be a process that can be used to check the functions of the communication partners on both sides. The admissible communication partners and their respective authorisations MUST always be documented and kept up to date.

OPS.2.1.A8 Provisions for Deploying the Personnel of the Outsourcing Service Provider [Human Resources Department] (S)

The employees of an outsourcing service provider SHOULD be obliged in writing to comply with relevant laws, regulations, and the outsourcing customer's rules. The employees of the outsourcing service provider SHOULD be briefed on their tasks and informed of existing information security regulations in a controlled manner. Deputising rules SHOULD be in place for the employees of the outsourcing service provider. There SHOULD be a controlled process that defines how the outsourcing service provider terminates its contractual relationships with its employees. Third-party personnel of the outsourcing service provider who are used on a short-term or one-off basis SHOULD be treated as visitors.

OPS.2.1.A9 Agreements on Connecting to Outsourcing Partner Networks (S)

Before the network of an outsourcing customer is connected to the network of its outsourcing service provider, all security-relevant aspects SHOULD be agreed in writing. The agreement SHOULD specifically define the areas and services to which the outsourcing service provider will be granted access in the network of the outsourcing customer. The affected areas SHOULD be suitably separated from each other. Compliance with the network connection agreements SHOULD be checked and documented. Contact persons SHOULD be appointed on both sides for organisational and technical questions about the network connection. The required security level SHOULD be ensured and verified with the outsourcing service provider before the network connection to the outsourcing service provider is activated. If there are security issues on one or both sides, it SHOULD be specified who must be informed and what escalation steps are to be initiated.

OPS.2.1.A10 Agreement on the Exchange of Data Between Outsourcing Partners (S)

The security safeguards required for regular exchanges of data with fixed communication partners SHOULD be agreed. Data formats and approaches for the secure exchange of data SHOULD also be defined. There SHOULD be contact persons for organisational and technical problems. Contact persons SHOULD also be named for any security-relevant events that occur when exchanging data with third parties. Availability and response times SHOULD be agreed for data exchanges with third parties. It SHOULD be defined which exchanged data may be used for what purposes.

OPS.2.1.A11 Planning and Maintaining Information Security During Ongoing Outsourcing Operations (S)

An operational concept SHOULD be drawn up which also takes the security aspects of a given outsourcing project into account. The security concepts of the outsourcing partners SHOULD

be regularly checked to ensure that they are up to date and consistent with each other. The status of the security safeguards agreed SHOULD be checked at regular intervals. There SHOULD be regular communication between the outsourcing partners. Proposals for changes and improvements SHOULD be discussed and agreed regularly.

The outsourcing partners SHOULD perform regular joint drills and tests to maintain the established level of security. Information on security risks and how to handle them SHOULD be exchanged between the outsourcing partners at regular intervals. A process SHOULD be a defined to secure the flow of information in case of security incidents that affect the contractual partners in question.

OPS.2.1.A12 Change Management [Process Owner] (S)

Outsourcing customers SHOULD be given sufficient notice of major changes. Outsourcing customers SHOULD regularly request documentation of all significant changes regarding planning, testing, approval, and documentation. Before any changes are made, fallback solutions SHOULD be developed in cooperation with the outsourcing service provider.

OPS.2.1.A13 Secure Migration in Outsourcing Projects (S)

For the migration phase of a given outsourcing project, a security management team consisting of qualified employees of the outsourcing customer and the outsourcing service provider SHOULD be established. For the migration phase, a preliminary security concept SHOULD be drawn up that also considers the test and introduction phase. It SHOULD be ensured that production data is not used as test data in an unprotected manner during the migration phase. All changes SHOULD be documented. Upon completion of the migration, the security concept SHOULD be updated. It SHOULD be ensured that all exceptions are reversed at the end of the migration phase. In the event of changes during the migration phase, the extent to which the contractual basis has to be adapted SHOULD be checked.

OPS.2.1.A14 Contingency Planning for Outsourcing [BCM Officer] (S)

A contingency planning concept for outsourcing SHOULD exist that covers the components of the outsourcing customer and the outsourcing service provider in question, as well as the associated interfaces and communication channels. The contingency planning concept for outsourcing SHOULD specify the responsibilities, contact persons, and processes between the outsourcing customer and the outsourcing service provider. The outsourcing customer SHOULD monitor whether the outsourcing service provider has implemented the business continuity safeguards defined. Outsourcing customers and service providers SHOULD conduct joint emergency drills for this purpose.

OPS.2.1.A15 Organised Termination of an Outsourcing Relationship [Procurement Department] (S)

Contracts with outsourcing service providers SHOULD specify all aspects regarding the termination of the service relationship concerned, including for both planned and unplanned termination. The business of an outsourcing customer SHOULD NOT be affected if its service relationship with its outsourcing service provider is terminated.

All information and data SHOULD be returned to the outsourcing customer upon termination. The outsourcing service provider SHOULD securely delete all related data once this information and data has been returned.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.2.1 *Outsourcing for Customers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

OPS.2.1.A16 Security Vetting of Employees (H)

There SHOULD be contractual agreements with outsourcing service providers that state that the trustworthiness of the personnel deployed will be checked appropriately. To this end, providers and customers SHOULD work together to define corresponding criteria.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for the management of service providers in the ISO/IEC 27001:2013 standard (section A.15.2, “Supplier Service Delivery Management”). DIN ISO 37500:2015-08 provides further information on dealing with service providers under “Guidance on Outsourcing”.

The Information Security Forum (ISF) defines various requirements (SC1) for service providers in “The Standard of Good Practice for Information Security”.

Germany's digital association Bitkom provides information on how business processes can be outsourced to service providers in “Leitfaden Business Process Outsourcing: BPO als Chance für den Standort Deutschland” [Guide to Business Process Outsourcing: BPO as an Opportunity for Germany as a Business Location].

Bitkom has also published guidance on the legal aspects of outsourcing in the "Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis" [Guide to Legal Aspects of Outsourcing in Practice].

The National Institute of Standards and Technology (NIST) lists requirements for service providers in NIST Special Publication 800-53.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are

covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module OPS.2.1 *Outsourcing for Customers*.

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.35 Coercion, Blackmail or Corruption

G 0.42 Social Engineering

OPS.2.2 Cloud Usage

1. Description

1.1. Introduction

In the context of cloud computing, IT services are provided, used, and billed over a network in arrangements that adapt to customers' changing requirements. These services are offered and used solely by means of defined technical interfaces and protocols. The range of the services offered within the framework of cloud computing covers the entire spectrum of information technology, including infrastructure (e.g. computing power, storage space), platforms, and software.

Cloud computing offers many advantages: IT services can be used in a scalable and flexible manner based on one's current needs and billed according to the range of functions, duration of use, and number of users in question. The specialised knowledge and resources of cloud service providers can also be accessed, which frees up internal resources for other tasks. In practice, however, the benefits that organisations expect from cloud use often fail to fully materialise. This is usually because factors critical to success were not sufficiently considered in advance. Cloud services must therefore be strategically planned and (security) requirements, responsibilities, and interfaces carefully defined and agreed. Awareness and understanding of the necessary changes in roles, both on the part of IT operation departments and the users in organisations that utilise cloud services, are also important success factors.

In addition, the topic of cloud governance should be considered when introducing cloud services. Critical areas here include the implementation of multi-client capability, contractual arrangements, ensuring the portability of different services, billing of the services used, monitoring of the rendering of services, security incident management, and numerous aspects of data protection.

1.2. Objective

This module describes requirements that facilitate the secure use of cloud services. It is aimed at all organisations that already use such services or want to use them in the future.

1.3. Scoping and Modelling

Module OPS.2.2 *Cloud Usage* must be applied to all cloud services. If an organisation uses different cloud services providers, the module must be applied once to each provider. The interface between cloud service providers is also covered in this module and must be examined for all cloud services.

Cloud services represent a special form of outsourcing in almost all delivery models, with the exception of on-premise private clouds (see module OPS.2.1 *Outsourcing for Customers*). The threats and requirements described in Module OPS.2.2 *Cloud Usage* are therefore also often frequently applied to outsourcing. However, cloud services have some special features that are only found in this module. Module OPS.2.1 *Outsourcing for Customers* is therefore not applicable to cloud services.

The threats and requirements described in this module apply regardless of the service and delivery model used.

Security requirements with which providers can protect their cloud services are not the subject of this module. Threats and specific security requirements that must be considered relevant due to the connection of a cloud service via corresponding application programming interfaces (APIs) are also not considered in this module.

Differentiation from Conventional IT Outsourcing

When the work, production, or business processes of an organisation are outsourced, they are dealt with completely or partially by external service providers. This is an established part of organisational strategies today. In most cases, conventional IT outsourcing is designed so that all the infrastructure rented is used exclusively by a single customer (single-tenant architecture) even if outsourcing providers usually have several customers. Moreover, outsourcing contracts are most often concluded over longer periods of time.

Using cloud services is similar to conventional outsourcing in many respects, but there are also several differences which have to be taken into account:

- For economic reasons, several users often share a joint infrastructure in a cloud.
- Cloud services are dynamic and thus scalable in both directions within much shorter periods. Cloud-based offerings can thus be adapted more quickly to the user's actual needs.
- The cloud services used are usually controlled by the cloud user via a web interface. This means that the user can automatically tailor the services used to their individual needs.
- The technologies used for cloud computing make it possible to distribute IT services dynamically over multiple locations that can be geographically dispersed, including both within and outside of one's home country.
- The customer can easily manage the services used and their resources via web interfaces or other suitable interfaces, which requires little interaction with the provider.

2. Threat Landscape

For module OPS.2.2 *Cloud Usage*, the following specific threats and vulnerabilities are of particular importance.

2.1. Insufficient Strategy for Cloud Use

Using cloud services in an organisation is a strategic decision. If an organisation lacks a sufficient strategy for cloud use, it may, for example, choose an inappropriate cloud service or provider. The selected cloud service may not be compatible with the organisation's own IT, internal business processes, or protection needs. This can have a negative impact on business processes in organisational, technical, or financial terms. In general, an inadequate strategy for cloud use can result in the associated objectives not being achieved or the corresponding security level falling significantly.

2.2. Dependence on a Cloud Service Provider (Loss of Control)

If an organisation uses external cloud services, it is more or less dependent on the respective cloud service provider. As a result, the organisation may no longer be able to fully control the outsourced business processes or the associated information—or, in particular, their security. Despite possible controls, the organisation also depends at a certain point on the cloud service provider to properly implement the necessary security safeguards. Failure in this regard results in inadequate protection of business processes and business-critical information.

In addition, the use of external cloud services can lead to the loss of knowledge about information security and technology within the organisation. As a result, the organisation may no longer be able to assess whether the protective safeguards taken by the provider are sufficient. This makes it very difficult to change providers, as well. The cloud service provider could also exploit this dependency—for example, to enforce price increases or lower its quality of service.

2.3. Poor Compliance Management When Using the Cloud

When an organisation decides to use a cloud service, the decision usually carries many expectations. For example, employees are hoping for higher performance or greater functionality from outsourced services, while those in charge of the organisation are betting on lower costs. However, a lack of compliance management prior to cloud use can lead to expectations not being met and the service not delivering the desired added value (e.g. in terms of availability).

2.4. Violations of Legal Provisions

Many cloud service providers offer their services in an international environment. They are thus often subject to other national legislation. Cloud customers, meanwhile, frequently only see the advantages associated with cloud computing (e.g. cost advantages) and misjudge the legal framework conditions with regard to aspects such as data protection, information obligations, insolvency law, liability, or information access for third parties. This could result

in violations of applicable policies and guidelines and also compromise the security of outsourced information.

2.5. Cloud Service Providers Offering Inadequate Multi-Client Capability

In cloud computing, different customers usually share a common infrastructure, such as IT systems, networks, and applications. If the resources of the different customers are not separated securely enough, a customer may be able to access the areas of another customer and manipulate or delete information there.

2.6. Inadequate Contractual Arrangements with a Cloud Service Provider

Inadequate contractual arrangements with a cloud service provider may result in a variety of security issues that can be severe. If areas of responsibility, tasks, performance parameters, or efforts are described insufficiently or ambiguously, it is possible that the cloud service provider will not implement security safeguards sufficiently (or at all) due to a lack of resources.

Situations that are not clearly regulated in contracts can also result in disadvantages for the client. For example, cloud service providers often use third-party services to provide their own services. If there are insufficient contractual agreements or if the dependencies between the service provider and third party have not been disclosed, this can also have a negative effect on information security and the service provided to the organisation.

2.7. Lack of Planning of Migrations to Cloud Services

A migration to a cloud service is almost always a critical phase. Poor planning can lead to errors that affect information security within the organisation in question. If, for example, an organisation does not plan properly and recklessly dispenses with a gradual migration, this can lead to considerable problems in practice. Without prior test phases, pilot users, or temporary parallel operation of the existing infrastructure and cloud services, important data can be lost or services can fail completely.

2.8. Inadequate Integration of Cloud Services into an Organisation's Own IT

Cloud services must be adequately integrated into an organisation's IT infrastructure. If the persons in charge do not implement this sufficiently, users may not be able to fully access the cloud services that have been commissioned. The cloud services may thus not deliver the required and agreed performance, or they may not be accessible (or only to a limited extent). This can slow down business processes or cause them to fail altogether. If cloud services are improperly integrated into an organisation's in-house IT, this can also lead to serious vulnerabilities.

2.9. Insufficient Provisions for Termination of Cloud Usage

Inadequate provisions for the potential termination of a cloud usage contract can have serious consequences for an organisation. Experience has shown that this is always particularly problematic if a situation that is critical from the organisation's point of view occurs unexpectedly, such as if its cloud service provider is sold, goes bankrupt, or faces serious security concerns. Without adequate internal precautions and detailed contract provisions, the organisation will have difficulty terminating its contract with the cloud service provider. In this case, it may be difficult (if not impossible) to transfer the outsourced cloud service promptly to another service provider, for example, or to reintegrate it back into the organisation.

Moreover, insufficient regulations regarding data deletion at the end of the contract may lead to unauthorised access to an organisation's information.

2.10. Inadequate Administration Model for Cloud Use

When cloud services are used, it often changes the understanding of roles within the cloud customer’s IT Operation Department. The role of administrators often evolves from conventional system administration into service administration. If this process is not accompanied sufficiently, it can have a negative impact on cloud use—for example, if administrators are not entirely in agreement with the changes or they are insufficiently trained for their new tasks. As a result, the cloud services may not be properly administered and thus only available to a limited extent, or they may fail altogether.

2.11. Insufficient Contingency Planning Concept

An insufficient contingency planning concept can quickly lead to serious consequences when using the cloud. If the cloud service in question or parts of it fail, then failings in the contingency planning concepts of the cloud service provider and in the related interfaces always lead to unnecessarily long downtimes, with corresponding consequences for the client's productivity or services. In addition, poor coordination of emergency scenarios between the client and the service provider may cause gaps in contingency planning.

2.12. Failure in the IT Systems of a Cloud Service Provider

The IT systems, applications, and processes operated by a cloud service provider might fail partially or completely, which will likely impact its customers, as well. If clients are insufficiently separated from each other, even a failed IT system that is not assigned to a given cloud customer can affect that customer's ability to access contractually guaranteed services. Similar problems arise when the connection between the cloud service provider and the customer fails, or when the cloud computing platform in use is successfully attacked.

3. Requirements

The specific requirements of module OPS.2.2 *Cloud Usage* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The

Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner, Data Protection Officer, Top Management, Human Resources Department

3.1. Basic Requirements

For module OPS.2.2 *Cloud Usage*, the following requirements MUST be met as a matter of priority:

OPS.2.2.A1 Drawing Up a Strategy for Cloud Usage [Process Owner, Top Management, Data Protection Officer] (B)

A strategy MUST be established for cloud usage. It MUST define the objectives, opportunities, and risks that a given organisation associates with cloud use. In addition, the legal and organisational framework conditions and the technical requirements arising from the use of cloud services MUST be examined. The results of this investigation MUST be documented in a feasibility study.

The services to be purchased from a cloud service provider in the future MUST be documented along with the chosen delivery model. In addition, it MUST be ensured that all fundamental aspects of technical and organisational security are sufficiently considered in the planning phase for cloud use.

A rough individual security analysis SHOULD be carried out for the planned cloud service. This SHOULD be repeated if technical and organisational framework conditions change significantly. For larger cloud projects, a roadmap SHOULD also be developed to determine when and how a cloud service will be deployed.

OPS.2.2.A2 Drawing Up a Security Policy for Cloud Usage [Process Owner] (B)

A security policy for cloud usage MUST be created based on an organisation's strategy for cloud usage. It MUST include specific security requirements for implementing cloud services within the organisation. It MUST also document specific security requirements for the cloud service provider and the defined level of protection for cloud services in terms of confidentiality, integrity and availability. If cloud services from international providers are used, the special country-specific requirements and legal regulations at hand MUST be taken into account.

OPS.2.2.A3 Service Definition for Cloud Services by the Customer [Process Owner] (B)

Cloud customers MUST develop a service definition for each cloud service they intend to use. All the cloud services planned and used SHOULD also be documented.

OPS.2.2.A4 Definition of Areas of Responsibility and Interfaces [Process Owner] (B)

Based on their service definitions for cloud services, cloud customers MUST identify and document all the interfaces and responsibilities relevant to cloud usage. The differentiation between the responsibilities of a given customer and its cloud service provider MUST be clearly evident.

3.2. Standard Requirements

For module OPS.2.2 *Cloud Usage*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

OPS.2.2.A5 Planning a Secure Migration to a Cloud Service [Process Owner] (S)

Before migrating to a cloud service, cloud customers SHOULD draw up a migration concept. To this end, organisational regulations and the distribution of tasks SHOULD first be defined. In addition, existing business processes that will be affected by the planned cloud usage SHOULD be identified and adjusted accordingly. It SHOULD be ensured that an organisation's own IT is sufficiently considered in the migration process. Those in charge SHOULD also determine whether the organisation's employees should receive additional training.

OPS.2.2.A6 Planning the Secure Integration of Cloud Services (S)

Before using a cloud service, organisations SHOULD carefully plan how it is to be integrated into their IT. For this purpose, they SHOULD check (at minimum) whether adaptations of interfaces, network connections, or the administration and data management models at hand are necessary. The results SHOULD be documented and updated at regular intervals.

OPS.2.2.A7 Drawing Up a Security Concept for Cloud Usage (S)

Cloud customers SHOULD develop a security concept for the use of cloud services based on the security requirements they have identified (see OPS.2.2.A2 *Drawing Up a Security Policy for Cloud Usage*).

OPS.2.2.A8 Careful Selection of a Cloud Service Provider [Top Management] (S)

Cloud customers SHOULD create a detailed requirements profile for their future cloud service provider based on their service definition of the cloud service they intend to use. A service specification and a requirements specification SHOULD be drawn up. Supplementary sources of information SHOULD also be used to assess cloud service providers. The service descriptions available from cloud service providers SHOULD also be carefully examined and reviewed.

OPS.2.2.A9 Contractual Arrangements with the Cloud Service Provider [Top Management] (S)

The contractual provisions between cloud customers and cloud service providers SHOULD be adapted in terms of their type, scope, and level of detail to the protection needs of the information to be used in the cloud. The location in which the cloud service provider renders its services SHOULD be specified. In addition, escalation levels and communication channels

SHOULD be defined between a given organisation and its cloud service provider. The manner in which the organisation's data should be securely deleted SHOULD also be agreed. Termination provisions SHOULD also be established in writing. Cloud service providers SHOULD disclose all the subcontractors they require to provide their service.

OPS.2.2.A10 Secure Migration to a Cloud Service [Process Owner] (S)

An organisation's migration to a cloud service SHOULD take place on the basis of its established migration concept. Whether its security concept for cloud usage needs to be adapted to potential new requirements SHOULD be checked during the migration. All preventive safeguards for emergencies SHOULD also be complete and up to date.

The migration to a cloud service SHOULD first be verified in a test run. Once the cloud service has gone live, it SHOULD be checked whether the cloud service provider meets the cloud customer's defined requirements.

OPS.2.2.A11 Drawing Up a Contingency Concept for a Cloud Service (S)

Cloud customers SHOULD create a contingency concept for the cloud services they use. It SHOULD contain all the necessary information about responsibilities and contact persons. In addition, detailed rules SHOULD be drawn up for backups. The specifications for redundant management tools and interface systems SHOULD also be recorded.

OPS.2.2.A12 Maintaining Information Security During Live Cloud Operations (S)

Cloud customers SHOULD regularly update all the documentation and policies they have created for the cloud services in use. Cloud customers SHOULD also periodically check whether their cloud service providers are rendering the contractually guaranteed services. Cloud service providers and their customers SHOULD also coordinate regularly if possible. Plans SHOULD be made and drills carried out on how to respond to system failures.

OPS.2.2.A13 Evidence of Sufficient Information Security for Cloud Usage (S)

Cloud customers SHOULD have their cloud service providers regularly prove that the agreed security requirements are being met. Such evidence SHOULD be based on an internationally recognised set of rules (e.g. IT-Grundschutz, ISO/IEC 27001, Compliance Control Catalogue (C5), Cloud Controls Matrix of the Cloud Security Alliance). Cloud customers SHOULD check whether the scope and protection needs cover the cloud services used.

If a cloud service provider uses subcontractors to provide its cloud services, it SHOULD regularly demonstrate to its cloud customers that they are performing the necessary audits.

OPS.2.2.A14 Orderly Termination of a Cloud Service Relationship [Process Owner, Top Management] (S)

If a cloud customer terminates its service relationship with a cloud service provider, it SHOULD ensure that this will not interfere with its business operations or processes. Contracts with cloud service providers SHOULD regulate how the service relationship in question can be terminated in an orderly manner.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.2.2 *Cloud Usage* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

OPS.2.2.A15 Ensuring the Portability of Cloud Services [Process Owner] (H)

Cloud customers SHOULD define all the requirements necessary to change cloud service providers or bring the cloud service or data back into their own IT infrastructure. Cloud customers SHOULD also conduct regular portability tests. Contracts with cloud service providers SHOULD include specifications to ensure the necessary portability.

OPS.2.2.A16 Implementing In-House Backups [Process Owner] (H)

Cloud customers SHOULD check whether they should create their own data backups in addition to the contractually specified data backups of their cloud service providers. In addition, they SHOULD create detailed requirements for a backup service.

OPS.2.2.A17 Use of Encryption When Using the Cloud (H)

If data is encrypted by a cloud service provider, the encryption mechanisms and key lengths that may be used SHOULD be contractually agreed. If the customer's own encryption mechanisms are used, suitable key management SHOULD be ensured. The encryption SHOULD take into account any special features of the selected cloud service model.

OPS.2.2.A18 Use of Federation Services [Process Owner] (H)

Customers SHOULD check whether Federation Services are being used in their cloud computing projects.

It SHOULD be ensured that a Security Assertion Markup Language (SAML) ticket only transmits the necessary information to the cloud service provider in question. Authorisations SHOULD be checked regularly so that only authorised users are issued an SAML ticket.

OPS.2.2.A19 Security Vetting of Employees [Human Resources Department] (H)

It SHOULD be contractually agreed with external cloud service providers that appropriate checks will be carried out to ensure that the personnel used are qualified and trustworthy. To this end, providers and customers SHOULD work together to define corresponding criteria.

4. Additional Information

4.1. Useful Resources

In its publication "Cloud Computing Compliance Controls Catalogue (C5)", the BSI describes criteria for assessing the information security of cloud services.

The Cloud Security Alliance (CSA) provides recommendations for the use of cloud services in its “Security Guidance for Critical Areas of Focus in Cloud Computing”.

The National Institute of Standards and Technology (NIST) provides recommendations on the use of cloud services in NIST Special Publication 800-144, “Guidelines on Security and Privacy in Public Cloud Computing”.

The European Union Agency for Network and Information Security (ENISA) has published the advanced document "Cloud Computing: Benefits, Risks, and Recommendations for Information Security".

In section SC 2 ("Cloud Computing") of “The Standard of Good Practice for Information Security”, the Information Security Forum (ISF) provides guidelines for the use of cloud services.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module OPS.2.2 *Cloud Usage*.

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.35 Coercion, Blackmail or Corruption

G 0.36 Identity Theft

G 0.41 Sabotage

G 0.45 Data Loss

OPS.3.1 Outsourcing for Service Providers

1. Description

1.1. Introduction

Within the framework of outsourcing, service providers handle business processes and services either in part or entirely on behalf of outsourcing customers. Outsourcing can involve the use and operation of hardware and software, and services can be provided on the outsourcing customer's premises or at an external operating facility of the outsourcing service provider. Typical examples involve the operation of a data centre, an application, or a web site. Outsourcing is a generic term that is often supplemented by other terms such as "hosting", "housing", or "colocation".

Regardless of the services actually taken over, outsourcing requires a close relationship between the service provider and the customer. This means the outsourcing service provider is not insulated from the risks of an outsourcing relationship. In addition, it must implement the risk-mitigating security requirements defined by outsourcing customers (see module OPS.2.1 *Outsourcing for Customers*). This is because it is also in the interest of the outsourcing service provider to provide the agreed service and maintain the agreed security level. If the requirements placed on the outsourcing service provider are not met, there is a risk of high contractual penalties and possibly further legal consequences. Along with financial consequences, this can also cause lasting damage to the provider's reputation.

1.2. Objective

The module describes the requirements that outsourcing service providers must meet in order to provide the level of security demanded by outsourcing customers and avoid uncontrollable risks that might result from these business relationships. This module concentrates on requirements that address the processes of planning, implementing, and controlling information security aspects within the framework of outsourcing from the service provider’s point of view.

1.3. Scoping and Modelling

Module OPS.3.1 *Outsourcing for Service Providers* must be applied from the service provider's perspective to any outsourcing customer that obtains services from an outsourcing provider.

The module contains security requirements that service providers should fulfil when offering outsourcing services.

The protection of transmission channels between service providers and the outsourcing customers is not addressed within the framework of this module.

The use of outsourcing services from the customer's perspective is covered in OPS.2.1 *Outsourcing for Customers*.

2. Threat Landscape

For module OPS.3.1 *Outsourcing for Service Providers*, the following specific threats and vulnerabilities are of particular importance:

2.1. Failure of a Wide Area Network (WAN)

Outsourcing providers that do not render their services on site with customers depend significantly on the availability of wide area networks (WAN). For economic reasons, such services are mostly provided from a few centralised locations. The service provider then connects to the outsourcing customer using these wide area networks. The failure of a wide area network may thus make it impossible to provide outsourced services.

2.2. Insufficient Rules Regarding Information Security

Within the framework of outsourcing, service providers receive and process large amounts of information from outsourcing customers. Depending on the protection needs of the information to be processed, insufficient rules may cause damage (e.g. if the related responsibilities are unclear). For example, the relevant rules and instructions might not be updated in the event of technical, organisational, or personnel changes, such as a change in contact person. The spectrum of inadequate rules ranges from unclear responsibilities and control functions to guidelines that are incomprehensible, incoherently formulated, or simply not in place.

2.3. Incorrect Administration of Site, System and Data Access Rights

Depending on the outsourcing project in question, the employees of the outsourcing customer may need site, system, and data access rights for IT systems, information, buildings, or rooms of the outsourcing service provider. If these rights are poorly assigned, managed, and controlled by the outsourcing service provider, this can lead to far-reaching security problems. If the processes for granting rights are too complex, for example, it may take too long for the employees of the outsourcing customer to obtain urgently needed rights. On the other hand, if the IT Operation Department grants its clients too many rights, they might also access areas of other clients as a consequence.

2.4. Inadequate testing and approval procedures

If an outsourcing service provider has not established sufficient testing and approval procedures for the hardware and software for which they are responsible, it represents a significant threat to IT operations. Existing errors in the hardware and software or security gaps in configurations might not be detected too late (or not at all). If new components are integrated into the operating environment without being tested sufficiently beforehand, errors or security vulnerabilities from the area of one client could also have a negative impact on other customers.

If inadequate testing and approval procedures lead to security incidents, the protection customer data requires is no longer guaranteed. This can have financial consequences if, for example, a contractual relationship is then terminated or contractual penalties have to be paid.

2.5. Insecure transport of files and storage media

Outsourcing service providers often process large amounts of customer data. However, if files, documents, and storage media are not transported in accordance with their protection requirements, both the outsourcing organisation and the outsourcing service provider can suffer considerable damage. This may be the case if information is manipulated en route, can be viewed by unauthorised persons, or is simply lost. This in turn can lead to significant problems in the business relationship between the outsourcing customer and service provider in question.

2.6. Insufficient information security management by the outsourcing service provider

Insufficiently established or inappropriately implemented information security management on the part of an outsourcing service provider entails significant risks. It is problematic, for example, if no one takes overall responsibility for the topic of information security, the provider's executives do not sufficiently support the topic, the strategic and conceptual guidelines are inadequate, or the security process is not transparent. If the outsourcing service provider's overall approach to information security is poorly organised, it runs the risk of not being able to meet the requirements of outsourcing organisations.

2.7. Inadequate contractual arrangements with an outsourcing customer

Inadequate contractual arrangements sometimes result in an outsourcing service provider failing to provide the service required to maintain an outsourcing customer’s level of security. However, if the outsourcing service provider is not sufficiently informed about the protection needs and security requirements of outsourced data or systems, it cannot adequately protect them.

2.8. Insufficient terms for the end of an outsourcing arrangement

If an outsourcing contract does not adequately specify how the contract can be terminated, conflicts may arise when the corresponding business relationship ends. For example, the outsourcing service provider may irrevocably delete the outsourcing customer's information before it has been completely and properly transferred to the customer. If this occurs, it may result in financial penalties for the service provider.

2.9. Inadequate contingency planning for outsourcing

If an outsourcing service provider does not have an adequate contingency planning concept, contractually agreed IT systems and applications might only be available to a limited extent in an emergency, or not at all. As a result, business processes based on these systems and applications may not available and contractually agreed services may not be provided.

2.10. Failure of an outsourcing service provider's systems

If an outsourcing service provider's IT systems and processes fail partially or completely, this will also impact its customers. Problems may also arise if clients are not sufficiently separated on the provider side. Under some circumstances, the failure of a system not assigned to a given outsourcing customer may nonetheless prevent that customer from using a contractually stipulated service. Similar problems arise when the connection between an outsourcing service provider and one of its customers fails.

If corresponding terms were agreed in the contract in question, the customer will then be able to claim damages from the service provider.

2.11. Vulnerabilities in the connection to an outsourcing service provider

If, within the framework of an outsourcing project, the IT connection between the outsourcing service provider and the outsourcing customer is insufficiently secured, the confidentiality and integrity of the data transmitted may be threatened. Open or poorly secured interfaces can also allow external unauthorised access to the systems of the organisations involved.

2.12. Social engineering

Social engineering is a method used to gain unauthorised access to information or IT systems by eavesdropping on employees. It can be used to manipulate employees into performing unauthorised tasks. Employees of outsourcing service providers may be a particularly worthwhile target in this regard because they have access to a wealth of data from different organisations.

2.13. Lack of multi-client capability with the outsourcing service provider

Outsourcing service providers normally have numerous different customers that rely on the same resources, such as IT systems, networks, or personnel. If the IT systems and data of the different outsourcing customers are not separated with a sufficient level of security, there is the risk that one customer may access the area of another. Furthermore, there might be conflicts of interest on the part of an outsourcing service provider if comparable resource requirements must be met simultaneously. If the respective outsourcing customers are also competitors, this can be particularly problematic.

3. Requirements

The specific requirements of module OPS.3.1 *Outsourcing for Service Providers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Organisation, Data Protection Officer, Central Administration, BCM Officer, Human Resources Department, Top Management

3.1. Basic Requirements

For module OPS.3.1 *Outsourcing for Service Providers*, the following requirements MUST be met as a matter of priority:

OPS.3.1.A1 Drawing Up a Rough Concept for the Outsourcing Service (B)

Outsourcing service providers MUST prepare rough concepts for the services they offer. These rough concepts MUST account for the framework conditions of the outsourcing in question, such as special requests. They MUST answer basic questions about the security level and the security requirements of outsourcing customers.

3.2. Standard Requirements

For module OPS.3.1 *Outsourcing for Service Providers*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

OPS.3.1.A2 Contractual Arrangements with Outsourcing Customers (S)

All the aspects of outsourcing projects SHOULD be agreed in writing with the respective outsourcing customers. All responsibilities and duties to collaborate on creating, reviewing,

and changing these aspects (e.g. persons) SHOULD be specified within the framework of each agreement, or also directly in the security concepts between outsourcing service providers and their customers.

OPS.3.1.A3 Creating a Security Concept for the Outsourcing Project (S)

An outsourcing service provider SHOULD have a security concept for its services. For individual outsourcing projects, it SHOULD also establish specific security concepts based on the respective outsourcing customers' security requirements. Common security objectives SHOULD be developed between outsourcing service providers and their customers. A common classification for all sensitive information SHOULD also be established. Regular checks SHOULD be performed to ensure that the applicable security concepts are implemented.

OPS.3.1.A4 Definition of Possible Communication Partners [Central Administration, Data Protection Officer] (S)

The internal and external communication partners who may transmit and receive specific information on a given outsourcing project SHOULD be defined between the outsourcing service provider and the outsourcing customer. It SHOULD be checked at regular intervals whether the communication partners are still working in their respective roles. The corresponding authorisations SHOULD be adapted in the event of changes. Criteria that determine which communication partners may receive which information SHOULD be specified between the outsourcing partners at hand.

OPS.3.1.A5 Provisions for Deploying the Personnel of Outsourcing Service Providers [Human Resources Department] (S)

The employees of an outsourcing service provider SHOULD be instructed regarding their tasks and informed of outsourcing customers' existing information security regulations. Where required, the outsourcing service provider’s employees SHOULD be vetted in accordance with the customer's requirements (e.g. by means of a certificate of good conduct). The employees of the outsourcing service provider SHOULD be obliged in writing to comply with the relevant laws, regulations, confidentiality agreements, and internal provisions. Deputising arrangements SHOULD be implemented in all areas.

OPS.3.1.A6 Procedures Regarding the Use of Third-Party Personnel [Human Resources Department] (S)

If an outsourcing service provider deploys external personnel, its outsourcing customers SHOULD be informed. External employees with responsibilities related to outsourcing SHOULD also be required in writing to comply with relevant laws, regulations, and internal rules. They SHOULD be briefed on their tasks, and in particular on security specifications. Third-party personnel deployed on short notice (or only once) SHOULD be treated as visitors. However, customers' security specifications SHOULD also be taken into account for third-party personnel.

OPS.3.1.A7 Creation of a Client Separation Concept by an Outsourcing Service Provider (S)

A suitable client separation concept SHOULD ensure that the application and data contexts of different outsourcing customers are separated appropriately. Client separation concepts SHOULD be drawn up by outsourcing service providers and made available to their customers. Client separation concepts SHOULD provide sufficient security for the protection needs of outsourcing customers. The necessary client separation mechanisms SHOULD be implemented sufficiently by the outsourcing service provider.

OPS.3.1.A8 Agreements on Connecting to Outsourcing Partner Networks (S)

Before a proprietary network is connected to the network of an outsourcing service provider, all the security-relevant aspects at hand SHOULD be specified in a written agreement. It SHOULD be defined who from one data network may access which areas and services of the other data network. Contact partners SHOULD be appointed on both sides for organisational and technical questions regarding the network connection. All security gaps identified SHOULD be eliminated and the required level of security SHOULD be verifiably achieved before the network connection is activated. In the event of security issues on one or both sides, it SHOULD be specified who must be informed and what escalation steps are to be initiated.

OPS.3.1.A9 Agreement on the Exchange of Data Between Outsourcing Partners (S)

The required security safeguards SHOULD be agreed for the regular exchange of data among fixed communication partners of the outsourcing partners in question. Data formats and a secure form of data exchange SHOULD be defined. Contact persons SHOULD be appointed for organisational and technical questions. Appropriate contact persons SHOULD also be named for security-relevant events that occur when exchanging data with third parties. Availability and response times when exchanging data with third parties SHOULD be agreed. The types of exchanged data that can be used for specific purposes SHOULD also be defined.

OPS.3.1.A10 Planning and Maintaining Information Security During Ongoing Outsourcing Operations (S)

The security concepts of outsourcing partners SHOULD be regularly checked to ensure that they are still up to date and consistent with each other. The status of the security safeguards agreed SHOULD be checked at regular intervals. Outsourcing partners SHOULD cooperate appropriately. They SHOULD also coordinate regularly on changes and improvements.

In addition, outsourcing partners SHOULD perform regular joint drills and tests. Information on security risks and how to handle them SHOULD be exchanged between outsourcing partners at regular intervals. A process SHOULD be a defined to secure the flow of information in case of security incidents that affect the contractual partners in question.

OPS.3.1.A11 Site, System, and Data Access Control [Central Administration] (S)

Site, system, and data access authorisations SHOULD be regulated for the employees of both outsourcing service providers and outsourcing customers. It SHOULD also be specified which authorisations are to be granted to auditors and other inspectors. Rights SHOULD always only

be granted when they are necessary to perform a task. There SHOULD be a controlled procedure for granting, managing, and withdrawing authorisations.

OPS.3.1.A12 Change Management [Organisation] (S)

There SHOULD be policies for making changes to IT components, software, and configuration data. When making changes, the relevant security aspects SHOULD also be considered. All changes MUST be planned, tested, approved, and documented. How and to what extent the changes are documented SHOULD be agreed with outsourcing customers. The documentation SHOULD be made available to outsourcing customers. Fallback solutions SHOULD be developed before changes are carried out. In the event of major security-relevant changes, the information security management department of the outsourcing organisation in question SHOULD already be involved in advance.

OPS.3.1.A13 Secure Migration in Outsourcing Projects (S)

For the migration phase of a given outsourcing project, a security management team consisting of qualified employees of the outsourcing customer and the outsourcing service provider SHOULD be established. A security concept SHOULD be drawn up for the migration phase. Upon completion of the migration, the security concept SHOULD be updated. It SHOULD be ensured that all exceptions are reversed at the end of the migration phase. If there are changes during the migration phase, it SHOULD be checked whether the contractual basis and existing documents need to be adjusted accordingly.

OPS.3.1.A14 Contingency Planning for Outsourcing [BCM Officer] (S)

There SHOULD be a contingency planning concept for outsourcing that comprises the components of the outsourcing customer and the outsourcing service provider in question, as well as the associated interfaces. The contingency planning concept for outsourcing SHOULD specify the responsibilities, contact persons, and processes between the outsourcing customer and the outsourcing service provider. Regular joint emergency drills SHOULD be performed.

OPS.3.1.A15 Orderly Termination of an Outsourcing Relationship [Top Management] (S)

If a contractual relationship with an outsourcing customer is terminated, the business activities of the customer and the outsourcing provider SHOULD NOT be affected. The outsourcing contract with the outsourcing customer SHOULD specify all aspects regarding the termination of the service relationship in question, including for both a planned and an unplanned end of the contractual relationship. The outsourcing service provider SHOULD return all the information and data of the outsourcing customer. The outsourcing service provider SHOULD then securely delete all data belonging to the customer. All authorisations configured within the framework of the outsourcing project in question SHOULD be reviewed and deleted if required.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.3.1 *Outsourcing for Service Providers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

OPS.3.1.A16 Security Vetting of Employees [Human Resources Department] (H)

The trustworthiness of an outsourcing service provider's new employees and external personnel SHOULD be checked with the help of appropriate certificates. To this end, criteria SHOULD be contractually stipulated with outsourcing customers.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for the management of service providers in the ISO/IEC 27001:2013 standard (annex A.15.2, “Supplier Service Delivery Management”). DIN ISO 37500:2015-08 provides further information on dealing with service providers under “Guidance on Outsourcing”.

The Information Security Forum (ISF) defines various requirements (SD1.1, SA2.2, SC1.2, SC2.2, LC1.1, BC1.1) for service providers in “The Standard of Good Practice for Information Security”.

Germany's digital association Bitkom provides information on how business processes can be outsourced to service providers in “Leitfaden Business Process Outsourcing: BPO als Chance für den Standort Deutschland” [Guide to Business Process Outsourcing: BPO as an Opportunity for Germany as a Business Location].

Bitkom has also published guidance on the legal aspects of outsourcing in the "Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis" [Guide to Legal Aspects of Outsourcing in Practice].

The National Institute of Standards and Technology (NIST) lists requirements for service providers in NIST Special Publication 800-53.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module OPS.3.1 *Outsourcing for Service Providers*.

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.33 Shortage of Personnel

G 0.38 Misuse of Personal Information

G 0.41 Sabotage

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

DER.1 Detecting Security-Relevant Events

1. Description

1.1. Introduction

In order to protect IT systems, security-relevant events must be detected and handled in good time. To this end, organisations must plan, implement, and regularly drill appropriate organisational, personnel, and technical safeguards in advance. When an organisation has a defined and tested method to build on, it can shorten its reaction times and optimise its existing processes.

The term "security-relevant event" refers to an event that affects information security or may impair confidentiality, integrity, and availability. Typical consequences of such events involve information being intercepted, manipulated, or destroyed. The reasons for this are manifold. Malware, legacy system infrastructures, or internal attackers can play a role. However, attackers often also capitalise on zero-day exploits—that is, on vulnerabilities in programs that have not yet been patched. Another threat to be taken seriously has to do with Advanced Persistent Threats (APTs). These are targeted cyber attacks on organisations in which an attacker gains permanent access to a network and subsequently extends this access to other IT systems. Such incursions are often difficult to detect and characterised by the very large amount of resources used, as well as significant technical skills on the part of the attackers.

1.2. Objective

This module illustrates a systematic way in which information may be collected, correlated, and evaluated in order to detect security-relevant events as completely and promptly as possible. The findings gained within the framework of detection should then improve an organisation's ability to detect and react appropriately to security-relevant events.

1.3. Scoping and Modelling

Module DER.1 *Detecting Security-Relevant Events* must be applied once to the entire information domain under consideration.

It includes basic specifications that must be considered and met when security-relevant events are detected. These requirements, however, depend on comprehensive logging. The requirements necessary in this regard are not described in this module, but are included in OPS.1.1.5 *Logging*.

When laying the groundwork for the detection of security-relevant events, it is important that responsibilities and competences be clearly defined and assigned. Particular attention should be paid to the principle of separation of duties. This topic is not part of this module; it is covered in module ORP. 1 *Organisation*.

Furthermore, this module does not describe how to handle security-relevant events after they have been detected. Recommendations on this subject are provided in the modules DER.2.1 *Security Incident Handling* and DER.2.2 *Provisions for IT Forensics*. This module also does not address the topic of data protection, which is covered in module CON.2 *Data Protection*.

In order to detect security-relevant events, additional programs are often required, such as anti-virus programs, firewalls, or intrusion detection/prevention systems (IDS/IPS). The security aspects of these systems are not considered in this module. They are addressed, for example, in the modules NET.3.4 *IDS/IPS*, OPS.1.1.4 *Protection Against Malware*, and NET.3.2 *Firewall*.

2. Threat Landscape

For module DER.1 *Detecting Security-Relevant Events*, the following specific threats and vulnerabilities are of particular importance.

2.1. Failure to Consider Statutory Provisions and Occupational Rights of Co-Determination

Programs that detect security-relevant events and evaluate logged data often collect a wealth of information on the network structure and internal processes of an organisation. This may include sensitive information such as personal or confidential data or employee workflows. Since such data can be stored, however, employees' personal rights and rights of co-determination may be violated. Under certain conditions, the organisation may also be in violation of the respective data protection laws.

2.2. Insufficient Employee Qualifications

During the day-to-day operations of an organisation, many failures and errors can occur, such as a sudden, dramatic increase in incoming logged data. If the employees responsible are not sufficiently aware or trained, they may not identify security-relevant events and thus allow an attack to remain unnoticed. Even if the employees are adequately aware of and trained in

issues relating to information security, they may still fail to recognise security incidents. Consider the following examples:

- A user who has not logged on to the organisation's local network for a long time does not think it is abnormal that their laptop has been noticeably slower while accessing the Internet for a week. They do not notice that a malicious program is active in the background. The user was evidently not adequately trained to recognise suspicious activities and inform the Chief Information Security Officer accordingly.
- A production manager does not notice that data in both the production systems and control display systems has been changed in a covert manner. They do not suspect anything when the SCADA controller of a production system displays unusual values because this only happens for a short period of time. The incident is not reported because all the displayed values have returned to normal. As a consequence, no one notices that the display values were manipulated by malware.

2.3. Improper Administration of the Detection Systems Used

Incorrect configurations may prevent detection systems from working properly. If the alarm settings are incorrect, for example, it can lead to more false alarms. This may prevent the employees responsible from differentiating between a false alarm and a security-relevant event. Furthermore, they might not notice messages quickly enough because too many alarms are being generated. Attacks might remain unnoticed as a result. The time required to analyse all the messages will also increase significantly.

2.4. Lack of Information Regarding the Information Domain to be Protected

Not having enough information about the information domain to be protected carries the risk that essential areas of the information domain will not be not protected sufficiently by detection systems. As a consequence, attackers might easily penetrate the respective organisation's network and access sensitive information. They may also stay in the system for extended periods of time and access the network without this being noticed.

2.5. Insufficient Use of Detection Systems

If neither detection systems nor the features available in IT systems and applications for detecting security-relevant events are being used, attackers may penetrate the network of an organisation more easily without this being noticed and access sensitive information without authorisation. Insufficient monitoring of the boundaries between networks is particularly critical.

2.6. Insufficient Personnel Resources

If not enough personnel are available to analyse logged data, security-relevant events may not be detected completely. As a consequence, attacks may remain unnoticed for extended periods of time or only be detected after a large amount of sensitive information has been compromised. If external sources of information are not evaluated due to a lack of sufficient

staff, vulnerabilities may remain open for too long. They may then be exploited by attackers to gain unauthorised access to an organisation's IT systems.

3. Requirements

The specific requirements of module DER.1 *Detecting Security-Relevant Events* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Employee, Process Owner, User, Supervisor

3.1. Basic Requirements

For module DER.1 *Detecting Security-Relevant Events*, the following requirements MUST be met as a matter of priority:

DER.1.A1 Creation of a Security Policy for the Detection of Security-Relevant Events (B)

Based on the general security policy of the organisation in question, a specific security policy MUST be drawn up for detecting security-relevant events. This specific security policy MUST comprehensibly describe requirements and specifications on how to plan, set up, and safely operate methods of detecting security-relevant events. This specific security policy MUST be known to all employees responsible in the field of detection and serve as the basis of their work. If the specific security policy is changed or there are deviations from its requirements, this MUST be agreed and documented with the responsible CISO. The correct implementation of this specific security policy MUST be regularly reviewed. The results of the checks MUST be documented in a meaningful way.

DER.1.A2 Compliance with Legal Conditions When Analysing Log Data (B)

When analysing log data, the provisions of current federal and state data protection law MUST be followed. If detection systems are used, employees' personal rights and rights of co-determination MUST be respected. It MUST also be ensured that all the additional legal provisions that apply are taken into consideration, such as the German Telemedia Act (TMG), the German Works Constitution Act, and the German Telecommunications Act.

DER.1.A3 Definition of Reporting Paths for Security-Relevant Events (B)

Appropriate channels for reports and alerts MUST be defined and documented for security-relevant events. They MUST determine which points of contact must be informed and when. They MUST also specify how the respective persons can be reached. A security-relevant event

MUST be reported using different communication channels depending on the urgency at hand.

All the relevant persons with regard to reporting and alarms MUST be informed of their tasks. All the steps of the reporting and alert process MUST be described in detail. The established reporting and alarm paths SHOULD be reviewed, tested, and updated at regular intervals as required.

DER.1.A4 Raising Employee Awareness [Supervisor, User, Employee] (B)

All users MUST be instructed not to simply ignore or close the event messages displayed by their clients. Each user MUST use the prescribed alert channels to pass on messages to those responsible for incident management (see DER.2.1 *Security Incident Handling*).

Every employee MUST immediately report a security incident they have detected to the incident management department.

DER.1.A5 Use of Detection Features Included in Systems [Process Owner] (B)

If IT systems or applications have features that can be used to detect security-relevant events, these MUST be enabled and used. If a security-relevant event occurs, the messages of the IT systems concerned MUST be evaluated. The logged events of other IT systems MUST be checked, as well. In addition, the collected messages SHOULD be checked randomly at mandatory intervals.

It MUST be checked whether additional malicious code scanners should be installed on central IT systems. If additional malware scanners are used, they MUST allow their messages and logs to be evaluated through a central access point. It MUST be ensured that the malicious code scanners will automatically report security-relevant events to the person responsible. The responsible parties MUST evaluate and investigate these messages.

3.2. Standard Requirements

For module DER.1 *Detecting Security-Relevant Events*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

DER.1.A6 Continuous Monitoring and Analysis of Log Data (S)

All log data SHOULD be actively monitored and analysed as constantly as possible. Employees SHOULD be made responsible for these activities.

If the employees responsible have to actively search for security-relevant events that have occurred (e.g. when testing or monitoring IT systems), such tasks SHOULD be documented in corresponding process instructions.

Sufficient personnel resources SHOULD be made available for detecting security-relevant events.

DER.1.A7 Training of Responsible Persons [Supervisor] (S)

The persons responsible for reviewing event messages SHOULD receive advanced training and qualifications. When new IT components are procured, a budget for training SHOULD be

planned. A training concept SHOULD be created before the responsible staff members receive training on new IT components.

DER.1.A8 ELIMINATED (S)

This requirement has been eliminated.

DER.1.A9 Use of Additional Detection Systems [Process Owner] (S)

The network plan in question SHOULD be used to determine which network segments need to be protected by additional detection systems. Additional detection systems and sensors SHOULD be added to the information domain. Malicious code detection systems SHOULD be used and administered from a central location. The transitions defined in the network plan between internal and external networks SHOULD be complemented by network-based intrusion detection systems (NIDS).

DER.1.A10 Use of TLS/SSH Proxies [Process Owner] (S)

At transitions to external networks, TLS/SSH proxies SHOULD be used to interrupt encrypted connections and make it possible to check the data being transmitted for malware. All TLS/SSH proxies SHOULD be protected against unauthorised access. Security-relevant events SHOULD be detected automatically on TLS/SSH proxies. An organisational regulation SHOULD be drawn up that specifies how log data can be evaluated manually in accordance with the provisions of data protection law.

DER.1.A11 Use of a Central Logging Infrastructure to Evaluate Security-Relevant Events [Process Owner] (S)

Event messages that are generated by IT systems and applications and stored on a central logging infrastructure (see OPS.1.1.5 *Logging*) SHOULD be retrievable using a tool. The selected tool SHOULD be able to analyse the messages. The collected event messages SHOULD be checked for anomalies at regular intervals. The signatures of the detection systems used SHOULD always be identically up to date so that security-relevant events can also be detected retrospectively.

DER.1.A12 Evaluation of Information from External Sources [Process Owner] (S)

External sources SHOULD be used to gain new insights into security-relevant events that could impact an organisation’s own information domain. Messages from different channels SHOULD be recognised as relevant by employees and forwarded to the correct recipients. Information from reliable sources SHOULD be evaluated as a general rule. All information received SHOULD be evaluated in terms of whether it is relevant to the organisation's own information domain. If this is the case, the information SHOULD be escalated in line with security incident handling.

DER.1.A13 Regular Audits of Detection Systems (S)

An organisation's detection systems and safeguards SHOULD be audited regularly to check whether they are still up to date and effective. The values assessed SHOULD include those that indicate how often security-relevant events are recorded, reported, and escalated. The results

of the audits SHOULD be documented transparently and compared against the organisation's goals. Deviations SHOULD be investigated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.1 *Detecting Security-Relevant Events* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

DER.1.A14 Evaluation of Log Data by Specialised Personnel (H)

Employees SHOULD be specially assigned to monitor all types of log data. The monitoring of log data SHOULD be the predominant task of the appointed employees. The appointed employees SHOULD receive specialised further training and qualifications. A group of persons SHOULD be appointed to be exclusively responsible for the evaluation of log data.

DER.1.A15 Central Detection and Real-Time Examination of Event Messages (H)

Central components SHOULD be used to detect and evaluate security-relevant events. Centralised, automated analyses SHOULD be carried out using software tools. These central, automated, software-based analyses SHOULD be used to record and correlate all the events that occur in the system environment at hand. The security-relevant processes SHOULD be transparent. It SHOULD be possible to view and evaluate all the data received in the log administration system in a seamless manner. The data SHOULD be analysed as constantly as possible. If defined threshold values are exceeded, an alarm SHOULD be generated automatically. The corresponding personnel SHOULD make sure that an alarm triggers a qualified response that is appropriate to the situation at hand. In this context, the employee concerned SHOULD also be informed immediately.

The persons in charge of the system SHOULD audit and (if required) adapt the analysis parameters at regular intervals. In addition, data that has already been audited SHOULD be examined automatically for security-relevant events at regular intervals.

DER.1.A16 Use of Detection Systems in Accordance with Protection Requirements (H)

Applications with higher protection needs SHOULD be protected by means of additional detection safeguards. To this end, detection systems SHOULD be used that also make it possible to guarantee that higher protection needs are being met from a technical perspective.

DER.1.A17 Automatic Reaction to Security-Relevant Events (H)

Should a security-relevant event occur, the detection systems used SHOULD automatically report the event and react with appropriate security safeguards. In the process, methods SHOULD be used that automatically detect possible attacks, misuse attempts, or security violations. It SHOULD be possible to automatically intervene in data flows in order to prevent a possible security incident.

DER.1.A18 Performance of Regular Integrity Checks (H)

The integrity of all detection systems SHOULD be checked regularly. User rights SHOULD also be checked. In addition, the sensors in use SHOULD regularly check the integrity of files. An automatic alarm SHOULD be triggered if certain values change.

4. Additional Information

4.1. Useful Resources

The Federal Office for Information Security (BSI) regulates the logging and detection of security-relevant events in its “Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen” [BSI Minimum Standard for Logging and Detection of Cyber Attacks].

On the topic of intrusion detection, the BSI has published the additional document “BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, Version 1.0” [BSI Guidelines for the Introduction of Intrusion Detection Systems, Version 1.0].

In "The Standard of Good Practice for Information Security", the Information Security Forum (ISF) provides guidelines for the use of intrusion detection systems in section TS1.5, "Intrusion Detection Systems".

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module DER.1 *Detecting Security-Relevant Events*.

G 0.18 Poor Planning or Lack of Adaptation

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.40 Denial of Service

G 0.46 Loss of Integrity of Sensitive Information

DER.2.1 Security Incident Handling

1. Description

1.1. Introduction

In order to limit damage and avoid additional ramifications, detected security incidents need to be addressed quickly and efficiently. To this end, it is necessary to establish a specified and tested method for handling security incidents (also referred to as security incident handling or security incident response).

A security incident may have significant effects on an organisation and entail major damage. Examples of such incidents include incorrect configurations that cause confidential information to be disclosed, or criminal acts such as attacks on servers, the theft of confidential information, sabotage, or blackmail associated with IT.

The causes of security incidents are manifold and can include malware, outdated system infrastructures, or internal attackers. Attackers also often take advantage of zero-day exploits—that is, vulnerabilities in programs that have not yet been patched. Another threat to be taken seriously has to do with Advanced Persistent Threats (APTs).

Furthermore, users, administrators, or external service providers may behave incorrectly, such as by changing system parameters in a security-critical manner or violating internal policies. Other plausible causes include violations of access rights, changes in software or hardware, or insufficient protection of sensitive rooms and buildings.

1.2. Objective

The objective of this module is to demonstrate a systematic way of creating a concept for security incident handling.

1.3. Scoping and Modelling

Module DER.2.1 *Security Incident Handling* must be applied once to the entire information domain under consideration.

This module focuses on handling security incidents from the standpoint of information technology. Before security incidents can be handled, however, they must first be recognised. The security requirements related to this are included in module DER.1 *Detecting Security-Relevant Events*, which is a prerequisite of this module. Safeguard required for conducting forensic IT examinations are described in module DER.2.2 *Provisions for IT Forensics*. The process of cleaning up after an ATP incident is covered in module DER.2.3 *Clean-Up of Extensive Security Incidents*. A special area of handling security incidents is business continuity management, which is addressed in module DER.4 *Business Continuity Management* and not considered further here. The present module does, however, cover how to determine whether or not a given situation is an emergency.

2. Threat Landscape

For module DER.2.1 *Security Incident Handling*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inappropriate Handling of Security Incidents

In practice, it is impossible to completely eliminate the possibility of security incidents occurring. This remains the case even when numerous security safeguards are implemented. That said, responding inappropriately to acute security incidents (or not at all) may result in major damage with catastrophic consequences. Consider the following examples:

- Suspicious entries are found in the log files of a firewall. If there is no prompt examination of whether this is the first sign of a possible incursion, attackers may successfully overcome the firewall without being noticed and penetrate the internal network of the respective organisation.
- Security vulnerabilities emerge in the IT systems and applications used by an organisation. If the organisation does not obtain this information in time and fails to take the necessary countermeasures quickly, these vulnerabilities can be exploited by attackers.
- A burglary at a branch office of a company is assumed to be a case of drug-related crime because laptops and flat-screen monitors were the only objects stolen. The fact that confidential information and access data for IT systems in the company's intranet were stored on the laptops was not considered important. The CISO was therefore not informed. As a result, the organisation is not prepared for the subsequent attacks on the IT systems its headquarters and other sites. The data found on the stolen laptops was used for the attacks.

In urgent, high-stress situations, poor decisions may be made if there is no appropriate procedure prescribed for handling security incidents. Such decisions could lead to the press being misinformed, for example. In addition, third parties could be damaged by an organisation’s IT systems and claim compensation. If the affected organisation has not planned fallback or recovery safeguards, the damage it suffers will be significantly greater.

2.2. Destruction of Evidence While Handling Security Incidents

If a security incident is handled carelessly or the applicable specifications are disregarded, important evidence for investigating the incident or pursuing legal action may be unintentionally destroyed or rendered inappropriate for court proceedings.

Consider the following examples:

- An attacker infects a client with malware whose mode of operation and objective can only be analysed when the system is running. For this analysis, information on the active processes and the content of the main memory must be backed up and evaluated. If the client is shut down prematurely, the information can no longer be used to analyse and get to the bottom of the security incident.
- An administrator finds a running process on a server that is causing an extraordinary CPU load. In addition, this process is creating temporary files and sending unknown information over the Internet. If the process is terminated prematurely and the temporary files are simply deleted, it will not be possible to find out whether confidential information has been stolen.
- An important server becomes compromised because the administrator was not able to install the latest security updates as planned due to the heavy load on the server and the lack of a free maintenance window. To avoid any possible disciplinary consequences, the administrator installs the missing updates before a security team is able to analyse the source of the intrusion and the damage resulting from it. A workplace culture with a low tolerance for employee errors has therefore prevented analysis of the problem.

3. Requirements

The specific requirements of this module are listed below. As a matter of principle, the Chief Information Security officer (CISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Process Owner, Data Protection Officer, IT Operation Department, BCM Officer, Top Management

3.1. Basic Requirements

For module DER.2.1 *Security Incident Handling*, the following requirements MUST be met as a matter of priority:

DER.2.1.A1 Definition of a Security Incident (B)

Within an organisation, the meaning of the term “security incident” MUST be clearly defined. A security incident MUST be distinguished from disruptions during day-to-day operations whenever possible. All employees involved in handling security incidents MUST be familiar with the definition of a security incident. The definition and occurrence thresholds of such incidents SHOULD be based on the protection needs of the business processes, IT systems, and applications affected.

DER.2.1.A2 Drawing Up a Policy for Handling Security Incidents (B)

A policy governing the handling of security incidents MUST be prepared. This policy MUST define its purpose and objective and govern all aspects of handling security incidents. It MUST therefore describe codes of conduct for the different types of security incidents. In addition, there MUST be target-group-oriented and practically usable instructions for all employees. Furthermore, the interfaces with other management areas SHOULD be taken into account, including in business continuity management.

All employees MUST be familiar with the policy. It MUST be agreed by the IT Operation Department and approved by the organisation’s Top Management. The policy MUST be reviewed and updated regularly.

DER.2.1.A3 Specification of Responsibilities and Contact Persons in the Event of Security Incidents (B)

It MUST be specified who will be responsible for what in the event of security incidents. The tasks and competencies applicable in the event of security incidents MUST be defined for all employees. In particular, the employees who will handle security incidents MUST be informed of their tasks and competencies. In this context, it MUST be specified who will make the eventual decision regarding a forensic examination, the criteria to be followed in carrying it out, and when this should take place.

The employees MUST know the contact persons for all types of security incident. Contact information MUST always be updated and easily accessible.

DER.2.1.A4 Notification of Entities Affected by Security Incidents [Top Management, IT Operation Department, Data Protection Officer, BCM Officer] (B)

When a security incident occurs, all the internal and external entities affected MUST be informed of the incident promptly. In this process, it MUST be checked whether the Data Protection Officer, the works council and personnel council, and employees from the legal department must be consulted. The reporting duties for public authorities and regulated industries MUST be taken into consideration, as well. Furthermore, it MUST be guaranteed that the entities affected are informed of the actions they need to take.

DER.2.1.A5 Remedial Action in Connection with Security incidents [IT Operation Department] (B)

In order for a security incident to be remedied successfully, the person responsible MUST initially contain the problem and find the cause. They MUST then select the safeguards necessary to fix the problem. The head of the IT Operation Department MUST approve the

safeguards before they are implemented. The cause MUST then be eliminated and a secure state established.

There MUST be a current list of internal and external security experts who may be consulted in the event of security incidents to answer questions from the subject areas involved. Secure communication methods with these internal and external entities MUST be established.

DER.2.1.A6 Recovering the Operating Environment After Security Incidents [IT Operation Department] (B)

After a security incident, the affected components MUST be removed from the network. In addition, all necessary data that could provide information about the nature and cause of the problem MUST be backed up. On all the components affected, the operating systems and all applications MUST be checked for changes.

The original data MUST be reinstalled from write-protected data storage media. In so doing, all security-related configurations and patches MUST also be implemented. If data from backups is reimported, it MUST be ensured that the data was not affected by the security incident. After an attack, all access data on the affected components MUST be changed before they are put back into operation. The components affected SHOULD be subjected to a penetration test before they are used again.

When recovering the secure operating environment, the users MUST be involved in the functional tests of the applications. After everything has been recovered, the components (including the network transitions) MUST be monitored in a targeted manner.

3.2. Standard Requirements

For module DER.2.1 *Security Incident Handling*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

DER.2.1.A7 Establishment of a Procedure for Handling Security Incidents [Top Management] (S)

A suitable procedure SHOULD be established for handling security incidents. The procedures and specifications for different security incidents SHOULD be clearly stipulated and documented appropriately. An organisation's Top Management SHOULD implement the agreed procedure and make it accessible to everyone involved. Regular checks SHOULD be carried out to ensure that the procedure is still up to date and effective. The procedure SHOULD then be amended as required.

DER.2.1.A8 Design of Organisational Structures for Handling Security Incidents (S)

Appropriate organisational structures SHOULD be defined for handling security incidents. A security incident team SHOULD be established with members who may be called in depending on the type of incident. Even if the security incident team only meets when a specific incident has occurred, appropriate members SHOULD be appointed in advance and instructed on how to perform their tasks. Regular checks SHOULD be carried out to ensure

that the composition of the security incident team is still appropriate. Changes SHOULD then be made to the security incident team as required.

DER.2.1.A9 Definition of Reporting Paths for Security Incidents (S)

Reporting channels SHOULD be established that are appropriate to the different types of security incidents. These SHOULD ensure that employees can report security incidents quickly and easily using reliable and trustworthy channels.

If a central contact point for reporting failures or security incidents is established, this SHOULD also be communicated to all employees.

There SHOULD be a communication and contact strategy. This strategy SHOULD specify who must be informed as a matter of principle, who may be informed, who is responsible for handling this and in what order, and the level of detail of the information provided. It SHOULD specify who will pass information about security incidents on to third parties. It SHOULD ensure that no unauthorised persons forward information on security incidents.

DER.2.1.A10 Limiting the Effects of Security Incidents [BCM Officer, IT Operation Department] (S)

During the root cause analysis of a security incident, a decision SHOULD be taken on whether it is more important to contain the damage caused or to resolve the incident. Sufficient information SHOULD be available to be able to estimate the effects of a security incident. For certain security incident scenarios, worst-case considerations SHOULD be undertaken in advance.

DER.2.1.A11 Classification of Security Incidents [IT Operation Department] (B)

A uniform procedure SHOULD be defined for classifying security incidents and disruptions. The classification procedure for security incidents SHOULD be coordinated between security management and fault (incident) management.

DER.2.1.A12 Specification of Where Security Incident Handling Overlaps with Fault Management [BCM Officer] (S)

The interfaces among fault management, business continuity management, and security management SHOULD be analysed. In so doing, resources that these areas could use in tandem SHOULD also be defined.

The employees involved in fault management SHOULD be made aware of issues related to handling security incidents and business continuity management. The security management SHOULD have read-only access to the incident management tools used.

DER.2.1.A13 Integration into Security and Business Continuity Management [BCM Officer] (S)

The handling of security incidents SHOULD also be coordinated with business continuity management. If a special fault management role has already been established in an organisation, this person SHOULD also be involved.

DER.2.1.A14 Escalation Strategy for Security Incidents [IT Operation Department] (S)

An escalation strategy SHOULD be formulated that goes beyond the communication and contact strategy at hand. This escalation strategy SHOULD be coordinated among the persons responsible for fault management and information security management.

It SHOULD contain clear instructions on who is to be involved in what way and when for each type of identifiable or suspected security incident. It SHOULD also specify the safeguards that are to follow an escalation and how those involved are to respond.

Suitable tools (e.g. ticket systems) SHOULD be selected for the defined escalation strategy. These SHOULD also be suitable for processing confidential information. It SHOULD be ensured that the tools will also be available during security incidents and emergencies.

The escalation strategy SHOULD be reviewed regularly and updated as required. The checklists (matching scenarios) for fault management SHOULD be complemented by security-relevant topics and updated regularly. The defined escalation paths SHOULD be tested by means of drills.

DER.2.1.A15 Training Service Desk Employees [IT Operation Department] (S)

Service desk employees SHOULD have appropriate tools at their disposal to enable them to identify security incidents. They SHOULD be sufficiently trained to use the tools themselves. Service desk employees SHOULD be familiar with the protection needs of the IT systems in question.

DER.2.1.A16 Documentation for Remedying Security Incidents (S)

The process of remedying security incidents SHOULD be documented in accordance with a standardised procedure. All actions performed and the respective times SHOULD be documented along with the log data of the components affected. In so doing, confidentiality SHOULD be guaranteed while documenting the information and archiving the reports.

The necessary information SHOULD be entered into the respective documentation systems before the disruption in question is considered over. The necessary quality assurance requirements SHOULD be defined in advance with the CISO.

DER.2.1.A17 Evaluation of Security Incidents (S)

Security incidents SHOULD be evaluated in a standardised manner. This SHOULD examine how quickly security incidents are detected and remedied. It should also investigate whether the reporting channels worked, whether sufficient information was available for evaluation, and whether the detection safeguards were effective. It SHOULD also check whether the implemented safeguards and activities were effective and efficient.

The experience gained from previous security incidents SHOULD be used to develop instructions for comparable security incidents. These instructions SHOULD be announced to the relevant groups of persons and updated at regular intervals on the basis of new findings.

An organisation's Top Management SHOULD be informed of the security incidents at annual intervals. If there is a need for immediate action, the Top Management MUST be informed immediately.

DER.2.1.A18 Further Development of Processes Based on Findings from Security Incidents and Industry Developments [Process Owner] (S)

After a security incident has been analysed, there SHOULD be an investigation of whether the procedures for handling security incidents need to be changed or developed further. All those involved in the incident SHOULD report on their respective experiences.

Whether there are new developments in the field of incident management and forensics and whether these can be incorporated into the respective documents and procedures SHOULD be examined.

If checklists and auxiliary resources are being used (e.g. by service desk members), a check SHOULD be carried out on whether these should be complemented by relevant questions and information.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.2.1 *Security Incident Handling* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

DER.2.1.A19 Specifying Priorities for Handling Security Incidents [Top Management] (H)

Priorities for handling security incidents SHOULD be established in advance and updated regularly. This SHOULD also take into account the classification of security incidents.

The priorities SHOULD be approved and implemented by an organisation’s Top Management. All those with decision authority who are involved in handling security incidents SHOULD be familiar with them. The defined priority classes SHOULD also be stored in an incident management system.

DER.2.1.A20 Creation of a Dedicated Reporting Office for Security Incidents (H)

A dedicated office SHOULD be established for reporting security incidents. It SHOULD be guaranteed that the reporting office is available during normal office hours. However, it SHOULD also be possible for employees to report security incidents outside of normal office hours. The reporting office employees SHOULD be adequately trained and aware of issues related to information security. All information on security incidents SHOULD be treated confidentially within the reporting office.

DER.2.1.A21 Assembling a Team of Experts for Handling Security Incidents (H)

A team of experienced and trusted experts SHOULD be established. Along with technical expertise, the members of the team SHOULD also have competences in the field of

communication. The trustworthiness of the members of the team of experts SHOULD be checked. The composition of the expert team SHOULD be checked regularly and changed as necessary.

The members of the team of experts SHOULD be included in the escalation and reporting channels. The team of experts SHOULD be trained to analyse security incidents in the systems deployed in their organisation. The members of the team of experts SHOULD receive regular training in both the systems used and detecting and responding to security incidents. The team of experts SHOULD have access to any existing documentation and the financial and technical resources required to handle security incidents quickly and discretely.

The expert team SHOULD be appropriately considered and integrated into the organisational structures at hand. The responsibilities of the expert team SHOULD be coordinated in advance with those of the security incident team.

DER.2.1.A22 Reviewing Management System Efficiency in Handling Security Incidents (H)

Regular checks SHOULD ensure that the management system for handling security incidents is still up to date and effective. To this end, both announced and unannounced drills SHOULD be conducted. The drills SHOULD be coordinated in advance with the Top Management of the organisation in question. The parameters that are measured when security incidents are recorded, reported, and escalated (e.g. the time from the initial report to the binding confirmation of a security incident) SHOULD be evaluated.

In addition, simulation exercises SHOULD be conducted on the handling of security incidents.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for handling security incidents in ISO/IEC 27001:2013 “Information technology – Security techniques – Information security management systems – Requirements” (annex A16, “Information security incident management”).

The International Organization for Standardization (ISO) provides guidelines for handling security incidents in the standard ISO/IEC 27035:2016, “Information technology – Security techniques – Information security incident management”.

The National Institute of Standards and Technology (NIST) provides general guidelines for handling security incidents in Special Publication 800-61 (Revision 2), “Computer Security Incident Handling Guide”.

The National Institute of Standards and Technology (NIST) provides specific guidelines for handling malware infections on laptops and desktops in Special Publication 800-83 (Revision 1), “Guide to Malware incident Prevention and Handling for Desktops and Laptops”.

The Information Security Forum (ISF) provides guidelines for handling security incidents in “The Standard of Good Practice for Information Security” (chapter TS1.4, “Technical Security Management; Identity and Access Management”).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module DER.2.1 *Security Incident Handling*.

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

DER.2.2 Provisions for IT Forensics

1. Description

1.1. Introduction

IT forensics involves the strictly methodical data analysis of storage media and data networks that is needed to get to the bottom of security incidents in IT systems.

Forensic investigation of IT security incidents is always necessary to assess damage, avert attacks and prevent them in the future, and identify attackers. Whether or not an IT security incident requires forensic examination is determined whilst handling the incident. In the context of this module, IT forensic examination consists of the following phases:

- Strategic preparation: During this phase, processes are planned and established to ensure that an organisation is able to forensically analyse IT security incidents. It is also required if the organisation does not have its own forensics experts.
- Initialisation: Once the responsible employees have decided to forensically examine an IT security incident, the processes planned in advance are triggered. The examination framework is also specified and the initial measures are implemented.
- Securing evidence: Here, the evidence to be secured is selected, and the data is secured forensically. In this regard, a differentiation is made between live forensics and post-mortem forensics. Live forensics ensures that the affected IT system's volatile data (in terms of network connections or RAM, for example) is secured. During post-mortem forensics, forensic copies of storage media are created.
- Analysis: The collected data is analysed forensically. In this regard, data is considered both individually and in the overall context at hand.
- Presentation of results: The relevant examination results are processed and communicated to meet the needs of specific target groups.

1.2. Objective

This module covers the safeguards required to conduct forensic IT examinations. The main focus is on how to prepare and carry out evidence recovery.

If providers of forensics services secure evidence either partially or entirely on their own, the requirements of this module also apply to them. Contractual arrangements and tests can be used to ensure that a service provider will comply with such requirements.

1.3. Scoping and Modelling

Module DER.2.2 *Provisions for IT Forensics* must be applied once to the entire information domain under consideration.

This module addresses safeguards that are essential for later forensic IT examinations.

The actual performance of forensic analysis is thus not part of this module. It does not describe requirements that are designed to ensure that attacks will be detected. These are included in module DER.1 *Detecting Security-Relevant Events* and are a prerequisite of this module. In addition, this module does not address criteria and processes used by the persons in charge to decide whether an IT security incident must be forensically examined. This decision will be made during the handling of each security incident (see DER.2.1 *Security Incident Handling*).

The module also not cover forensic IT investigations of criminal offences.

Finally, this module does not address how IT infrastructures can be cleaned after being attacked (see DER.2.3 *Clean-Up of Extensive Security Incidents*). The activities described in DER.2.3 can, however, be supported significantly by the results of forensic IT examinations.

2. Threat Landscape

For module DER.2.2 *Provisions for IT Forensics*, the following specific threats and vulnerabilities are of particular importance:

2.1. Violation of legal framework conditions

For IT forensic investigations, all the data deemed necessary is often copied, secured, and evaluated. This typically also includes personal data of employees or external partners. If such data is accessed without justification and without the involvement of the Data Protection Officer, for example, the organisation in question may have violated related legal regulations (e.g. with regard to appropriation). It is also possible that the collected data can be used to deduce how employees behave or establish associations to them. This carries the risk that internal regulations may be violated, as well.

2.2. Failure to Secure Evidence due to Incorrect or Incomplete Methods

If evidence is not secured correctly or quickly enough, this may result in the loss of important data that cannot be recovered later. In the worst case, this will result in a forensic examination that produces no findings. At minimum, however, the value of the evidence will be limited.

The risk of losing important evidence increases significantly if employees use forensic tools incorrectly, secure data too slowly, or practise too little. In addition, evidence often gets lost if the persons in charge do not identify volatile data as relevant and thus fail to secure it.

3. Requirements

The specific requirements of module DER.2.2 *Provisions for IT Forensics* are listed below. As a matter of principle, the Chief Information Security officer (CISO) is responsible for fulfilling the requirements. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Process Owner, Data Protection Officer, Top Management

3.1. Basic Requirements

For module DER.2.2 *Provisions for IT Forensics*, the following requirements MUST be met as a matter of priority:

DER.2.2.A1 Examination of Legal and Regulatory Framework Conditions for Acquisition and Evaluation [Data Protection Officer, Top Management] (B)

If data is acquired and evaluated for forensic examinations, all the legal and regulatory framework conditions MUST be identified and met (see ORP.5 *Compliance Management*). Internal regulations and agreements with employees MUST NOT be violated. To that end, the supervisory/personnel board and the Data Protection Officer MUST be involved.

DER.2.2.A2 Drawing Up a Guide for Initial Measures in Case of an IT Security Incident (B)

A guide MUST be drawn up for the IT systems used that describes the initial measures that must be carried out in the event of an IT security incident in order to destroy as little evidence as possible. This guide MUST also describe the actions that could destroy potential evidence and how they can be avoided.

DER.2.2.A3 Pre-Selection of Forensic Service Providers (B)

If an organisation does not have its own forensics team, suitable providers of forensic services MUST be identified during the preparatory phase. The eligible providers of forensic services MUST be documented.

3.2. Standard Requirements

For module DER.2.2 *Provisions for IT Forensics*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

DER.2.2.A4 Identifying Common Areas Between IT Forensics and Crisis/Business Continuity Management (S)

The areas in which forensic IT examinations and crisis / business continuity management overlap SHOULD be defined and documented. The employees responsible for specific tasks and the channels to be used to communicate with them SHOULD be specified. Furthermore, it SHOULD be ensured that the responsible contact persons are always available.

DER.2.2.A5 Drawing Up a Guide to Securing Evidence in Case of IT Security Incidents (S)

A guide describing how evidence is to be secured SHOULD be drawn up. This guide SHOULD specify procedures, technical tools, legal framework conditions, and documentation requirements.

DER.2.2.A6 Training Personnel on Forensic Securing of Evidence (S)

All the employees responsible SHOULD know how to secure evidence and use forensic tools correctly. In this regard, suitable training SHOULD be carried out.

DER.2.2.A7 Selecting Tools for Forensics (S)

It SHOULD be ensured that tools for securing and analysing evidence forensically are suitable for these purposes. Before using a tool for forensics, it SHOULD be checked that it works properly. It SHOULD also be verified and documented that it has not been manipulated.

DER.2.2.A8 Selection and Order of Evidence to Be Secured [Process Owner] (S)

A forensic examination SHOULD always start by defining the goals or assignment in question. The goals SHOULD be formulated as precisely as possible. All the required data sources SHOULD then be identified. The order in which data is to be secured and a detailed process for doing so SHOULD also be specified. The order SHOULD be based on the volatility of the data to be secured. Highly volatile data SHOULD be secured promptly. Non-volatile data such as read-only memory SHOULD only be secured afterwards, followed by backups.

DER.2.2.A9 Pre-Selection of Forensically Relevant Data [Process Owner] (S)

The method and time period for storing secondary data (e.g. log data or traffic transcripts) within the scope of the legal framework conditions for forensic measures to secure evidence SHOULD be specified.

DER.2.2.A10 Forensic Securing of IT Evidence [Process Owner] (S)

Storage media SHOULD be forensically duplicated as completely as possible. If this is not possible (e.g. in the case of volatile data in RAM or SAN partitions), a method that changes as little data as possible SHOULD be selected.

The original storage media SHOULD sealed and retained. Cryptographic checksums that are documented in writing SHOULD be created from the storage media. These SHOULD be kept separately and in multiple copies. In addition, it SHOULD be ensured that the checksums documented in this way cannot be changed. A witness SHOULD confirm the corresponding procedure and certify the checksums so that the data is admissible in court.

Only trained personnel (see DER.2.2.A6 *Training Personnel on Forensic Securing of Evidence*) or a provider of forensic services (see DER.2.2.A3 *Pre-Selection of Forensic Service Providers*) SHOULD be assigned to secure evidence.

DER.2.2.A11 Documentation of Securing Evidence [Process Owner] (S)

When evidence is secured forensically, all the steps carried out SHOULD be documented. The documentation SHOULD provide seamless proof of how secured original evidence has been handled. In addition, the employed methods and the reasons why the persons in charge used them SHOULD be documented.

DER.2.2.A12 Secure Storage of Original Storage Media and Evidence [Process Owner] (S)

All secured original storage media SHOULD be stored physically in such a way that only investigating employees known by name can access them. If original storage media and evidence are stored, the period for which they are to be retained SHOULD be specified. After this period expires, it SHOULD be checked whether the storage media and evidence must be stored further. After the end of the storage period, evidence SHOULD be securely deleted or destroyed, and original storage media SHOULD be returned.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.2.2 *Provisions for IT Forensics* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

DER.2.2.A13 Framework Agreements with External Service Providers (H)

An organisation SHOULD conclude call-off agreements or framework contracts with forensic service providers in order to have possible IT security incidents forensically investigated more quickly.

DER.2.2.A14 Specifying Standard Procedures for Securing Evidence (H)

Standard procedures that make it possible to forensically secure volatile and non-volatile data as completely as possible SHOULD be created for applications, IT systems, and IT system groups with increased protection needs, as well as for distributed system configurations.

The relevant system-specific standard procedures SHOULD be implemented by proven (and preferably automated) processes. Furthermore, they SHOULD be supported by checklists and auxiliary technical resources—for example, by software, software tools on mobile storage media, and forensic IT hardware such as write-blockers.

DER.2.2.A15 Conducting Drills on Securing Evidence (H)

All the employees involved in forensic analyses SHOULD take part in regular drills that provide training on how to secure evidence should an IT security incident occur.

4. Additional Information

4.1. Useful Resources

The BSI provides further information on this subject in “Leitfaden IT-Forensik” [BSI Guide for IT Forensics], which also serves as a reference work for individual problems that can arise in practice.

The International Organization for Standardization (ISO) provides guidelines for conducting forensic analyses in the standards ISO/IEC 27042:2015 and 27043:2015 01:2013.

“The Standard of Good Practice for Information Security” published by the Information Security Forum (ISF) provides guidelines for conducting forensic analyses (section TM 2.4, "Forensic Investigations").

Request for Comments (RFC) 3227, “Guidelines for Evidence Collection and Archiving”, provides information on basic procedure in securing forensic evidence.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module DER.2.2 *Provisions for IT Forensics*.

G 0.17 Loss of Devices, Storage Media and Documents

G 0.20 Information or Products from an Unreliable Source

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.37 Repudiation of Actions

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

DER.2.3 Clean-Up of Extensive Security Incidents

1. Description

1.1. Introduction

Advanced Persistent Threats (APT) are cyber attacks that target specific organisations and facilities. In such cases, an attacker gains permanent access to a network and expands this access to further IT systems. The attacks are characterised by a very high use of resources and extensive technical skills on the part of the attackers. Attacks of this type are usually difficult to detect.

After an APT attack has been detected, the persons in charge at the affected organisation face great challenges in carrying out a clean-up effort that goes beyond the usual procedure for dealing with IT security incidents. It can be assumed that the discovered attackers have been able to access the affected IT infrastructure for quite some time. They have probably also been using complex attack tools to bypass standard security mechanisms and establish various backdoors. Furthermore, there is the risk that the attackers are observing the infected environment in detail and will react to cleaning attempts by erasing their traces and sabotaging the investigation.

This module assumes that the organisation in question faces a serious threat because it has fallen victim to a targeted attack by highly motivated perpetrators with above-average resources. In real-world situations, a (certified) forensics expert is usually consulted in the event of an incident like this if the organisation does not have its own forensic experts. While forensic service providers are already called in during the forensic analysis phase, they are also involved (at least in an advisory capacity) during clean-up.

1.2. Objective

This module describes what an organisation should do in order to clean its IT systems and restore the normal and secure operating condition of its information domain after an APT attack.

1.3. Scoping and Modelling

Module DER.2.3 *Clean-Up of Extensive Security Incidents* must always be applied when the regular and secure operating condition of an information domain is to be restored following an APT incident. The module must be applied to the information domain under consideration.

An information domain can only be cleaned after an APT incident has been detected successfully and analysed forensically. Detection and forensics are therefore not dealt with in this module. These topics are covered in the modules DER.1 *Detecting Security-Relevant Events* and DER.2.2 *Provisions for IT Forensics*.

This module deals exclusively with the process of cleaning up after APT incidents. Other incidents are covered in module DER.2.1 *Security Incident Handling*. This module does not describe how indicators of compromise (IoCs, which are evidence of penetration) are to be derived and how they may be used to identify recurring attackers. It also does not address how to find backdoors that may have been overlooked during analysis and cleaning.

This module only considers cyber attacks; attacks in which attackers gain physical access to an information domain are not considered. For example, forms of attack in which data centres are broken into, administrators are bribed, newly acquired hardware is intercepted and manipulated, or electromagnetic radiation is intercepted are not considered in this module.

The requirements of this module also apply to forensic service providers that clean up affected IT systems either entirely or in part. Contractual agreements and checks can be used to ensure that the service providers adhere to these requirements (see OPS.2.1 *Outsourcing for Customers*).

2. Threat Landscape

For module DER.2.3 *Clean-Up of Extensive Security Incidents*, the following specific threats and vulnerabilities are of particular importance.

2.1. Incomplete Cleaning

APT attackers normally aim to infiltrate an information domain permanently. They have access to the necessary resources and are capable of performing long-term attack campaigns. To this end, they use tools and methods that are tailored to their specific target. Even if an APT incident is detected, it cannot be assumed that all the access routes of the attackers have been found, all infections and malware communication channels have been eliminated, and all backdoors have been removed. If an incomplete cleaning process is conducted, it is very likely that an attacker will regain access to the IT systems and start to broaden their access at a later point in time (e.g. after a longer period of inactivity). This can be done not only by placing backdoors in operating systems and application software, but by manipulating hardware-oriented components like firmware, as well. Such modifications are very hard to identify and very few people have the expertise required to extract and analyse them. If the persons in charge try to clean IT components by overwriting or updating the firmware, for example, the attacker may have also modified the update routines. This provides an opportunity to re-enter the system.

2.2. Destruction of Trace Evidence

After an APT incident, IT systems are often installed from scratch or decommissioned entirely. However, if no forensic copy has been made of the IT systems beforehand, trace evidence may be destroyed that would be required to clear up the incident further or even assemble a corresponding court case.

2.3. Premature Alerting of the Attacker

Normally, an attack is observed and analysed forensically over a longer period of time before an APT incident is cleaned. Here, the purpose of cleaning is to identify all the access paths, tools and methods in use. If the attacker notices that they have been discovered during this phase, they might take countermeasures. They may, for example, try to cover their tracks or sabotage additional IT systems. They may also abort the attack for the time being or set up more backdoors to continue the attack later.

Since it must be assumed that the entire IT infrastructure of the organisation in question has been compromised by an APT attack, the risk is high that the attacker will detect cleaning activities. This is particularly applicable if the compromised IT infrastructure is used to plan and coordinate the cleaning process. If essential steps for cleaning are not performed in the correct order or critical safeguards are not performed simultaneously in a coordinated manner, this will increase the risk of the attacker being alerted. If the persons in charge isolate the network in a step-by-step manner instead of all at once, for example, the attacker may be warned before their access is terminated effectively.

2.4. Data Loss and Failure of IT Systems

During the clean-up of an APT incident, various IT systems are reinstalled and networks are also temporarily isolated. As a consequence, IT systems will inevitably fail and services may only be available to a limited extent (or not at all). If the clean-up takes a long time, it can reduce the respective organisation's productivity. This in turn may cause significant economic losses that could even threaten the organisation's existence. This is particularly the case if documentation for the recovery process is insufficient or unavailable.

2.5. Lack of Network Restructuring after an APT Attack

In the event of an APT attack, the attacker obtains detailed knowledge of how the target environment is structured and configured. They will be familiar, for example, with the existing network segments, the naming schemes for IT systems and user and service accounts, and the software and services used. This knowledge may enable the same attacker to regain access to the target environment after the cleaning process is complete. They can move within the network in a targeted, efficient, and unobtrusive manner and quickly achieve a high degree of infection once more.

3. Requirements

The specific requirements of module DER.2.3 *Clean-Up of Extensive Security Incidents* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module DER.2.3 *Clean-Up of Extensive Security Incidents*, the following requirements MUST be implemented as a matter of priority:

DER.2.3.A1 Creation of a Management Committee (B)

In order to clean up an APT incident, a management committee MUST be created to plan, coordinate, and monitor all the necessary activities. The committee MUST be provided with all the managerial authority necessary for its tasks.

If a management committee of this kind was already in place when the APT incident was detected and classified, the same committee SHOULD also plan and oversee the cleaning process. If a specialised forensic service provider has already been brought in to analyse the APT incident, it SHOULD also be involved in the clean-up effort.

The idea of setting up a crisis team SHOULD be examined if the IT systems in question are too compromised to continue operating or the clean-up measures are very extensive. In this case, the management committee MUST monitor the clean-up measures. The management committee MUST then report to the crisis team.

DER.2.3.A2 Deciding on a Cleaning Strategy (B)

Before an APT incident is actually cleaned up, the management committee MUST define a cleaning strategy. Here, it MUST be decided in particular whether the malware can be removed from the compromised IT systems and whether certain IT systems have to be reinstalled or replaced completely (including their hardware). Furthermore, the IT systems to be cleaned MUST be defined. These decisions MUST be based on the results of a previous forensic examination.

All the IT systems affected SHOULD be reinstalled. Afterwards, the organisation's recovery schemes MUST be followed. Before backups are restored, however, forensic examinations MUST be performed to ensure that no manipulated data or programs will be transferred to a reinstalled IT system.

If the organisation decides that it does not want to reinstall all of its IT systems, a targeted APT clean-up process MUST be implemented. To minimise the risk of overlooked backdoors, IT systems MUST be specifically monitored after the clean-up to see if they are still communicating with the attacker.

DER.2.3.A3 Isolation of Affected Network Segments (B)

The network segments affected by an APT incident MUST be isolated completely. In particular, these network segments MUST be cut off from the Internet. In order to effectively lock out the attacker and prevent them from covering their tracks or sabotaging other IT systems, the network segments MUST be isolated simultaneously.

The network segments to be isolated MUST be determined in advance through forensic analysis. This MUST identify all the segments affected. If this cannot be guaranteed, all suspicious network segments MUST be isolated along with all those that are only theoretically infected.

To effectively isolate network segments, all local Internet connections (e.g. additional DSL connections in individual sub-networks) MUST be documented as comprehensively as possible and taken into account.

DER.2.3.A4 Blocking and Changing Access Data and Cryptographic Keys (B)

All access data MUST be changed after an affected network is isolated. Furthermore, access data managed in a centralised manner MUST also be reset, including in Active Directory environments or when the Lightweight Directory Access Protocol (LDAP) has been used.

If the central authentication server (domain controller or LDAP server) has been compromised, all the users on it MUST be blocked and have their passwords changed. This MUST be implemented by experienced administrators and with the help of internal or external forensics experts, if necessary.

If TLS keys or an internal certification authority (CA) has been compromised by the APT attack, corresponding keys, certificates, and infrastructures MUST be regenerated and redistributed. The compromised keys and certificates MUST also be reliably blocked and withdrawn.

DER.2.3.A5 Closing the Initial Entry Route (B)

If a forensic examination determines that the attackers used a technical vulnerability to penetrate the network of the organisation in question, this vulnerability MUST be closed. If the attackers were able to compromise the IT systems as a consequence of human error, organisational, personnel-related, and technical measures MUST be taken to prevent similar incidents in the future.

DER.2.3.A6 Returning to Production Operations (B)

After the affected network has been cleaned successfully, the IT systems MUST be returned to production operations in a controlled manner. In so doing, all the previously used IT systems and installed programs that were used to observe and analyse the attack MUST either be removed or incorporated into the productive environment. The same MUST be done with communication and collaboration systems procured for the purpose of cleaning. Evidence and

decommissioned IT systems MUST either be deleted or destroyed securely, or archived appropriately.

3.2. Standard Requirements

For module DER.2.3 *Clean-Up of Extensive Security Incidents*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

DER.2.3.A7 Targeted System Hardening (S)

After an APT attack, all the IT systems affected SHOULD be hardened. This SHOULD be based on the results of forensic examinations. In addition, there SHOULD be a further check on whether the affected environment is still secure.

If possible, IT systems SHOULD already be hardened as they are being cleaned. Safeguards that cannot be performed on short notice SHOULD be added to an action plan and implemented in the medium term. The CISO SHOULD draw up the plan and check that it has been implemented properly.

DER.2.3.A8 Establishing Secure, Independent Communication Channels (S)

Secure communication channels SHOULD be established for the management committee in question and the employees charged with cleaning. If third-party communication services are used, care SHOULD be taken to ensure that a secure communication channel is selected.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.2.3 *Clean-Up of Extensive Security Incidents* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

DER.2.3.A9 Hardware Replacement in Affected IT Systems (H)

Whether hardware needs to be replaced completely after an APT incident SHOULD be considered. If suspicious behaviour is still observed after cleaning the individual IT systems affected, the respective systems SHOULD be replaced.

DER.2.3.A10 Modifications to Help Thwart a Repeat Attack (H)

If an organisation wants to prevent a previous attacker from performing another APT attack on its IT systems, the organisation SHOULD change the internal design of its network environment. Furthermore, mechanisms SHOULD be established that can be used to quickly detect a recurring attacker.

4. Additional Information

4.1. Useful Resources

The BSI has published the following documents associated with APTs:

- BSI publication on cyber security (BSI-CS 072): “Erste Hilfe bei einem APT Angriff” [First Aid in the Event of an APT Attack]
- Common Criteria Protection Profile for Remote-Controlled Browsers System (ReCoBS): BSI-PP-0040

CERT-EU has published the security whitepaper 2014-007, "Kerberos Golden Ticket Protection: Mitigating Pass-the-Ticket on Active Directory" on the topic of APTs.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module DER.2.3 *Clean-Up of Extensive Security Incidents*.

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

DER.3.1 Audits and Revisions

1. Description

1.1. Introduction

Audits and revisions are fundamental to every successful information security management system (ISMS). An organisation's overall level of information security can only be assessed when established security safeguards and processes are regularly audited to determine whether they are still effective, complete, appropriate, and up to date. Hence, audits and revisions are a suitable tool for determining, achieving, and maintaining an appropriate level of security. Audits and revisions make it possible to identify security deficiencies and undesirable developments and create appropriate safeguards in response.

An audit (lat. *audire* = to hear, to listen) is a systematic, independent examination of activities and their results. This involves checking compliance with defined requirements such as norms, standards, or guidelines. A revision (revise = control, check) investigates whether documents, conditions, objects, or methodologies are correct, effective, and appropriate. Unlike an audit, a revision does not necessarily have to be performed independently. A revision may also include maintenance that incorporates subsequent improvements.

1.2. Objective

Module DER.3.1 *Audits and Revisions* defines requirements for audits and revisions in order to improve information security in an organisation, avoid improper developments in this area, and optimise security safeguards and processes.

1.3. Scoping and Modelling

The module must be applied once to the entire information domain under consideration. It covers internal audits (first-party audits) and revisions, as well as audits of service providers and partners (second-party audits). Certification audits (third-party audits) are not considered in this module.

The IS audits that are obligatory for federal government agencies in Germany are also not addressed. These are covered in module DER 3.2 *Audits Based on the BSI "Guideline for IS Audits"*.

2. Threat Landscape

For module DER.3.1 *Audits and Revisions*, the following specific threats and vulnerabilities are of particular importance.

2.1. Insufficient or Unplanned Implementation of Security Safeguards

The level of protection of an organisation depends on the complete and correct implementation of security safeguards. However, security safeguards may be suspended temporarily, particularly during the critical phases of projects or under certain framework conditions. Forgetting to reactivate them can result in an insufficient level of security.

2.2. Ineffective or Inefficient Implementation of Security Safeguards

If security safeguards are implemented without considering certain practical aspects, they might prove ineffective. For example, it does not make sense to block an entrance area using turnstiles if employees can easily access the building using an open side entrance.

Individual safeguards may also be implemented that do not make sense from an economic point of view. Hence, a properly implemented rights and role concept is a more reasonable and economical way to protect information with normal levels of confidentiality than complex, certificate-based encryption of a file server.

2.3. Insufficient Implementation of the ISMS

In many organisations, the Chief Information Security Officer checks whether security safeguards have been implemented. However, the auditing of the ISMS itself is often forgotten, particularly because this should be done by an independent third party. As a consequence, the processes of an ISMS might be implemented inefficiently or inappropriately. The level of security of the respective organisation may thus be impaired.

2.4. Insufficient Auditor Qualifications

If an auditor or revisor is insufficiently qualified or prepared, they might incorrectly assess the security status of an organisation. The resulting audit report could thus fail to include necessary corrective actions or even recommend improper safeguards. In the worst case, this could lead to excessive (and thus non-economical) protection of information, or insufficient protection that entails a great many risks.

2.5. Lack of Long-Term Planning

If audits and revisions are not planned in a long-term, centralised manner, individual areas may be audited very frequently, and others not at all. As a consequence, it may be very difficult or impossible to assess the security status of the information domain at hand.

2.6. Lack of Planning and Coordination when Performing an Audit

If an audit is not planned sufficiently and coordinated with all the affected employees of the organisation in question, the required contact persons may not be present during the on-site audit. As a result, it may be impossible to audit individual areas at all. If the auditor has set too tight a schedule for the individual areas, the audit might only be performed superficially due to a lack of time.

2.7. Lack of Coordination with Employee Representatives

Audits and revisions may also examine aspects that could be used to draw conclusions on the performance of employees. Hence, these audits and revisions may be considered a performance evaluation. If an organisation's Employee Representatives are not involved, this may result in violations of the applicable right of co-determination.

2.8. Deliberate Concealment of Deviations

Employees may try to conceal security issues because they are afraid their errors will be discovered during an audit. This might convey an inaccurate picture of the status quo.

3. Requirements

The specific requirements of module DER.3.1 *Audits and Revisions* are listed below. As a matter of principle, the Chief Information Security officer (CISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Audit Team, Top Management

3.1. Basic Requirements

For module DER.3.1 *Audits and Revisions*, the following requirements MUST be met as a matter of priority:

DER.3.1.A1 Definition of Responsibilities [Top Management] (B)

An organisation's Top Management MUST appoint an employee who will be responsible for planning and initiating audits and revisions. The Top Management MUST ensure that there is no conflict of interests in this appointment.

The organisation MUST use audits and revisions to improve its security safeguards.

DER.3.1.A2 Preparing an Audit or Revision (B)

Prior to an audit or revision, an organisation MUST define the audit object and its corresponding goals. The affected contact partners MUST be informed. Depending on the object of the audit or revision, the employee responsible MUST inform the Employee Representatives of the planned audit or revision.

DER.3.1.A3 Conducting an Audit [Audit Team] (B)

During an audit, the Audit Team MUST check whether the requirements of guidelines, norms, standards, and other relevant specifications are being fulfilled. The organisation being audited MUST be aware of these requirements.

The Audit Team MUST carry out a document check and an on-site audit during each audit process. During the on-site audit, the Audit Team MUST ensure that it never actively interferes with systems itself and does not issue instructions regarding changes to the audit object.

The Audit Team MUST document all the results of the audit in writing and summarise them in an audit report. The audit report MUST be submitted to the contact person of the organisation in a timely manner.

DER.3.1.A4 Performing a Revision (B)

Within the framework of a revision, the Audit Team MUST check that the current requirements are being met in a complete, correct, and appropriate manner. The organisation in question MUST correct any deviations found as quickly as possible. The respective revisions MUST be documented in a revision history.

3.2. Standard Requirements

For module DER.3.1 *Audits and Revisions*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

DER.3.1.A5 Integration into the Information Security Process (S)

An organisation SHOULD provide a policy for internal ISMS auditing. It SHOULD also establish a policy on the management of corrective action. These policies SHOULD specify that regular audits and revisions are part of the security process and initiated by said process.

Furthermore, the CISO SHOULD ensure that the results of audits and revisions are returned to the ISMS and incorporated into its improvement. The CISO SHOULD include the audits and revisions carried out and their results in their regular report to the organisation's Top Management. This SHOULD also detail the deficiencies eliminated and the quality improvements made.

DER.3.1.A6 Definition of an Audit and Revision Basis and a Uniform Evaluation Scheme (S)

An organisation SHOULD establish a uniform basis for audits. A uniform evaluation scheme SHOULD be defined and documented for evaluating the implementation of requirements.

DER.3.1.A7 Drawing Up an Audit Program (S)

The CISO SHOULD draw up an audit program that contains all the audits and revisions to be performed in the next several years. Objectives SHOULD be defined for the audit program that are derived in particular from the information security goals at hand and the aims of the corresponding organisation.

The CISO SHOULD provide for contingency reserves in the organisation's annual resource planning. The audit program SHOULD be subject to its own continuous improvement process.

DER.3.1.A8 Creation of a Revision List (S)

The CISO SHOULD maintain one or more revision lists that document the current status of the revision objects and the scheduled revisions.

DER.3.1.A9 Selection of an Appropriate Audit Team or Revision Team (S)

An organisation SHOULD assemble a suitable team for every audit and revision. It SHOULD appoint a leading auditor (Audit Team Leader) or a leading revisor. This person SHOULD take complete responsibility for carrying out the audits or revisions.

The size of the Audit Team or revision team SHOULD correspond to the area to be audited. In particular, the organisation SHOULD consider the competencies required for the subjects of an audit and the size and local distribution of the area to be audited. The members of the audit or revision team SHOULD be appropriately qualified.

The neutrality of the Audit Team SHOULD be guaranteed. The revisors SHOULD also be independent. If external service providers are deployed as auditors or revisors, their independence SHOULD be checked and they SHOULD be obliged to maintain confidentiality.

DER.3.1.A10 Creation of a Audit Plan or Revision Plan [Audit Team] (S)

Prior to an audit or a major revision, the Audit Team Leader or the lead revisor SHOULD create an audit or revision plan. For audits, the audit plan SHOULD be part of the final audit report. The audit plan SHOULD be updated throughout the audit and adjusted as required. Minor revisions SHOULD be scheduled according to the revision list.

The respective organisation SHOULD provide sufficient resources to the Audit Team or revision team.

DER.3.1.A11 Communication and Behaviour During Audits [Audit Team] (S)

The Audit Team SHOULD set clear rules for the exchange of information between the Audit Team or revision team and the employees of the organisation or department to be audited. The Audit Team SHOULD use suitable safeguards to ensure that the information shared in an audit remains confidential and its integrity remains intact.

Persons supporting the audit SHOULD NOT influence its activities. Furthermore, they SHOULD be obliged to maintain confidentiality.

DER.3.1.A12 Holding an Initial Meeting [Audit Team] (S)

The Audit Team or revision team SHOULD hold an initial meeting with the relevant contact persons. The audit or revision procedure SHOULD be explained and the framework conditions of the on-site audit agreed. The respective persons in charge SHOULD confirm this.

DER.3.1.A13 Inspection and Review of Documents [Audit Team] (S)

The documents SHOULD be checked by the Audit Team based on the requirements defined in the Gap Analysis Plan. All the relevant documents SHOULD be reviewed as to whether they are up to date, complete, and comprehensible. The results of the document check SHOULD be documented. To the extent that doing so makes sense, the results SHOULD also be incorporated into the on-site audit.

DER.3.1.A14 Selection of Samples [Audit Team] (S)

The Audit Team SHOULD select the samples for the on-site audit in a risk-oriented manner and justify them in a comprehensible way. The selected samples SHOULD be documented. If the audit is being performed based on the target objects and requirements of an IT-Grundschutz module, these SHOULD be selected on the basis of a previously defined method. When selecting samples, the results of previous audits SHOULD be taken into consideration, as well.

DER.3.1.A15 Selection of Appropriate Audit Techniques [Audit Team] (S)

The Audit Team SHOULD implement suitable methods for each of the areas to be audited. Furthermore, it SHOULD be ensured that all audits are proportionate to the situation at hand.

DER.3.1.A16 Schedule of the On-Site Audit [Audit Team] (S)

The Audit Team SHOULD set the schedule of the on-site audit together with the contact person in question. The results SHOULD be documented in the audit plan.

DER.3.1.A17 Performance of the On-Site Audit [Audit Team] (S)

At the beginning of an on-site audit, the Audit Team SHOULD hold an initial meeting with the persons in charge at the organisation concerned. Afterwards, all the requirements specified in the Gap Analysis Plan SHOULD be checked using the audit methods defined. If a selected sample deviates from the documented status, the sample SHOULD be extended as needed until the issue is clarified. The Audit Team SHOULD conduct a closing meeting after the audit. It SHOULD briefly present the results (without assessments) and explain the steps ahead. The meeting SHOULD be documented in writing.

DER.3.1.A18 Conducting Interviews [Audit Team] (S)

The Audit Team SHOULD conduct structured interviews. Questions SHOULD be concise, precise, and easy to understand. In addition, appropriate interviewing techniques SHOULD be used.

DER.3.1.A19 Revision of the Risk Treatment Plan [Audit Team] (S)

The Audit Team SHOULD check that the remaining residual risks are appropriate and acceptable for the information domain concerned. It SHOULD also check whether the organisation's Top Management has acknowledged its acceptance of these risks in a binding manner. Safeguards that fundamentally support the information security of the entire organisation MUST NOT be included in this assumption of risk.

The auditor SHOULD verify at random whether and to what extent the safeguards defined in the risk treatment plan have been implemented.

DER.3.1.A20 Holding a Closing Meeting [Audit Team] (S)

The Audit Team SHOULD conduct a closing meeting with the respective persons in charge at the audited organisation. This SHOULD present the preliminary audit findings and lay out the next steps.

DER.3.1.A21 Analysis of Audits [Audit Team] (S)

After an on-site audit, the Audit Team should further consolidate and evaluate the information gained. After any additional information and documentation requested after the fact are analysed, the audited safeguards SHOULD be subjected to a final evaluation. The Audit Team SHOULD allow the organisation in question a sufficient time frame for providing the requested documentation. Documents not received by the agreed date SHOULD be considered non-existent.

DER.3.1.A22 Creation of an Audit Report [Audit Team] (S)

The Audit Team SHOULD transfer the results obtained into an audit report and document them transparently.

The organisation audited SHOULD ensure that all the entities affected are provided with the sections of the audit report that are important and necessary for them within an appropriate time frame.

DER.3.1.A23 Documentation of Revision Results (S)

The results of a revision SHOULD be documented uniformly by the revision team.

DER.3.1.A24 Conclusion of the Audit or Revision [Audit Team] (S)

After the audit or revision, all the relevant documents, data storage media, and IT systems SHOULD be returned or destroyed. This SHOULD be coordinated with the audited organisation. In doing so, storage obligations resulting from legal or other binding requirements SHOULD be taken into account accordingly. Furthermore, the CISO SHOULD have all the forms of access granted to the Audit Team or revision team disabled or deleted.

There SHOULD be an agreement with the auditors or revisors as to how the results are to be handled. This SHOULD also establish that the audit results must not be forwarded to other organisations without the consent of the audited organisation.

DER.3.1.A25 Evaluation of an Audit (S)

The audited organisation SHOULD eliminate the deviations or shortcomings identified in the audit report or within the framework of a revision within a reasonable period of time. The

corrective measures to be taken SHOULD be documented, along with the corresponding deadlines and the persons responsible. Corrective measures that have been completed already SHOULD also be documented. The organisation SHOULD establish and use a defined procedure for this purpose.

In the event of serious deviations or shortcomings, the Audit Team or revision team SHOULD check whether the corrective measures have been carried out.

DER.3.1.A26 Monitoring and Adapting the Audit Program (S)

The audit program followed SHOULD be monitored and adapted continuously to ensure compliance with regard to dates, audit objectives, audit contents, and audit quality.

The appropriateness of the audit program SHOULD be checked based on the requirements it is meant to fulfil and the results of the audits performed. It SHOULD be adapted as necessary.

DER.3.1.A27 Storage and Archiving of Documents on Audits and Revisions (S)

The organisation in question SHOULD file and store audit programs and documents on audits and revisions in a traceable and audit-proof manner in accordance with regulatory requirements. This SHOULD ensure that only authorised persons can access audit programs and documents. The organisation SHOULD securely destroy the audit programs and documents after the retention period has expired.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.3.1 *Audits and Revisions* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

DER.3.1.A28 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) describes guidelines for auditing management systems in the standard ISO 19011:2011.

The International Organization for Standardization (ISO) describes guidelines for auditing an ISMS in the standard ISO/IEC 27007:2011.

The Information Security Forum describes guidelines for auditing an ISMS in “The Standard of Good Practice for Information Security”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module DER.3.1 *Audits and Revisions*.

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.46 Loss of Integrity of Sensitive Information

Federal Office
for Information Security

DER.3.2 Audits Based on the BSI "Guideline for IS Audits"

1. Description

1.1. Introduction

Information security (IS) audits based on IT-Grundschutz represent a special form of auditing that follows the document *Information Security Audit (IS Audit) – A Guideline for IS Audits Based on IT-Grundschutz* (in short, the "*Guideline for IS Audits*").

The "Guideline for IS Audits" is a document published by the BSI that describes the procedure for IS auditing. Federal authorities are obliged to review their information security management systems (ISMS) using IS audits. If they want to check the implementation of their ISMS, other organisations can carry out an IS audit based on the guideline instead of a regular IT audit.

IS audits based on the BSI guideline feature a holistic approach. This means that all levels of an ISMS are checked, from the establishment of an information security organisation and personnel aspects to the configuration of IT systems and applications. Economic efficiency and compliance, which are the focus of traditional IT audits, are only of secondary importance. Information security (including the adequacy of the security safeguards at hand) is thus the essential test criterion of an IS audit based on IT-Grundschutz.

An IS audit based on IT-Grundschutz is a fundamental part of successful information security management. After all, regular checks are the only way to evaluate whether the established measures and information security processes are effectively implemented, complete, up to date, and appropriate. An IS audit based on IT-Grundschutz is therefore a suitable tool for determining, achieving, and maintaining an appropriate and continuously improving level of security in an organisation.

The main task of an IS audit based on IT-Grundschutz is to support and accompany the top management, the IS management team and, in particular, the Chief Information Security Officer (CISO) in achieving the highest possible level of information security in their organisation.

1.2. Objective

This module defines requirements for an IS audit based on IT-Grundschutz in order to improve the information security in an organisation, avoid improper developments in this area, and optimise security safeguards and processes.

1.3. Scoping and Modelling

This module must be applied whenever an organisation is obliged to carry out audits based on the "Guideline for IS Audits" or wishes to do so voluntarily. The module must be applied once to the entire information domain under consideration.

The ways in which an IS audit based on IT-Grundschutz can be integrated into an existing overarching audit unit (e.g. an internal auditing department) within an organisation are not covered. Module DER.3.2 *Audits Based on the BSI "Guideline for IS Audits"* is a specific example of the requirements described in general in module DER.3.1 *Audits and Revisions*. Organisations that implement the present module no longer need to implement DER.3.1 *Audits and Revisions*, as its requirements are fully contained in this module.

IS audits and the certification of an ISMS in line with ISO 27001 on the basis of IT-Grundschutz complement each other. IS audits can accompany the path to certification and, in contrast, can be carried out during the initiation of the security process in a given organisation. They show the organisation where there is an urgent need for action and which security deficiencies should be addressed as a matter of priority. If individual information domains in the organisation are certified according to ISO 27001 on the basis of IT-Grundschutz, recertification and IS audits for these information domains should be carried out together if possible. The findings of surveillance audits or certification procedures can be used for IS audits.

If an ISO 27001 certificate based on IT-Grundschutz is available for the entire organisation, the surveillance audits required in the certification procedure replace the IS audits.

The regulations regarding the protection of classified information and the General Administrative Instructions for the physical and organisational protection of classified material (Classified Material Instructions) issued by the Federal Ministry of the Interior remain unaffected and apply regardless of the requirements of this module.

2. Threat Landscape

For module DER.3.2 *Audits Based on the BSI "Guideline for IS Audits"*, the following specific threats and vulnerabilities are of particular importance.

2.1. Violation of Specifications of UP Bund

The "Implementation Plan for the Federal Administration" (UP Bund 2017) is the defined guideline for information security in the Federal Administration of Germany. It establishes a form of cross-departmental information security management for federal agencies in which each agency is responsible for creating and implementing its own specific security concept. In

addition to federal agencies, other organisations may be obliged by law, contract, or other regulations to implement UP Bund 2017. UP Bund 2017 explicitly stipulates that the BSI standards on information security and IT-Grundschutz, as well as the procedure for standard protection described therein, must be implemented as a minimum requirement. Furthermore, UP Bund 2017 stipulates that all organisations that are obliged to implement the plan must regularly review the status of their own ISMS (e.g. by means of a suitable IS audit) and apply the "*Guideline for Information Security Audits Based on IT-Grundschutz*". Any organisation that fails to do so will find itself in breach of the provisions of UP Bund.

2.2. Suspension of Security Safeguards

The level of security within an organisation depends on the complete and correct implementation of security safeguards. Security safeguards are often temporarily suspended, particularly during the critical phases of projects or under certain conditions. In some cases, however, the need to reactivate them may be forgotten, resulting in an insufficient security level.

2.3. Ineffective or Inefficient Implementation of Security Safeguards

If security safeguards are implemented without considering the practical aspects at hand, the safeguards might be ineffective in some circumstances. For example, it does not make sense to block an entrance area using turnstiles if employees can access the building using an open side entrance instead.

Individual safeguards may also be implemented that do not make sense from an economic point of view. To protect information with normal protection needs with regard to confidentiality, an appropriately implemented rights and role concept makes more sense and is more economical than establishing complex, certificate-based encryption on a file server.

2.4. Inadequate Implementation of the Information Security Management System

In many organisations, the Chief Information Security Officer (CISO) checks whether security safeguards have been implemented. In this context, the examination of the actual ISMS can often be forgotten because the CISO is part of the ISMS, and thus not impartial. Consequently, the processes of an ISMS may have been inefficiently or inappropriately implemented, resulting in an unintentionally low level of security for the organisation.

2.5. Insufficient Auditor Qualifications

If IS auditors are not sufficiently qualified or do not sufficiently prepare for audits, they may misjudge the security status of an organisation during an IS audit. In some circumstances, they may then fail to recommend the necessary corrective measures—or even recommend incorrect measures—in their audit report. This can lead to information being protected in an uneconomical or high-risk manner.

2.6. Partiality of Internal IS Audit Teams

Internal employees can be formed into IS audit teams within organisations. If these teams are not kept sufficiently separate from other processes, the IS auditors may be influenced or biased. This is particularly the case if members of the IS audit team are or have been involved in the planning or implementation of the ISMS in question.

2.7. Lack of Long-Term Planning

If IS audits are not planned in a centralised, long-term manner, individual units within an organisation may be audited very frequently, and others not at all. It is also possible that changes to the ISMS will not be sufficiently investigated if audits are only carried out sporadically. In such cases, it is very difficult or even impossible to assess the security status of the information domain at hand.

2.8. Insufficient Planning and Coordination when Performing IS Audits

If an IS audit is planned insufficiently and not coordinated with all the employees responsible in the organisation in question, the correct contact persons may not available during the on-site audit. As a result, it may be impossible to audit individual areas at all. If the IS auditors set too tight a schedule for auditing individual areas, the organisation may only be superficially audited due to a lack of time.

2.9. Lack of Coordination with Employee Representatives

IS audits based on IT-Grundschutz can also cover aspects that enable conclusions to be drawn on employee conduct and performance at work. These audits may therefore be considered as conduct and performance appraisals. If Employee Representatives are not involved, an on-site audit may be delayed or even cancelled.

2.10. Deliberate Concealment of Deviations or Problems

Employees may fear that their own errors will be discovered during an IS audit. To avoid this, they could conceal security problems and thus give a false impression of the actual level of security at their organisation. This allows security deficiencies to remain undiscovered and uncorrected. It also prevents the organisation's top management from assessing the risk associated with such deficiencies.

2.11. Loss of Confidentiality of Sensitive Information

During an IS audit based on IT-Grundschutz, the IS auditors collect confidential information (such as on vulnerabilities and attack options). They may also identify shortcomings in the information security of the audited organisation. If these shortcomings become known to unauthorised third parties, they could be used to attack the organisation or bring its name into disrepute.

3. Requirements

The specific requirements of module DER.3.2 *Audits Based on the BSI "Guideline for IS Audits"* are listed below. As a matter of principle, the Chief Information Security officer (CISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	IS Audit Team, Top Management

3.1. Basic Requirements

For module DER.3.2 *Audits Based on the BSI "Guideline for IS Audits"*, the following requirements MUST be met as a matter of priority:

DER.3.2.A1 Designation of Persons in Charge of the IS Audit [Top Management] (B)

An organisation MUST designate a person in charge of IS auditing. This person MUST plan and initiate IS audits and track their results.

DER.3.2.A2 Creation of an IS Audit Manual (B)

The person in charge of an IS audit MUST create an IS audit manual that contains the objectives, legal requirements, and information about the organisation, its resources, and the framework conditions at hand. It MUST also describe how to archive the related documentation. The manual MUST be approved by the Top Management.

DER.3.2.A3 Definition of the Audit Basis (B)

An IS audit MUST be carried out based on BSI Standards 200-1 to 200-3 and the IT-Grundschutz Compendium. The IT-Grundschutz Standard Protection SHOULD be used for this. These audit principles MUST be known to all the parties involved.

DER.3.2.A4 Drawing Up a Plan for the IS Audit (B)

If an organisation is not certified in line with ISO 27001 on the basis of IT-Grundschutz, the person in charge of its IS audit and the organisation's Top Management MUST ensure that an IS partial audit or IS cross-cutting audit is carried out at least every three years. In addition, further audits should be planned if the information domain in question is significantly changed.

The person in charge of the IS audit should draw up a rough multi-year plan for audits. This schedule SHOULD then be made more specific in a detailed one-year schedule.

DER.3.2.A5 Selection of an Appropriate IS Audit Team (B)

A team consisting of at least two IS auditors MUST be assembled or commissioned. The IS Audit Team MUST be granted unlimited information and inspection rights for its activities. In internal IS Audit Teams, the individual IS auditors MUST be impartial. The members of an IS Audit Team MUST NOT be or have been involved in planning or implementing the ISMS in question.

DER.3.2.A6 Preparation of an IS Audit [IS Audit Team] (B)

An IS Audit Team MUST be commissioned to conduct an IS audit. The IS Audit Team MUST determine the reference documents required for the IS audit. The organisation to be audited MUST hand over its security concept and all other necessary documents to the IS Audit Team.

DER.3.2.A7 Performance of an IS Audit [IS Audit Team] (B)

Within the framework of an IS audit, the IS Audit Team MUST perform a document audit and an on-site audit. All the results of the two audits MUST be documented in writing and summarised in an IS audit report.

Before performing an IS cross-cutting audit for the first time, the person in charge of the IS audit MUST select an IS partial audit as the IS audit procedure. The IS partial audit MUST be completed with a positive result before an IS cross-cutting audit is performed.

DER.3.2.A8 Storage of IS Audit Reports (B)

The organisation in question MUST securely store the IS audit report and the reference documents the report is based on for at least 10 years after it is produced, unless different laws or regulations apply. The organisation MUST ensure that only authorised persons may access the IS audit reports and reference documents.

3.2. Standard Requirements

For module DER.3.2 Audits Based on the BSI “Guideline for IS Audits”, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

DER.3.2.A9 Integration into the Information Security Process (S)

The Chief Information Security Officer SHOULD ensure that IS audits based on IT-Grundschutz form part of their organisation's security process. Furthermore, the results of IS audits SHOULD be incorporated back into the improvement of the ISMS at hand.

In addition, the results of IS audits and activities to remedy deficiencies and improve quality SHOULD be included in the CISO's regular report to the organisation's Top Management.

DER.3.2.A10 Communication Coordination (S)

There SHOULD be clear rules on how information is to be exchanged between the IS Audit Team and the organisation to be audited. This SHOULD ensure that the confidentiality and integrity of this information remains intact.

DER.3.2.A11 Holding an Initial Meeting for an IS Cross-Cutting Audit [IS Audit Team] (S)

When an IS cross-cutting audit is to be conducted, an initial meeting SHOULD take place between the IS Audit Team and the contact persons within the organisation to be audited. The meeting SHOULD include the following items:

- explanation and presentation of the IS audit process
- presentation of the organisation to be audited (focus of work and overview of the IT used)
- handover of the reference documents to the IS Audit Team

DER.3.2.A12 Creation of a Gap Analysis Plan [IS Audit Team] (S)

Prior to an IS audit, the IS Audit Team SHOULD create a Gap Analysis Plan. If it is necessary to extend or otherwise adapt the planned procedures during the audit, the Gap Analysis Plan SHOULD be adapted accordingly. The Gap Analysis Plan SHOULD also be included in the final IS audit report.

During an IS partial audit, the binding audit subject list from BSI SHOULD be used as the Gap Analysis Plan.

DER.3.2.A13 Inspection and Review of Documents [IS Audit Team] (S)

The IS Audit Team SHOULD check the requirements defined in the Gap Analysis Plan during its document check. The IS Audit Team SHOULD check whether all the relevant documents are up to date and complete. When checking whether documents are up to date, their granularity SHOULD be taken into consideration. Care SHOULD be taken to ensure that all the relevant aspects are included and appropriate roles are assigned.

Furthermore, the transparency of the documents and the decisions they contain SHOULD be checked. To the extent that doing so makes sense, the results of the document review SHOULD be documented and incorporated into the on-site audit.

DER.3.2.A14 Selection of Target Objects and Requirements to Be Audited [IS Audit Team] (S)

Within the framework of an IS cross-sectional audit or an IS partial audit, the IS Audit Team SHOULD select the module target objects for the on-site audit based on the results of the checks of documents. However, the information security management module (see ISMS.1 *Security Management*)) of the IT-Grundschutz Compendium, including all its related requirements, SHOULD always be checked completely. A further 30 per cent of the remaining module target objects SHOULD be selected for auditing in a risk-based approach. The selection SHOULD be documented in a transparent manner. For the module target objects selected in this way, 30 per cent of the respective requirements SHOULD be checked during the IS audit.

In addition, the requirements for which shortcomings have been found in previous IS audits SHOULD be taken into account when selecting the module target objects to be audited. All requirements for which serious security shortcomings have been ascertained in previous IS audits SHOULD be audited.

DER.3.2.A15 Selection of Appropriate Audit Techniques [IS Audit Team] (S)

The IS Audit Team SHOULD ensure that appropriate audit techniques are used to determine the areas to be audited. All audits SHOULD be proportionate.

DER.3.2.A16 Creating a Procedure for the On-Site Audit [IS Audit Team] (S)

Together with the contact person of the organisation to be audited, the IS Audit Team SHOULD draw up a schedule for the on-site audit. The results SHOULD be documented along with the IS Gap Analysis Plan.

DER.3.2.A17 Conducting the On-Site Audit [IS Audit Team] (S)

The IS Audit Team SHOULD investigate and determine whether the selected measures for the on-site audit meet the requirements of IT-Grundschutz in a practical and adequate manner.

The audit SHOULD start with an initial meeting. All the requirements of the Gap Analysis Plan that are selected for the audit and/or all the subject areas from the audit subject list SHOULD then be checked. The envisaged audit techniques SHOULD be used for this purpose. If deviations from the documented status of a selected sample are identified, the sample SHOULD be extended as required until the matter is clarified.

During the on-site audit, the IS auditors SHOULD never actively interfere with IT systems or issue any instructions regarding changes to the object of the audit.

All essential issues and details on source, information, and presentation requests, as well as meetings carried out, SHOULD be documented in writing.

In a closing meeting, the IS Audit Team SHOULD briefly present the main findings to the contact persons of the audited organisation. The IS Audit Team SHOULD NOT specifically evaluate the findings, but provide indications of possible deficiencies and explain the next steps. Minutes SHOULD also be taken for this closing meeting.

DER.3.2.A18 Conducting Interviews [IS Audit Team] (S)

Interviews conducted by the IS Audit Team SHOULD be structured. Questions SHOULD be concise, precise, and easy to understand. In addition, appropriate interviewing techniques SHOULD be used.

DER.3.2.A19 Reviewing Risk Treatment Options [IS Audit Team] (S)

The IS Audit Team SHOULD check whether the remaining residual risks are appropriate and acceptable for the information domain at hand and whether the Top Management has officially acknowledged its acceptance of them in a binding manner. The IS Audit Team SHOULD randomly verify whether and to what extent the options selected to treat risks have been implemented.

DER.3.2.A20 Following Up on the On-Site Audit [IS Audit Team] (S)

After the on-site audit, the information collected by the IS Audit Team SHOULD be further consolidated and analysed. After any additional information and documentation requested after the fact have been assessed, the audited requirements SHOULD be subject to a final evaluation.

DER.3.2.A21 Creation of an IS Audit Report [IS Audit Team] (S)

The IS Audit Team SHOULD transfer the results obtained into an IS audit report and document them transparently. A draft version of the report SHOULD be sent in advance to the audited organisation. It SHOULD be verified whether the issues established by the IS Audit Team were correctly recorded.

The audited organisation SHOULD ensure that all affected entities within the organisation are provided with the sections of the IS audit report that are important and necessary for them within an appropriate time frame. In particular, the contents SHOULD be communicated to the Top Management, the person in charge of the IS audit, and the CISO.

IS audit reports SHOULD be assigned an appropriate confidentiality rating based on the sensitive information they contain.

The possibility of having the IS Audit Team provide the results of the IS audit to the Top Management in the form of a presentation SHOULD be considered.

DER.3.2.A22 Following Up on an IS Audit (S)

The deviations identified in the IS audit report SHOULD be corrected by the CISO within a reasonable period of time. The corrective measures to be performed SHOULD be documented along with the respective responsibilities, dates of implementation, and status. The implementation SHOULD be followed up on continuously and the implementation status updated.

The necessity of additional IS audits SHOULD be checked as a matter of principle. The person in charge of the IS audit SHOULD adapt both the rough and detailed plans for the IS audit.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.3.2 *Audits Based on the BSI "Guideline for IS Audits"* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

DER.3.2.A23 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

The Federal Office for Information Security (BSI) describes how an IS audit should be carried out in "Information Security Audit (IS Audit) – A Guideline for IS Audits Based on IT-Grundschutz".

The Federal Office for Information Security (BSI) describes topics that should be audited during an IS partial audit in the document "Verbindliche Prüfthemen für die IS-Kurzrevision" [Binding Audit Subject List for IS Partial Audits].

The Federal Office for Information Security (BSI) provides an example manual for IS auditing in “Revisionshandbuch zur Informationssicherheit nach UP Bund” [Audit Manual for Information Security in Line with UP Bund].

The Federal Ministry of the Interior (BMI) describes the specifications to be observed when handling classified material in the "Verschlusssachenanweisung" [Classified Material Instructions].

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module DER.3.2 *Audits Based on the BSI “Guideline for IS Audits”*.

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.46 Loss of Integrity of Sensitive Information

Federal Office
for Information Security

DER.4 Business Continuity Management

1. Description

1.1. Introduction

In emergencies, organisations must having continued access to information in order to be able to restore a business process, an IT system, or a specialised task. To be able to maintain information security even in an emergency, appropriate processes should therefore be planned, established, and reviewed.

Optimal contingency planning and emergency response can only be achieved by adopting a planned and organised approach. A professional process for business continuity management reduces the impact of an emergency and thereby secures operations and the continued existence of the organisation affected. Suitable measures must be identified and implemented to make time-critical business processes and specialised tasks more robust and fail-safe. On the other hand, these measures should make it possible to deal with an emergency in a quick and targeted manner.

The preservation of information security in an emergency must be integrated into overarching business continuity management, ideally as part of an emergency management system. However, business continuity management has its own Process Owner: the BCM Officer, who coordinates with the Chief Information Security Officer.

1.2. Objective

The aim of this module is to describe requirements to ensure information security in organisations even in critical situations. For this purpose, the corresponding measures should be embedded in a holistic approach to business continuity management. In addition, all aspects should be considered that are necessary for maintaining information security even in the event of damage or emergencies. This includes anything from planning to the checking of all processes.

1.3. Scoping and Modelling

Module DER.4 *Business Continuity Management* must be applied once to the entire information domain under consideration.

In the event of damage, the correct information must be fully available. The present module does not address criteria or processes used by persons in charge to decide whether an emergency has occurred. This decision will be made during the handling of each security incident (see DER.2.1 *Security Incident Handling*).

Crises are considered within the scope of an own crisis management and only are addressed as interface in this module, e.g. within the scope of further escalation of emergencies. Further information on the individual phases of business continuity management and the differentiation between business continuity management and crisis management is included in BSI Standard 100-4, “Business Continuity Management”.

2. Threat Landscape

For module DER.4 *Business Continuity Management*, the following specific threats and vulnerabilities are of particular importance:

2.1. Shortage of Personnel

If staff members are absent, this can quickly mean that an organisation can no longer carry out its specialised tasks and business processes. The reasons for staff absences can be manifold. For example, unsanitary conditions in the canteen or a strike can cause many employees to be absent at the same time. The death of an employee can also lead to downtime or impair important business processes or specialised tasks. In addition, relevant information for restarting a business process or IT system may no longer be accessible. If individual persons have exclusive expert knowledge, even a minimal personnel shortage can result in damage.

2.2. Failure of IT Systems

If the components of an IT system fail (e.g. due to defective hardware or a power failure), all of an organisation's IT operations can be disrupted. This threatens the availability of information affected, and thus of the relevant business processes, as well. Furthermore, important information required for restoration measures may be unavailable.

2.3. Failure of a Wide Area Network (WAN)

A wide area network (WAN) can fail for a variety of reasons. It is thus possible that a WAN failure will only affect individual users, a particular provider, or a certain region. Such failures are often short and only affect business processes and specialised tasks that require high WAN availability. That said, long-lasting failures also occur with relative regularity and may result in severe communication and availability problems.

2.4. Inability to Use a Building

Buildings may unexpectedly become unusable, such as when they have been destroyed partially or completely by a fire, storm, flood, earthquake, or explosion. However, a building can also become unavailable if the police or fire department block off the surrounding area, or if personnel need to leave the building because the electricity, water, sewage, heating, or air conditioning will not be available for a certain period of time (for example).

2.5. Unavailability of a Supplier or Service Provider

If organisations are dependent on service providers, this can quickly lead to interruptions in their operational continuity if an outsourcing service provider or a supplier are partially or completely unavailable. For example, if supplier is no longer able to provide a certain material that is needed for production, the entire production operation may be at risk. The failure of a cloud or e-mail service provider can also severely restrict or even completely interrupt an organisation's own operations. This endangers critical business processes and specialised tasks in particular.

3. Requirements

The specific requirements of module DER.4 *Business Continuity Management* are listed below. As a matter of principle, the BCM Officer is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	BCM Officer
Further responsibilities	Chief Information Security Officer (CISO), Supervisor, Top Management, Human Resources Department

3.1. Basic Requirements

No Basic Requirements are defined for module DER.4 *Business Continuity Management*.

3.2. Standard Requirements

For module DER.4 *Business Continuity Management*, the following requirements correspond to the state-of-the-art technology. They SHOULD be implemented as a matter of principle.

DER.4.A1 Creating a Business Continuity Plan (S)

A business continuity plans SHOULD be drawn up that contains the most important information on the following:

- roles
- immediate measures
- alerts and escalation
- communication plans, basic business continuity plans, and restoration plans

Responsibilities and competencies SHOULD be assigned, communicated, and recorded in the business continuity plan. It SHOULD be ensured that appropriately trained personnel are available in emergencies. Tests and drills SHOULD be performed regularly to check that the safeguards described in the business continuity plan work as intended.

The business continuity plan SHOULD be checked regularly and updated as required. It SHOULD be accessible in an emergency. The business continuity plan SHOULD be supplemented with codes of conduct for special cases (involving a fire, for example). These rules SHOULD be communicated to all employees.

DER.4.A2 Integration of Business Continuity Management and Information Security Management [Chief Information Security Officer (CISO)] (S)

Security management processes SHOULD be coordinated with business continuity management (see DER.2.1 *Security Incident Handling*).

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.4 Business Continuity Management are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

DER.4.A3 Specifying the Scope and the Business Continuity Strategy [Top Management] (H)

The scope of the business continuity management system at hand SHOULD be clearly specified. The respective organisation's Top Management SHOULD specify a business continuity strategy that states the goals to be reached and the level of risk considered acceptable.

DER.4.A4 Policy for Business Continuity Management and Acceptance of Overall Responsibility by Top Management [Top Management] (H)

The Top Management SHOULD adopt a policy for business continuity management. This SHOULD include the essential aspects of business continuity management. The business continuity policy SHOULD be checked regularly and revised when necessary. All employees SHOULD be informed of its provisions.

DER.4.A5 Establishing a Suitable Organisational Structure for Business Continuity Management [Top Management] (H)

Roles for business continuity management SHOULD be appropriately defined for the circumstances of the organisation in question. This SHOULD be documented in writing together with the tasks, obligations, and competencies of the roles. Qualified employees

SHOULD be appointed to all the roles involved in the organisation's business continuity management. The organisational structure in business continuity management SHOULD be regularly checked to ensure it is effective, efficient, and fit for purpose.

DER.4.A6 Providing Adequate Resources for Business Continuity Management [Top Management] (H)

The financial, technical, and personnel resources provided SHOULD be sufficient to achieve an organisation's intended goals in business continuity management. The BCM Officer and the members of the business continuity management team SHOULD be allocated sufficient time to perform their tasks.

DER.4.A7 Creating a Contingency Concept [Top Management] (CIA)

All critical business processes and resources SHOULD be identified (e.g. based on a business impact analysis, or BIA). The most important and relevant risks to critical business processes and specialised tasks and the resources they require SHOULD be identified. The strategies to be used to treat risks SHOULD be specified for each identified risk. An organisation SHOULD develop continuity strategies that enable its critical business processes to be restored and restarted within the required time. A contingency concept SHOULD be drawn up. Contingency plans and safeguards SHOULD also be developed and implemented that enable an effective emergency response and quick recovery of the critical business processes. The contingency concept SHOULD include considerations of information security and elaborate on corresponding security concepts for business continuity solutions.

DER.4.A8 Integrating Employees into the Business Continuity Management Process [Supervisor, Human Resources Department] (H)

All employees SHOULD receive appropriate awareness training on business continuity management on a regular basis. There SHOULD be a training and awareness concept for business continuity management. The employees on the business continuity management team SHOULD receive regular training to hone the skills they need.

DER.4.A9 Integrating Business Continuity Management into Organisation-Wide Procedures and Processes [Top Management] (H)

It SHOULD be ensured that business continuity aspects are taken into account in all of an organisation's business processes and specialised tasks. The processes, requirements and responsibilities in business continuity management SHOULD be coordinated with risk management and crisis management.

DER.4.A10 Tests and Emergency Drills [Top Management] (H)

Regular and event-based testing and drills of all essential emergency measures and emergency plans SHOULD be carried out in an appropriate manner. The time frame and technical coverage of all drills SHOULD be documented in an overall drill plan. Business continuity management SHOULD have adequate resources available for planning, designing, executing, and assessing tests and drills.

DER.4.A11 ELIMINATED (H)

This requirement has been eliminated.

DER.4.A12 Documentation in the Business Continuity Management Process (H)

The sequence of events in the business continuity management process, the results of the work done in each of the phases, and all major decisions SHOULD be documented. An established procedure SHOULD ensure that these documents are regularly updated. Furthermore, access to the documentation SHOULD be limited to authorised persons.

DER.4.A13 Checking and Controlling the Business Continuity Management System [Top Management] (H)

The Top Management of the organisation at hand SHOULD regularly obtain information on the status of its business continuity management system through management reports. It SHOULD therefore review and assess the business continuity management system on a regular basis and make any necessary corrections.

DER.4.A14 Regular Checking and Improvement of Business Continuity Safeguards [Top Management] (H)

All business continuity safeguards SHOULD be checked regularly or in case of major changes to see if they are still being adhered to and correctly implemented. Whether they are still suitable to achieve the defined objectives SHOULD be checked.

During this process, it SHOULD be determined whether technical safeguards are implemented and configured correctly, and whether organisational safeguards are implemented effectively and efficiently. In case of deviations, the causes of defects SHOULD be identified and measures for improvement initiated. The organisation's Top Management SHOULD approve the summary of results. Furthermore, a process that controls and monitors whether and how measures for improvement are implemented SHOULD be established. Delays SHOULD be reported promptly to Top Management.

The organisation's Top Management SHOULD specify how to coordinate the reviews. These examinations SHOULD be planned so that no relevant parts are skipped. In particular, the examinations performed in the areas of auditing, IT, security management, information security management, and business continuity management should be coordinated with each other. To this end, regulations SHOULD be in place that define who should which safeguards and when.

DER.4.A15 Assessing the Performance of the Business Continuity Management System [Top Management] (H)

The performance and effectiveness of a business continuity management system SHOULD be assessed regularly. Measurement and assessment criteria such as key performance indicators SHOULD be defined for this purpose. These metrics SHOULD be determined regularly and compared against suitable previous values, including (at minimum) the previous year's values. If the values deviate in a negative way, the causes SHOULD be identified and measures for improvement defined. The results of the assessment SHOULD be reported to Top Management.

Top management SHOULD define the safeguards to be included in the further development of the business continuity management system. All Top Management decisions SHOULD be documented and the previous records updated.

DER.4.A16 Contingency Planning and Emergency Response Planning for Outsourced Components [Top Management] (H)

Contingency planning and emergency response planning for outsourced components SHOULD include regular reviews of the business continuity management systems of the respective suppliers and service providers with respect to the contracts signed with them. The processes in place SHOULD also be coordinated and, if applicable, performed together with the suppliers and outsourcing service providers in business continuity tests and drills.

The results and assessments SHOULD be exchanged regularly between suppliers and service provides and the Top Management of the organisation in question. The assessments SHOULD also include any possible measures for improvement.

4. Additional Information

4.1. Useful resources

The International Organization for Standardization (ISO) provides guidelines for ensuring information security in the event of an emergency in ISO/IEC 27001:2013, “Information Technology - Security Techniques – Information Security Management Systems – Requirements” (annex A17, “Information Security Aspects of Business Continuity Management”).

The International Organization for Standardization (ISO) provides a framework for business continuity management in the standard ISO/IEC 22301:2012, “Societal Security – Business Continuity Management Systems – Requirements”. The requirements from the aforementioned standard ISO/IEC 27001:2013 (for example) can be integrated into this standard.

BSI Standard 100-4, “Business Continuity Management”, describes how a BCM can be established, maintained, and continuously improved.

The implementation framework (UMRA) published by the BSI on business continuity management in line with BSI Standard 100-4 contains further auxiliar resources to facilitate the establishment of a BCMS.

In addition, the web course “Business Continuity Management” provides an introduction to the topic in line with BSI Standard 100-4.

In “The Standard of Good Practice for Information Security”, the Information Security Forum (ISF) provides specifications on business continuity in the category BC (Business Continuity). Among other things, it requires that a continuity strategy be coordinated with a corresponding information security strategy.

In its Special Publication 800-34, Rev. 1, “Contingency Planning Guide for Federal Information Systems”, the National Institute of Standards and Technology (NIST) provides a guide for

establishing continuity planning for (federal) information systems, which also incorporates information security. This document also provides information on interrelationships between continuity planning for information systems and other types of plans related to security and emergency management (e.g. a business continuity plan).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module DER.4 *Business Continuity Management*.

G 0.11 Failure or Disruption of Service Providers

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

APP.1.1 Office Products

1. Description

1.1. Introduction

Office products primarily comprise applications that are used to create, edit or view documents. They include the free LibreOffice applications and the proprietary Microsoft Office applications used in many organisations. For the majority of organisations, Office products are necessary basic IT equipment. Among other things, they comprise word processing, spreadsheets, presentation creation, and drawing programs, as well as simple database systems.

1.2. Objective

The objective of this module is to protect the information processed and used by means of Office products. Achieving this involves special requirements with regard to how the components of Office products function. The module thus illustrates preconditions that should be met in order to protect Office products against specific threats.

1.3. Scoping and Modelling

Module APP.1.1 *Office Products* applies to every Office product used to view, edit or create documents.

This module considers the use of Office products from the perspective of an IT operation department and provides information for users as to how Office products should be used. As a supplement to this module, the requirements of the generic module APP.6 *General Software* must also be implemented. E-mail applications are not considered in this module. The relevant requirements are covered in module APP.5.3 *General E-Mail Clients and Servers*. When using integrated database systems such as Base in LibreOffice or Access in Microsoft Office, module APP.4.3 *Relational Database Systems* must be considered. This module also does not include any pure cloud office applications, such as the Docs and Sheets applications in Google's G Suite. Requirements for cloud applications are defined in module OPS.2.2 *Cloud Usage*.

2. Threat Landscape

For module APP.1.1 *Office Products*, the following specific threats and vulnerabilities are of particular importance.

2.1. Poor Adaptation of Office Products to an Organisation's Requirements

If Office products are procured or customized without considering the requirements of this software, operations can be significantly disrupted. For example, existing templates and documents may not be compatible or interoperable with business partner applications. If Office products are not adapted to an organisation's requirements, this may cause reduced performance, failures, and errors within business processes.

2.2. Harmful Content in Office documents

In many cases, Office documents can include different “active content” or macros that can be used for complex automation processes. However, active content can also contain malicious code that is executed when a document is opened. Malicious functions of this kind in Office documents can manipulate other data and programs, as well as the affected documents themselves. Malicious code can also spread further. This may impair or block the functions of all the business processes affected at an organisation. In the worst case, the manipulation remains undetected, resulting in vulnerabilities and the processing of falsified information.

2.3. Loss of Integrity of Office Documents

The integrity of Office documents can be corrupted if unintentional or deliberate changes are made to their contents. If Office products are handled carelessly or users do not know how to handle Office documents, undetected changes may be made to them. This is particularly problematic if the documents are used in production environments. If documents that have been falsified continue to be used without this being recognised, the wrong decisions may be made or an organisation's image may be damaged.

3. Requirements

The specific requirements of module APP.1.1 *Office Products* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	User

3.1. Basic Requirements

For module APP.1.1 *Office Products*, the following requirements MUST be met as a matter of priority:

APP.1.1.A1 ELIMINATED (B)

This requirement has been eliminated.

APP.1.1.A2 Limiting Active Content (B)

The automatic execution of embedded active content MUST be disabled. If it is nevertheless necessary to run active content, care MUST be taken to ensure that active content is only run when it comes from trusted sources. All users MUST be instructed about features that restrict active content.

APP.1.1.A3 Secure Opening of Documents from External Sources [User] (B)

All documents obtained from external sources MUST be scanned for malware before they are opened. All file formats considered problematic and those not required within an organisation MUST be prohibited. They SHOULD be blocked if possible. Technical safeguards SHOULD be implemented to enforce the scanning of documents from external sources.

APP.1.1.A4 ELIMINATED (B)

This requirement has been eliminated.

APP.1.1.A17 Awareness of Specific Office Properties (B)

Appropriate efforts MUST be taken to make all users aware of the threat posed by active content. Appropriate efforts MUST also be taken to make all users aware of how documents from external sources are to be handled.

Users SHOULD be informed about the capabilities and limits of the security functions of the software employed and the storage formats used. Users SHOULD be trained on the features they can use to protect documents from subsequent modification and editing.

Users SHOULD be made aware of how the encryption functions in Office products are to be handled.

3.2. Standard Requirements

For module APP.1.1 *Office Products*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.1.1.A5 ELIMINATED (S)

This requirement has been eliminated.

APP.1.1.A6 Testing New Versions of Office Products (S)

New versions of Office products SHOULD be tested for compatibility with established tools such as macros, document templates, or organisation forms prior to productive use (see *OPS.1.1.6 Software Tests and Approvals).* It SHOULD be ensured that important tools will continue to function as they should with each new software version. If compatibility issues are detected, appropriate solutions SHOULD be found for the tools affected.

APP.1.1.A7 ELIMINATED (S)

This requirement has been eliminated.

APP.1.1.A8 ELIMINATED (S)

This requirement has been eliminated.

APP.1.1.A9 ELIMINATED (S)

This requirement has been eliminated.

APP.1.1.A10 Regulations for Software Development by End Users (S)

For software development based on Office applications (e.g. with macros), binding regulations SHOULD be established (see also APP.1.1.A2 *Limiting Active Content)*. First, every organisation SHOULD make a policy decision as to whether or not it wants to allow in-house development of this kind by end users at all. The decision SHOULD be documented in the corresponding security policies. If custom developments are permitted, a process for handling corresponding features of the Office products SHOULD be created for the end users. Responsibilities SHOULD be clearly defined. All information pertaining to the applications created SHOULD be documented. Current versions of the regulations SHOULD be made available to and observed by all affected users in a timely manner.

APP.1.1.A11 Controlled Use of Extensions for Office Products (S)

All add-ons and extensions for Office products SHOULD be tested in the same way as new versions prior to productive use. This testing SHOULD only be carried out on isolated test systems. The tests SHOULD check if the extensions have any adverse effects on the Office products and IT systems in operation. The tests of the extensions in use SHOULD follow a defined test plan. This test plan SHOULD be designed in such a way that third parties can understand the procedure.

APP.1.1.A12 No Cloud Storage [User] (S)

The cloud storage features integrated into some Office products SHOULD be disabled as a matter of principle. All cloud drives SHOULD be disabled. All documents SHOULD be stored by users on file servers centrally managed by the organisation. Specialised applications SHOULD be used to share documents with third parties. These applications SHOULD at least encrypt the storage and transmission of data and have a suitable system for user and rights management.

APP.1.1.A13 Use of Viewer Features [User] (S)

Data from potentially unsafe sources SHOULD be automatically opened in a protected mode. Users SHOULD NOT be allowed to disable this feature. A list of trustworthy places from which content can be opened and edited directly SHOULD be defined.

In the protected mode, it SHOULD NOT be possible to edit data directly. Active content such as macros and scripts SHOULD NOT be executed automatically in the protected mode. Only general navigation SHOULD be allowed. When documents are only to be viewed, appropriate viewer applications SHOULD be used if available.

APP.1.1.A14 Protection Against Subsequent Changes to Documents [User] (S)

Depending on their intended use, documents SHOULD be suitably protected against subsequent modification.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.1.1 *Office Products* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.1.1.A15 Use of Encryption and Digital Signatures (H)

Data that requires increased protection SHOULD only be stored and transmitted in encrypted form. Before using an encryption method integrated into an Office product, it SHOULD be checked to ensure that it offers sufficient protection. In addition, a process SHOULD be used that supports the digital signing of macros and documents.

APP.1.1.A16 Checking Document Integrity (H)

When storing or transmitting data that requires increased protection, appropriate integrity checks SHOULD be used. Cryptographic procedures SHOULD also be used for data that requires protection against manipulation.

4. Additional Information

4.1. Useful Resources

The BSI has published the following documents on the secure configuration of Microsoft Office 2013/2016/2019 in “BSI Publications on Cyber Security”:

- BSI-CS 135: Secure Configuration of Microsoft Office 2013/2016/2019
- BSI-CS 136: Secure Configuration of Microsoft Excel 2013/2016/2019
- BSI-CS 137: Secure Configuration of Microsoft PowerPoint 2013/2016/2019
- BSI-CS 138: Secure Configuration of Microsoft Word 2013/2016/2019
- BSI-CS 139: Secure Configuration of Microsoft Outlook 2013/2016/2019

- BSI-CS 140: Secure Configuration of Microsoft Access 2013/2016/2019
- BSI-CS 141: Secure Configuration of Microsoft Visio 2013/2016/2019

The International Organization for Standardization (ISO) provides specifications that apply to the operation of Office products in the ISO/IEC 27001:2013 standard (Annex A, A.9.4 System and application access control and A.12.5 Control of operational software).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.1.1 *Office Products*.

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.1.2 Web Browsers

1. Description

1.1. Introduction

Web browsers are application programs that can access (hypertext) documents, images, video, audio, and other data formats on the Internet for processing, viewing, output, and storage on local IT systems. Web browsers can also transmit data to the Internet.

Today, stationary and mobile clients are unthinkable without web browsers because many private and business applications use corresponding content. At the same time, online content is becoming more and more diverse. Most websites use embedded videos, animated elements, and other live content. State-of-the-art web browsers cover a large spectrum of further functions through the integration of plug-ins and external libraries. In addition, there are extensions for certain functions, data formats, and content. However, the complexity of state-of-the-art web browsers also comes with a great deal of potential for serious design errors and technical vulnerabilities. It increases possible risks pertaining not only to attacks from the Internet, but to programming and operating errors, as well.

The risks to data confidentiality and integrity are also significant. Moreover, such vulnerabilities threaten the availability of entire IT systems. As a matter of principle, Internet content must thus be considered untrustworthy from a web browser perspective.

1.2. Objective

The objective of this module is to describe security requirements for web browsers used on clients—that is, on stationary and mobile IT systems, including tablets and smartphones.

1.3. Scoping and Modelling

APP.1.2 *Web Browsers* must be applied once to every web browser.

It includes basic security requirements to be considered and met when installing and operating web browsers to access data from the Internet.

Web browsers are some of the most commonly used applications. They access unchecked, potentially malicious data on the Internet and thus provide a gateway for attackers to spread to other parts of operating systems. In order to safeguard operating systems, the requirements of the modules in the layers SYS.2 *Desktop Systems* and SYS.3.2 *Tablets and Smartphones* should be met.

Web applications used with browsers, along with the servers that provide such applications, are addressed in the modules APP.3.1 *Web Applications and Web Services* and APP.3.2 *Web Servers*.

General requirements for the safe use of software are not covered in this module. These are included in APP.6 *General Software,* which should be used in addition to this module.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module APP.1.2 *Web Browsers*, the following specific threats and vulnerabilities are of particular importance.

2.1. Execution of Malicious Code by Web Browsers

Web browsers regularly download data from untrusted sources. Such data may contain executable malicious code that can exploit vulnerabilities and infect the user's IT system without their knowledge.

This may include code (in JavaScript or WebAssembly, for example) that can be directly executed by the web browser. It can also involve the executable code of a plug-in or an extension in connection with the browser and Java or parts of PDF documents, for example. Finally, code can be downloaded by a web browser onto a client and executed there outside of the browser's process. A failure to make adequate use of the basic protection mechanisms of state-of-the-art web browsers threatens the confidentiality, integrity, and availability of information or services on the client side, and potentially in any connected networks, as well.

2.2. Exploit Kits

Lists of vulnerabilities and exploit kits make it significantly easier to develop custom malware. Cyber attacks can be automated to allow the use of drive-by downloads or other methods of distribution by simple means that require no expert knowledge. Attackers may exploit known vulnerabilities of a web browser or related resources or extensions to prepare subsequent attacks, or to load and install malicious code on a client. Malicious code loaded onto clients in this way often causes further malware to be loaded, which is then executed on the clients with user privileges.

2.3. Eavesdropping on Internet Communications

The basic security of communication on the Internet depends to a large extent on the authentication methods used and the encryption of data during transmission.

In implementing these methods, it is possible for errors to be made that prevent effective authentication and encryption. Furthermore, many web services still offer outdated encryption methods. As a result, attackers can bypass server authentication techniques, and communications or data may not be sufficiently encrypted. This may allow unauthorised individuals to access or modify information as it is being transmitted. In the past, certification bodies have also been compromised, allowing attackers to obtain certificates for third-party websites.

2.4. Loss of Integrity in Web Browsers

If web browsers, plug-ins, or extensions are obtained from untrustworthy sources, malicious functions may be inadvertently executed without being noticed. For example, attackers may falsify browser components such as toolbars to lure users to manipulated copies of webpages that are used for phishing attacks. Malicious extensions may also manipulate the content of viewed webpages or collect data and send it to the attacker.

2.5. Loss of Privacy

If web browsers are not securely configured, sensitive data can be disclosed to unauthorised third parties inadvertently or deliberately. Passwords may also be unintentionally forwarded to others. If cookies, passwords, histories, input data, and search requests are stored or unnecessary extensions are activated, it will be easier for third parties or malware to access and misuse this data.

3. Requirements

The specific requirements of module APP.1.2 *Web Browsers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	User

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

APP.1.2.A1 Use of Basic Security Mechanisms (B)

Any web browser used MUST ensure that every instance and process can only access its own resources (sandboxing). Webpages MUST be isolated from each other in independent processes, or at least in their own threads. Plug-ins and extensions MUST also be executed in isolated areas.

Any web browser used MUST implement the Content Security Policy (CSP). The current highest level of the CSP SHOULD be met.

Browsers MUST support same-origin policy and subresource integrity safeguards.

APP.1.2.A2 Support for Secure Communication Encryption (B)

Web browsers MUST support a secure version of Transport Layer Security (TLS). Connections to web servers MUST be encrypted with TLS whenever this is supported by the web server in question. Insecure versions of TLS SHOULD be deactivated. Web browsers MUST support and implement the HTTP Strict Transport Security (HSTS) security mechanism according to RFC 6797.

APP.1.2.A3 Use of Trusted Certificates (B)

If a web browser provides its own list of trusted root certificates, it MUST be ensured that only administrators can change them. If this is not possible by means of technical safeguards, users MUST be prohibited from changing this list. It MUST also be ensured that web browsers can revoke certificates locally.

Web browsers MUST comprehensively check the validity of server certificates using the public key while taking the respective validity periods into account. Web browsers MUST also verify the lock status of server certificates. The certificate chain, including the root certificate, MUST be verified.

Web browsers MUST indicate to the user in a clear and visible manner whether communication is taking place in plain text or in an encrypted manner. Web browsers SHOULD be able to show the user the server certificate in use upon request. Web browsers MUST alert the user when certificates are missing, invalid, or revoked. In such cases, the web browser in use MUST terminate the connection until the user explicitly confirms it.

APP.1.2.A4 ELIMINATED (B)

This requirement has been eliminated.

APP.1.2.A6 Password Management in Web Browsers (B)

If a password manager is used in a web browser, it MUST create a direct and unique relationship between each webpage and the password stored for it. The stored passwords MUST be encrypted. It MUST be ensured that the passwords stored in the password manager can only be accessed after entering a master password. Furthermore, it MUST be ensured that the authentication for password-protected access is only valid only for the current session.

The IT Operation Department MUST ensure that web browsers allow users to delete stored passwords.

APP.1.2.A13 Use of DNS over HTTPS (B)

An organisation MUST check whether the browsers in use employ DNS-over-HTTPS (DoH). Whether or not the function should be used MUST be specified.

If an organisation uses DNS servers as resolvers that are accessed over untrusted networks, DoH SHOULD be used. If DoH is used, the organisation MUST specify a trusted DoH server.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

APP.1.2.A5 ELIMINATED (S)

This requirement has been eliminated.

APP.1.2.A7 Data Economy in Web Browsers [User] (S)

Cookies from third parties SHOULD be refused in web browsers. It SHOULD be possible for users to delete stored cookies.

The auto-complete function for data SHOULD be deactivated. If this function is nevertheless used, the user SHOULD be able to delete the corresponding data. The user SHOULD also be able to delete the web browser's history data.

If available, a web browser's synchronisation with cloud services SHOULD be deactivated. Telemetry functions and the automatic sending of crash reports, URL entries, and search entries to a browser's provider or other external parties SHOULD be disabled whenever possible.

Location sharing and peripheral devices such as microphones or webcams SHOULD only be enabled for websites on which they are absolutely necessary. Browsers SHOULD offer the option to configure and deactivate WebRTC, HSTS, and JavaScript.

APP.1.2.A8 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

APP.1.2.A9 Using an Isolated Web Browser Environment (H)

In case of increased protection needs, web browsers SHOULD be used that run in an isolated environment such as ReCoBS or on dedicated IT systems.

APP.1.2.A10 Using the Private Mode [User] (H)

In case of increased confidentiality requirements, web browsers SHOULD be run in private mode so that no information or content will be stored permanently on the user's IT system. Browsers SHOULD be configured so that local content will be deleted once a browser is closed.

APP.1.2.A11 Checking for Malicious Content (H)

Web browsers SHOULD check the Internet addresses accessed by the user for potentially malicious content. Web browsers SHOULD warn the user if information on malicious content is present. It SHOULD NOT be possible to establish a connection that is classified as malicious. The procedure used for checking MUST NOT infringe on provisions of data protection or the protection of classified information.

APP.1.2.A12 Two-Browser Strategy (H)

If a web browser in use has unresolved security problems, an alternative browser on a different platform SHOULD be installed as a fallback option for the user.

4. Additional Information

4.1. Useful Resources

- BSI publication on cyber security, BSI-CS 047: “Safeguarding Options When Using Web Browsers”
- Minimum standard of the BSI for the use of SSL/TLS protocol by federal authorities according to Section 8, subsection 1(1) of BSIG
- Minimum standard of the BSI for secure web browsers according to Section 8, subsection 1(1) of BSIG
- Common Criteria Protection Profile for Remote-Controlled Browsers System (ReCoBS): BSI-PP-0040

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module APP.1.2 *Web Browsers*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.39 Malware

G 0.46 Loss of Integrity of Sensitive Information

APP.1.4 Mobile Applications (Apps)

1. Description

1.1. Introduction

Today, smartphones, tablets, and similar mobile devices are also widely used by public authorities and companies. Employees can use them to access their organisation's data and other information and applications at any time regardless of where they are.

Mobile applications (or "apps") are installed and executed on the operating systems used on mobile devices, such as iOS or Android. Apps are usually obtained from app stores. These are operated and maintained by the manufacturers of the operating systems used on mobile devices. In professional environments, however, it is also common for an organisation to develop its own apps and install and manage them on end devices using mobile device management (MDM) solutions. Compared to applications on desktop operating systems, iOS or Android apps are subject to special framework conditions, such as the authorisation management ensured by the operating system.

There is now a large selection of available apps for different mobile operating systems. There are also standardised libraries and development environments that enable apps to be developed quickly compared to conventional applications.

1.2. Objective

The objective of this module is to protect information that is processed with apps on mobile end devices. It also covers the integration of apps into existing IT infrastructure. The module defines requirements for the proper selection and secure operation of apps, regardless of whether they are obtained from an app store or installed by an organisation on its own.

1.3. Scoping and Modelling

Module APP.1.4 *Mobile Applications (Apps)* must be applied to all applications that are used on mobile devices.

The module covers apps on mobile operating systems such as iOS and Android. Requirements that affect the underlying operating systems are not considered here. These requirements are

covered, for example, in the modules SYS.3.2.3 *iOS (for Enterprise)* and SYS.3.2.4 *Android*. Apps are often managed centrally in a mobile device management system. The requirements for such systems are covered in module SYS.3.2.2 *Mobile Device Management (MDM)*.

Similarly, the aspects of specific apps are not discussed in this module. These are covered in the corresponding modules of the APP layer (*Applications*), such as APP.1.2 *Web Browsers*.

Apps often rely on back-end systems or server/application services. For cases in which an organisation operates these back-end systems or servers on its own, please refer to the corresponding modules of the IT-Grundschutz Compendium for security recommendations. These include, for example, APP.3.1 *Web Applications and Web Services* and APP.4.3 *Relational Database Systems*. Modules dealing with general aspects of applications, such as OPS.1.1.6 *Software Tests and Approvals* or APP.6 *General Software*, should also be considered, as these aspects are not covered in this module. The requirements of module CON.8 *Software Development* should be considered when developing in-house apps.

2. Threat Landscape

For module APP.1.4 *Mobile Applications (Apps)*, the following specific threats and vulnerabilities are of particular importance:

2.1. Inappropriate Selection of apps

Selected apps have a strong impact on the information they process, the mobile device used, and often on an organisation's IT infrastructure in general. Failure to consider this when selecting apps can lead to far-reaching problems. The threat is particularly high when dealing with apps that have not been developed specifically for the business processes to be mapped. An app's operating requirements might not be sufficiently considered, for example. Mobile network connections may then prove to be inadequate, or the hardware to be used may not be compatible. In addition, apps may not be suitable if they do not support sufficient long-term stability and planning or are not adequately maintained by the manufacturer.

2.2. Excessive Authorisations

Apps need certain authorisations to access particular functions and services. An app can usually always access a mobile device's Internet connection, for instance. The device's location or address book, on the other hand, are usually subject to separate approval. If apps are used that require authorisations that are too extensive or not sufficiently restricted, it can affect the confidentiality and integrity of the information on the corresponding end device. Apps can also share other data such as locations, photos, or contact and calendar information with unauthorised third parties. They are also able to change or delete data that is stored locally. Finally, apps can also generate costs, such as through telephone calls, sent SMS messages, or in-app purchases.

2.3. Undesired Functions in Apps

Although some app store operators check the apps they offer, they may still contain security vulnerabilities or built-in malicious functions. The risk is particularly high when apps are obtained from untested or unreliable sources. This can threaten the confidentiality, integrity, and availability of the information they process.

2.4. Software Vulnerabilities and Errors in Apps

Apps can contain vulnerabilities that allow attacks on a device either directly or through network connections. Furthermore, many apps stop being maintained by their developers after some time, which means that any security deficiencies detected will no longer be corrected by corresponding updates.

2.5. Insecure storage of local application data

Some apps store data such as documents or user profiles on end devices. If this data is not sufficiently protected, other apps may be able to access it. In addition to data that has been consciously stored, this applies to temporary data, such as information stored in the cache. This data can also be easily accessed by unauthorised persons if an employee loses a device, for example. Furthermore, locally stored information is often not considered in data backup concepts. If this is the case and an end device is lost or stops working, its locally stored data will no longer be available.

2.6. Deriving Confidential Information from Metadata

Apps accumulate a great deal of metadata. This metadata can be used by third parties to gain confidential information such as phone and network connections, transaction data, or web browsing histories. Further information can then be derived, including on the structure of an organisation, its exact locations, and the staff who work there.

2.7. Leaks of Confidential Data

Data is transferred to and from apps in different ways. Mobile operating systems provide various interfaces for this purpose. Users also have different options for exchanging data with an app, such as locally via a memory card, using the clipboard or a device's camera, and other applications. In addition, data can be transferred via cloud services or a server operated by an app or device provider. This may give third parties access to confidential data. Finally, an operating system can also cache data for faster access. This can enable the inadvertent outflow of data or allow attackers to access confidential information.

2.8. Insecure Communication with Back-End Systems

Many apps communicate with back-end systems that exchange data with an organisation's data network. In the case of mobile devices, this data is usually transmitted via insecure means such as mobile networks or WLAN hotspots. If insecure protocols are used for communication with back-end systems, information can be intercepted or manipulated.

2.9. Communication Channels Beyond an Organisation's Infrastructure

If apps can communicate with third parties in an uncontrolled manner, this can create communication channels that an organisation may be unable to identify and monitor. For example, a user could transfer information from an end device to the outside world through a cloud data storage app. The close integration between many apps and social media services also makes it difficult to check whether and how information leaves an end device. These types of communication channels are very hard to trace. This can cause even more problems, such as when a user or organisation is required to archive information or processes.

3. Requirements

The specific requirements of module APP.1.4 *Mobile Applications (Apps)* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner

3.1. Basic Requirements

For module APP.1.4 *Mobile Applications (Apps)*, the following requirements MUST be implemented as a matter of priority:

APP.1.4.A1 Requirements Analysis for the Use of Apps [Process Owner] (B)

During requirements analysis, risks arising from mobile use in particular MUST be considered. The organisation MUST verify that its ability to check and influence the operating system environment of mobile devices is sufficient to facilitate their secure use.

APP.1.4.A2 ELIMINATED (B)

This requirement has been eliminated.

APP.1.4.A4 ELIMINATED (B)

This requirement has been eliminated.

APP.1.4.A5 Minimising and Checking App Authorisations [Process Owner] (B)

Security-relevant authorisation settings MUST be established so that they cannot be changed by users or apps. If this is not technically possible, the authorisation settings MUST be regularly checked and reset.

Before an app is introduced in an organisation, it MUST be ensured that it only has the minimum app authorisations required for its function. Authorisations that are not absolutely necessary MUST be scrutinised and, if necessary, disabled.

APP.1.4.A6 ELIMINATED (B)

This requirement has been eliminated.

APP.1.4.A7 Secure Storage of Local App Data (B)

If apps can access an organisation's internal documents, it MUST be ensured that the local data storage of the app is adequately secured. In particular, access keys MUST be stored in an encrypted form. In addition, a mobile device's operating system MUST NOT be allowed to cache confidential data in other locations.

APP.1.4.A8 Preventing Data Leaks (B)

To prevent unintended instances of apps transmitting confidential data or this data being used to create profiles of users, app communication MUST be appropriately restricted. To this end, communication SHOULD be analysed as part of the testing and approval procedure. Checks SHOULD also be carried out to determine whether an app is writing unwanted log or auxiliary files that may contain confidential information.

3.2. Standard Requirements

For module APP.1.4 *Mobile Applications (Apps)*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.1.4.A3 Distributing Sensitive Apps (S)

Apps developed within an organisation and apps that process sensitive information SHOULD be distributed through the organisation's own app store or MDM solution.

APP.1.4.A9 ELIMINATED (S)

This requirement has been eliminated.

APP.1.4.A10 ELIMINATED (S)

This requirement has been eliminated.

APP.1.4.A11 ELIMINATED (S)

This requirement has been eliminated.

APP.1.4.A12 Secure App Removal (S)

When an app is uninstalled, the data it has stored on external systems (such as those operated by the app provider) SHOULD also be deleted.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.1.4 *Mobile Applications (Apps)* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into

account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.1.4.A13 ELIMINATED (H)

This requirement has been eliminated.

APP.1.4.A14 Support for Additional Authentication Features for Apps (H)

Whenever possible, a second factor SHOULD be employed for user authentication in apps. Here, it SHOULD be ensured that any required sensors or interfaces are present in all the devices used. In addition, biometric procedures SHOULD take into account how resistant the corresponding authentication is to possible forgery attempts.

APP.1.4.A15 Performing Penetration Tests for Apps (H)

Before an app is approved for use, a penetration test SHOULD be performed. All communication interfaces to back-end systems, as well as the local storage of data, SHOULD be examined for possible vulnerabilities. The penetration tests SHOULD be repeated regularly and when major changes are made to the app.

APP.1.4.A16 Mobile Application Management (H)

Whenever possible, a mobile application management solution SHOULD be used for the central configuration of business apps.

4. Additional Information

4.1. Useful Resources

Germany's digital association, Bitkom, has published a decision-making aid for apps and mobile services in companies in the guide entitled "Apps & Mobile Services – Tipps für Unternehmen" [Apps & Mobile Services - Tips for Companies] (2nd edition, 2014).

The Information Security Forum (ISF) has published a paper entitled "Securing Mobile Apps – Embracing Mobile, Balancing Control" (2018).

"NIST Special Publication 800-163: Vetting the Security of Mobile Applications" (2015) also provides extensive information on apps.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security

objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.1.4 *Mobile Applications (Apps)*.

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.42 Social Engineering

APP.2.1 General Directory Service

1. Description

1.1. Introduction

A data network's directory service provides information on various types of objects in a defined manner. Associated attributes can be stored in an object—the first and last name, personnel number, and the name of the IT system pertaining to a particular user ID, for example. This data can then be used by various applications. A directory service and its data are normally administered from a central location.

Some typical areas of application of directory services include:

- Administration of address books, e.g. for telephone numbers, e-mail addresses, and certificates for electronic signatures
- Resource administration, e.g. for IT systems, printers, scanners, and other peripheral devices
- User administration, e.g. for user accounts and user authorisations
- Authentication, e.g. for logging into operating systems or applications

Directory services are optimised for read-only access because data is typically retrieved. Write access for creating, changing, or deleting entries is needed less often.

This type of directory service is especially useful in networks where the number of clients used in the network makes local administration difficult, for example. Without a directory service, it would no longer be possible to ensure that local settings, such as those pertaining to security policies, are being configured reliably due to the considerable effort involved. Administrative tasks within a network—changing passwords, creating accounts, and assigning access rights, for instance—can also be performed more efficiently using a directory service.

1.2. Objective

The objective of this module is to ensure the secure operation of general directory services and the appropriate protection of information processed using such services.

1.3. Scoping and Modelling

Module APP.2.1 *General Directory Service* must be applied to all directory services used.

This module examines general security aspects of directory services. The IT-Grundschutz Compendium includes additional modules for product-specific security aspects that should also be applied to the particular directory service in use. Modules on the server operating systems on which directory services are usually operated can be found in the layer SYS.1 *Servers*.

Directory services should always be included as part of the modules ORP.4 *Identity and Access Management*, OPS.1.1.3 *Patch and Change Management*, CON.3 *Backup Concept*, OPS.1.2.2 *Archiving*, OPS.1.1.5 *Logging*, and OPS.1.1.2 *Proper IT Administration*.

2. Threat Landscape

For module APP.2.1 *General Directory Service*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inadequate Planning of the Use of Directory Services

The security of directory services is based in large part on the security of the underlying operating system, and especially on the security of its file system. Directory services can be installed and operated on many operating systems, and this may result in a wide variety of security settings that need to be configured. This variety requires increased planning and corresponding knowledge of the operating system in question. If the resulting overall solution is very heterogeneous or complex, insufficiently planned use of the directory service may cause vulnerabilities during actual operations. Role-based administration of a directory database is also common in connection with directory services. Individual administrative tasks can also be delegated, which leads to the risk of insecure or inadequate system administration if these tasks are not properly planned.

2.2. Inadequate Planning of Partitioning and Replication in the Directory Service

During partitioning, the directory data of a directory service is distributed among separate areas (partitions). Directory service partitions are generally replicated to ensure better load distribution. Redundant data storage also improves reliability and thereby increases availability. Appropriate planning is therefore also of crucial importance here: while partition and replication settings can be changed later on, doing so can cause problems. If the partitioning and replication of the directory service is planned incorrectly or inadequately, this can have negative effects. It can lead to losses of data as well as to inconsistencies in the data stored, to poor availability of the directory service, to a lower overall system performance, and possibly even to failures.

2.3. Inadequate Planning of Directory Service Access

Managing system and data access rights in the context of a directory service is a very labour-intensive task. In extreme cases, it requires multiple manual steps that can lead to errors and make it difficult to maintain an overview. Inadequate planning regarding whether (and if so, which) data is allowed to be transmitted in plain text may also lead to inconsistencies or contradictions with an organisation's internal security policies. Incorrect planning of the safeguards and security technologies of the directory service to protect confidential data can lead to incompatibilities or even to the failure of the encryption component. This can directly impact confidentiality and integrity.

2.4. Incorrect Administration of System and Data Access Rights

Site access rights to an IT system and data access rights to stored information and IT applications may only be granted in the scope required to perform the corresponding tasks. This also applies to authorisations assigned to users and groups administered by a directory service. If these rights are administered incorrectly, operations can be disrupted if required rights have not been assigned. On the other hand, the granting of rights that exceed those necessary can result in vulnerabilities. If access rights are assigned incorrectly or inconsistently in a directory service, the security of the overall system will be significantly threatened as a result. Administrative rights also are a very critical aspect. Assigning such rights incorrectly could put the entire administration concept in question at risk and, under certain circumstances, even result in the directory system administration becoming blocked.

2.5. Errors in the Configuration of Directory Service Access

In many cases, additional applications such as Internet or intranet applications must access a directory service. Misconfiguration can lead to access rights being assigned incorrectly. A directory service can also be accessed without authorisation, and authentication data can be transmitted in clear text. In such cases, unencrypted information can be intercepted.

2.6. Failure of Directory Services

Technical failures due to hardware or software problems may lead to the failure of directory services or parts thereof. As a consequence, it may be temporarily impossible to access the data stored in the directory. In extreme cases, data may also be lost. As a consequence, business processes and internal processes may be impaired. If functioning copies of the failed parts of a system are available, it will still be possible to gain access, but performance may be limited depending on the network topology at hand.

2.7. Infiltration of Directory Services due to Unauthorised Access

An attacker who is able to successfully circumvent the authentication procedure required by a directory service can then access a large amount of data without authorisation. As a consequence, the entire directory service may be compromised. Furthermore, unauthorised persons may access network resources or services by means of extended authorisations. This

may lead to an attacker circumventing all the defensive safeguards of the directory service. The affected system could then be impaired or even destroyed.

The security of a directory service may also be threatened if anonymous users are allowed. Since their identity is not checked, anonymous users are initially able to send any query to the directory service and obtain at least some information on its structure and content. If anonymous access is permitted, it will also be easier for attackers to conduct DoS attacks on the directory service because they will have more access options that are more difficult to control.

2.8. Improper Configuration of Directory Services

Directory services have numerous functions that support users with very different needs. Incorrect configuration of these numerous functions can lead to unauthorised access to the directory service. If, for example, the default configuration is not sufficiently checked and adapted, authentication information can be transmitted in plain text. Malicious users could tap into unencrypted transmissions of this and other information and misuse it for further attacks.

3. Requirements

The specific requirements of module APP.2.1 *General Directory Service* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner, Data Protection Officer

3.1. Basic Requirements

For module APP.2.1 *General Directory Service*, the following requirements MUST be implemented as a matter of priority:

APP.2.1.A1 Creation of a Security Policy for Directory Services (B)

A security policy MUST be drawn up for the directory service. This policy SHOULD be in agreement with the organisation's overall security concept.

APP.2.1.A2 Planning the Use of Directory Services [Data Protection Officer, Process Owner] (B)

The use of directory services MUST be planned carefully. The specific use of the directory service MUST be defined. It MUST be ensured that the directory service and all applications

using it are compatible. In addition, a model consisting of object classes and attribute types MUST be developed that meets the requirements of the intended types of use. When planning the directory service, Employee Representatives and the Data Protection Officer MUST be involved. A needs-based access control policy MUST be designed for the directory service. In general, the planned directory service structure SHOULD be fully documented. Safeguards SHOULD be planned to prevent the unauthorised collection of data from the directory service.

APP.2.1.A3 Setting Up Access Authorisations for Directory Services [Process Owner] (B)

The tasks pertaining to the administration of the directory service itself and to the actual data administration MUST be clearly separated. The administrative tasks SHOULD be delegated such that overlap is avoided whenever possible. All administrative task areas and authorisations SHOULD be sufficiently documented.

The data access rights of the user and administrator groups MUST be configured and implemented based on the established security policy. If several directory service trees are merged, the resulting effective rights MUST be verified.

APP.2.1.A4 Secure Installation of Directory Services (B)

An installation concept MUST be drawn up in which administration and access authorisations will already be configured when installing the directory service.

APP.2.1.A5 Secure Configuration and Configuration Changes in Directory Services (B)

The directory service MUST be configured securely. In addition to the server, the clients (IT systems and programs) MUST be included in the secure configuration of a directory service infrastructure.

If the configuration of the connected IT systems is to be changed, users SHOULD be informed in good time about the corresponding maintenance work. Backups SHOULD be performed for all affected files and directories prior to any changes to the configuration.

APP.2.1.A6 Secure Operation of Directory Services (B)

The security of the directory service MUST be maintained constantly during operation. All policies, regulations, and processes related to the operation of a directory service system SHOULD be documented. The workstations of directory service administrators MUST be sufficiently secured. Normal users MUST be prohibited from accessing any administration tools.

3.2. Standard Requirements

For module APP.2.1 *General Directory Service*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.2.1.A7 Drawing Up a Security Concept for the Use of Directory Services (S)

The directory service security concept SHOULD specify rules for all the relevant topic areas. The security policies developed on this basis SHOULD be documented in writing and communicated to directory service users.

APP.2.1.A8 Planning of Partitioning and Replication in the Directory Service (S)

The availability and protection needs of the directory service SHOULD be taken into account during partitioning. The partitioning of the directory service SHOULD be documented in writing so that it can be reconstructed manually. Sufficient bandwidth SHOULD be made available to perform replication in a timely manner.

APP.2.1.A9 Selection of Suitable Components for Directory Services [Process Owner] (S)

Suitable components SHOULD be selected for the use of a directory service. A catalogue of criteria SHOULD be drawn up and used as a basis for selecting and acquiring components for the directory service. As part of the planning and design of the directory service, requirements for its security SHOULD be formulated in accordance with its intended use.

APP.2.1.A10 ELIMINATED (S)

This requirement has been eliminated.

APP.2.1.A11 Setting Up Access to Directory Services (S)

Access to a directory service SHOULD be configured according to the security policy at hand. If the directory service is used as a server on the Internet, it SHOULD be protected accordingly by a security gateway. If anonymous users are to be granted extended access rights to individual sub-areas of the directory tree, a separate user account (known as a proxy user) SHOULD be created for anonymous access. The access rights for this proxy user SHOULD be assigned in a sufficiently restrictive manner. They SHOULD also be removed completely if the account is no longer needed. To avoid inadvertently releasing sensitive information, the search function of the directory service SHOULD be appropriately limited in accordance with its intended purpose.

APP.2.1.A12 Monitoring Directory Services (S)

Directory services SHOULD be monitored and logged together with the server on which they are running.

APP.2.1.A13 Protection of Communications with Directory Services (S)

All communications with a directory service SHOULD be encrypted using SSL/TLS. The communication endpoint of the directory service server SHOULD NOT be reachable from the Internet.

Exchanges of data between clients and the directory service server SHOULD be secured. The data that may be accessed SHOULD be defined. To protect the service entries in a service registry in the case of a service-oriented architecture (SOA), all requests sent to the registry SHOULD be checked to see if the user is valid.

APP.2.1.A14 Orderly Decommissioning of a Directory Service [Process Owner] (S)

When decommissioning a directory service, it SHOULD be ensured that the required rights and information continue to be sufficiently available. All other rights and information SHOULD be deleted. Furthermore, the users affected SHOULD be informed when a directory service is being decommissioned. When decommissioning individual partitions of a directory service, it SHOULD be ensured that no other partitions will be affected.

APP.2.1.A15 Migration of Directory Services (S)

In the event of a scheduled migration of directory services, a migration concept SHOULD be drawn up beforehand. The changes that have been made to a directory service scheme SHOULD be documented. Any extensive authorisations that were used to perform the directory service migration SHOULD be reset. The access rights for directory service objects on the systems that were updated to a new version or were obtained from other directory systems SHOULD be updated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.2.1 *General Directory Service* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.2.1.A16 Creation of a Business Continuity Plan for Directory Service Failure (H)

Within the framework of contingency planning, there SHOULD be a need-based business continuity plan for directory services. Business continuity plans SHOULD be in place in case important directory service systems fail. All contingency procedures for the overall system configuration of directory service components SHOULD be documented.

4. Additional Information

4.1. Useful Resources

No further information is available for module APP.2.1 *General Directory Service*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the

second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.2.1 *General Directory Service*.

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.40 Denial of Service

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.2.2 Active Directory

1. Description

1.1. Introduction

Active Directory (AD) is a directory service developed by Microsoft that was introduced for the first time with the Windows 2000 Server operating system. Based on the Active Directory functions available in Microsoft Windows 2000 Server, additional key functions have been added to the service in every release of the Windows Server family of operating systems.

Active Directory is mainly used in networks with Microsoft components. An AD stores information about objects within a network, such as users or IT systems. It makes it easier for users and administrators to provide, organise, use, and monitor this information. Since Active Directory is an object-based directory service, it facilitates the administration of objects and their mutual relationships, which is what constitutes an actual network environment. Active Directory thus provides central control and monitoring capabilities for a given network.

1.2. Objective

This module is designed to help secure Active Directory in normal operations in organisations that use it to administer their infrastructure of Windows systems (client and server).

1.3. Scoping and Modelling

Module APP.2.2 *Active Directory* must be applied to all directory services that are based on Microsoft Active Directory.

This module examines the threats and requirements that apply specifically to Active Directory. General security recommendations for directory services can be found in module APP.2.1 *General Directory Service*. The general requirements described therein are explained in detail and complemented by this module. This module does not repeat the requirements for securing the operating systems of servers and clients used to operate and administrate AD; these are covered, for example, in SYS.1.2.2 *Windows Server 2012* and SYS.2.2.3 *Windows 10 Clients*. This module does not revisit the requirements of the underlying network infrastructure either.

Active Directory should always be included when considering the modules ORP.4 *Identity and Access Management*, OPS.1.1.3 *Patch and Change Management*, CON.3 *Backup Concept*, OPS.1.1.2 *Archiving*, OPS.1.1.5 *Logging* and OPS.1.1.2 *Proper IT Administration*.

2. Threat Landscape

For module *APP.2.2 Active Directory*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inadequate Planning of Security Boundaries

An AD instance generates a forest as a container at the highest level for all domains of the instance. A forest may include one or more domain container objects characterised by a common logical structure, a global catalogue, a scheme, and automatic transitive trust relationships. The forest—not a single tree—is thus the default security boundary within which information is forwarded in AD. If these boundaries are not planned in a conscious and structured manner, information may leak out unintentionally and the organisation's security concept may fail. As a consequence, it may be necessary to establish additional forests if different security requirements apply to certain infrastructural components. However, this makes setup and management even more complex.

2.2. Excessive or Negligent Trust Relationships

If the trust relationships between forests and domains are not regularly evaluated to determine whether they are still needed and justified, problems with authorisations can occur and information can leak out. It is also necessary to regularly check whether these relationships are of the correct type, especially with regard to whether a two-way trust relationship is really necessary and whether the security controls for such relationships are sufficient. In particular, if the Security Identifier (SID) filtration that is active by default is disabled, complex vulnerabilities may arise that are difficult to understand. The same applies if selective authentication is waived for trust relationships between forests.

2.3. Lack of Security Features due to Older Operating Systems and Domain Functional Level

Every new generation of the Windows Server operating system includes additional security features and extensions, including for AD. Furthermore, the default settings are made more secure with every new release. Some of them can be used once the new system has been installed, and others only after the domain or forest functional level has been increased. If older operating systems are used as (primary) domain controllers or outdated domain functional levels are used, up-to-date security functions cannot be employed. This increases the threat of insecure default settings. An insecurely configured domain endangers the information processed therein and makes it easier for third parties to carry out attacks.

2.4. Operation of Additional Roles and Services on Domain Controllers

If other services are operated on a domain controller in addition to AD, this increases the number of potential attacks on these central infrastructure components due to additional possible vulnerabilities and misconfigurations. Such services may be misused inadvertently or wilfully in order to copy or change information without authorisation, for example.

2.5. Insufficient Monitoring and Documentation of Delegated Rights

If the formation of company-specific groups and the delegation of rights to these groups is not systematically planned and implemented, this delegation will be difficult to control. It could then grant much more access than intended, for example, which could be abused by third parties. A lack of regular auditing of groups and their access rights can further exacerbate the problem. Even if standard groups are used and their rights are delegated to their own groups—such as when "account operators" are delegated to help desk employees—more rights are usually granted than are actually needed.

2.6. Insecure Authentication

Legacy (i.e. obsolete) authentication mechanisms in the field of AD, such as LAN Manager (LM) and NT LAN Manager (NTLM) v1, are now considered insecure and can easily be circumvented by attackers under certain conditions. As a consequence, an attacker may obtain or misuse rights without knowing, guessing, or otherwise cracking user passwords, and may thus compromise the domain or parts thereof.

2.7. Overly Powerful or Insufficiently Secure Service Accounts

Application software providers sometimes require AD rights for service accounts to make it easier to test and deploy their products, even though significantly fewer rights are actually required for their operation. Additional rights for service accounts may be misused by attackers in order to access further areas of a domain. Since the credentials of a service that is executed in the context of a service account are stored in the protected memory of the Local Security Authority Subsystem (LSASS), an attacker may extract them there. A single weakly secured service account can thus result in an entire domain being compromised,

particularly if the service account is secured using a weak password. This is because an attacker using Kerberos authentication can easily request a TGS (Ticket Granting Service) ticket in which the password of the service account is processed. The password can then be broken offline using brute force.

2.8. Use of the Same Local Administrator Password on Multiple IT Systems

Local accounts may log into an IT system even if it is not connected to the corresponding domain. If the same credentials are used on several IT systems, the administrator may also log into the other IT systems. This increases the risk of an attacker finding domain credentials with higher rights on one of the IT systems and misusing these to compromise the domain.

3. Requirements

The specific requirements of module APP.2.2 *Active Directory* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner

3.1. Basic Requirements

For module APP.2.2 *Active Directory*, the following requirements MUST be met as a matter of priority:

APP.2.2.A1 Planning Active Directory [Process Owner] (B)

The domain functional level selected MUST be appropriate and as high as possible. The justification for this choice SHOULD be documented appropriately. An access control policy for Active Directory MUST be developed in accordance with the requirements at hand. Administrative delegations MUST be assigned restrictive authorisations that meet the requirements at hand. The planned Active Directory structure, including possible scheme changes, SHOULD be documented in a comprehensible manner.

APP.2.2.A2 Planning of Active Directory Administration [Process Owner] (B)

In large domains, the administrative users MUST be divided in terms of the service and data administration pertaining to Active Directory. Here, the administrative tasks MUST also be distributed in Active Directory according to a delegation model so that there is no overlap.

APP.2.2.A3 Planning of Group Policy in Windows (B)

There MUST be a concept for configuring group policies. Multiple overlaps MUST be avoided whenever possible in the group policy concept. It MUST be possible to recognise exceptions to the group policy concept in the documentation. All group policy objects MUST be protected by restrictive access rights. Secure specifications MUST be defined for the parameters in all group policy objects.

APP.2.2.A4 ELIMINATED (B)

This requirement has been eliminated.

APP.2.2.A5 Hardening Active Directory (B)

Built-in accounts MUST be configured with complex passwords. They MUST ONLY be used as emergency accounts. Privileged accounts MUST be members of the “protected users” group. Managed service accounts (for groups) MUST be used for service accounts.

All domain controllers MUST be assigned restrictive access rights at the operating system level. The Active Directory restore mode MUST be protected by an appropriate password. Work in this mode SHOULD only be performed in compliance with the two-person principle.

A map of the domain controller SHOULD be created on a regular basis. The authorisations for the “Everyone” group MUST be restricted. The domain controller MUST be protected against unauthorised restarts.

The policies for domains and domain controllers MUST include secure settings for passwords, account lockout, Kerberos authentication, user rights, and monitoring. A sufficient size MUST be set for the security log of the domain controller. If external trust relationships exist with other domains, user authorisation data MUST be filtered and anonymised.

APP.2.2.A6 Maintaining the Operational Continuity of Active Directory (B)

All trust relationships in AD MUST be evaluated at regular intervals.

The domain administrators group MUST be empty or as small as possible. Accounts that are no longer used MUST be disabled in AD. They SHOULD be deleted after a reasonable retention period has expired.

All the necessary parameters of Active Directory SHOULD be kept up to date and documented comprehensibly.

APP.2.2.A7 Implementation of Secure Administration Methods for Active Directory [Process Owner] (B)

It MUST be possible to clearly trace every account to an employee.

The number of service administrators and data administrators for Active Directory MUST be limited to the required minimum of trustworthy persons.

The default “Administrator”" account SHOULD be renamed. An “Administrator” account without privileges SHOULD be created.

It MUST be ensured that the administration of service administrator accounts is only performed by members of the Service Administrator group. The “Account Operators” group SHOULD be empty.

Administrators SHOULD only be assigned to the “Scheme Administrators” group temporarily for the time required to change the scheme. For the groups “Organisational Administrators” and “Domain Administrators”, the dual-control principle SHOULD be established for administration of the root domain.

It MUST be ensured that the “Administrators” and “Domain Administrators” groups are also owners of the domain root object of the domain in question.

The use of domain-local groups for controlling the read privileges of object attributes SHOULD be avoided.

The recycle bin of AD SHOULD be enabled.

In large organisations, an enterprise identity management solution SHOULD be used in order to ensure that the rights of all users comply with the defined specifications.

3.2. Standard Requirements

For module APP.2.2 *Active Directory*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.2.2.A8 Configuration of Secure Channel in Windows (S)

Secure Channel SHOULD be configured in Windows according to the security requirements and the local conditions at hand. All the relevant group policy parameters SHOULD be taken into account in the process.

APP.2.2.A9 Authentication Protection When Using Active Directory (S)

The Kerberos authentication protocol SHOULD be used consistently in the Active Directory environment. If NTLMv2 is used temporarily for compatibility reasons, the migration to Kerberos SHOULD be planned and scheduled. LM authentication SHOULD be disabled. SMB data traffic SHOULD be signed. Anonymous access to domain controllers SHOULD be prevented.

APP.2.2.A10 Secure Use of DNS for Active Directory (S)

Integrated DNS zones or the secure dynamic updating of DNS data SHOULD be used. Access to the configuration data of the DNS server SHOULD only be permitted from administrative accounts. The DNS cache on DNS servers SHOULD be protected against unauthorised changes. Access to the DNS service of the domain controllers SHOULD be restricted to the necessary minimum. Network activities related to DNS requests SHOULD be monitored. Access to the DNS data in Active Directory SHOULD be restricted to administrators using ACLs.

Secondary DNS zones SHOULD be avoided. At minimum, the zone file SHOULD be protected against unauthorised access.

If IPsec is being used to protect DNS communications, sufficient data throughput SHOULD be ensured within the network.

APP.2.2.A11 Monitoring Active Directory Infrastructure (S)

Changes at the domain level and in the overall structure of Active Directory SHOULD be monitored, logged, and evaluated.

APP.2.2.A12 Backups for Domain Controllers (S)

There SHOULD be a backup and recovery policy for domain controllers. The backup software used SHOULD be explicitly approved by the provider for use in backing up the data of domain controllers. A separate backup account with service administrator rights SHOULD be set up for the domain controllers. The number of members of the “Backup Operators” group SHOULD be restricted to the required minimum. Access to the AdminSDHolder object SHOULD be placed under special protection in order to protect the authorisations.

The data of the domain controllers SHOULD be backed up at regular intervals. Here, a method that avoids legacy objects whenever possible SHOULD be used.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.2.2 *Active Directory* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.2.2.A13 ELIMINATED (H)

This requirement has been eliminated.

APP.2.2.A14 Use of Dedicated Privileged Administration Systems (H)

The administration of Active Directory SHOULD be limited to dedicated administration systems. These SHOULD be subject to particularly strong hardening based on their limited tasks.

APP.2.2.A15 Separation of Administration and Production Environments (H)

Particularly critical systems such as domain controllers and domain administration systems SHOULD be placed in a separate forest with a unilateral trust relationship towards the production forest.

4. Additional Information

4.1. Useful Resources

The website "Active Directory Security" (https://adsecurity.org) contains a great deal of further information about AD security.

Microsoft itself provides additional information about Active Directory and its security aspects:

- Enhanced Security Administrative Environment: https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access
- Privileged Access Workstations: http://download.microsoft.com/download/9/3/9/9392A4D2-D530-4344-8447-4A7CF1C01AEE/Privileged%20Access%20Workstation_Datasheet.pdf
- Einstiegspunkt Active Directory für Windows Server 2012 (R2): https://technet.microsoft.com/en-us/library/dn283324.aspx
- Introduction to Active Directory for Windows Server 2008 R2: https://technet.microsoft.com/en-us/library/dd378801.aspx

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.2.2 *Active Directory*.

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.40 Denial of Service

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.2.3 OpenLDAP

1. Description

1.1. Introduction

OpenLDAP is a freely available directory service that provides information on any objects, such as users or IT systems, in a defined manner within a data network. The information can include simple attributes—the names or numbers of objects, for example—but also complex formats such as photos or certificates for electronic signatures. The typical application scenarios include address books and user administration systems.

OpenLDAP is a reference implementation for a server service within the framework of the Lightweight Directory Access Protocol (LDAP). Since it is open-source software, OpenLDAP can be installed on a variety of operating systems and is one of the most widely used directory services. Overlays are a special feature of OpenLDAP. Overlays add numerous functions to OpenLDAP and are also used for basic functions such as logging, replication, and maintaining integrity.

1.2. Objective

The objective of this module is to facilitate the secure operation of directory services based on OpenLDAP and appropriate protection of the information processed using these services.

1.3. Scoping and Modelling

Module APP.2.3 *OpenLDAP* must be applied to every OpenLDAP directory.

This module examines the threats and requirements that apply specifically to OpenLDAP. It does so based on version 2.4 of OpenLDAP. General security recommendations for directory services can be found in module APP.2.1 *General Directory Service*. These must also be taken into consideration. The requirements described therein are explained in detail and expanded upon in this module.

OpenLDAP should always be considered as part of the modules ORP.4 *Identity and Access Management*, OPS.1.1.3 *Patch and Change Management*, CON.3 *Backup Concept*, OPS.1.1.2 *Archiving*, OPS.1.1.5 *Logging* and OPS.1.1.2 *Proper IT Administration*.

2. Threat Landscape

For module APP.2.3 *OpenLDAP*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inadequate Planning of OpenLDAP

OpenLDAP can be used in conjunction with numerous other applications. These applications can access and usually modify directory service information. If the use of OpenLDAP is planned insufficiently (or not at all), the following problems may occur:

- If the back ends and the associated directives and parameters are selected incorrectly, they will unintentionally influence the functions that OpenLDAP can offer. If, for example, the "back-ldif" back end is used for data storage to avoid the installation of an additional database, only rudimentary functions of the directory service will be available. This will make it impossible to appropriately manage a large number of users or other objects.
- If the use of overlays is poorly planned, operations that are not needed in OpenLDAP may be performed or other functions may be impaired. For instance, access to the directory service can be incorrectly logged or not logged at all if the debug function of the slapd server itself and the auditlog and accesslog overlays are insufficiently planned.
- OpenLDAP can be run in an unsuitable system environment. If a distributed file system such as the Network File System (NFS) is used to store OpenLDAP data, OpenLDAP file functions will not be available. An example of this is the locking function used by many databases, which allows the directory service database to be locked if several users want to access the database in parallel.
- Incompatible versions of one or more applications could access the databases used by OpenLDAP. For example, the LDAPv3 protocol specifications are not met by OpenLDAP without additional extensions. In addition, there can be connection problems with the applications if the wrong version of a program is used that is not compatible with OpenLDAP.

2.2. Inadequate Separation of offline and online access to OpenLDAP

The data managed by OpenLDAP (objects in the directory service and the configuration settings) can be accessed in various ways. Here, the offline and online access options fulfil partially or completely identical functions. For online access, the LDAP protocol is used to access the data; for offline access, the database files are accessed directly. If these options are mixed or the respective method of operation for offline or online access is not understood, numerous errors can occur. As a result, the restored database will be inconsistent for OpenLDAP and thus no longer usable.

3. Requirements

The specific requirements of module APP.2.3 *OpenLDAP* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The

Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module APP.2.3 *OpenLDAP*, the following requirements MUST be implemented as a matter of priority:

APP.2.3.A1 Planning and Selecting Back Ends and Overlays for OpenLDAP (B)

The use of OpenLDAP in an organisation MUST be carefully planned. If OpenLDAP is to be used together with other applications, the planning, configuration, and installation of applications and OpenLDAP MUST be coordinated. The version of the database used for data storage MUST be checked to ensure it is compatible. Back ends and overlays for OpenLDAP MUST be selected restrictively. It MUST be ensured that the OpenLDAP overlays are used in the correct order for this purpose. When planning OpenLDAP, the client applications to be selected and supported MUST be considered.

APP.2.3.A2 ELIMINATED (B)

This requirement has been eliminated.

APP.2.3.A3 Secure Configuration of OpenLDAP (B)

Secure configuration of OpenLDAP requires a correctly configured slapd server. The client applications used MUST also be securely configured. When configuring OpenLDAP, the permissions MUST be set correctly in the operating system. The default values of all relevant OpenLDAP configuration directives MUST be checked and adapted if necessary. The back ends and overlays of OpenLDAP MUST be included in the configuration. Appropriate time and size restrictions MUST be set for searching within OpenLDAP. The configuration on the slapd server MUST be checked after each change.

APP.2.3.A4 Configuration of the Database Used by OpenLDAP (B)

The access rights for newly created database files MUST be limited to the user ID in whose context the slapd server is being run. The standard settings of the database used by OpenLDAP MUST be adapted.

APP.2.3.A5 Secure Assignment of Access Rights to OpenLDAP (B)

The global and database-specific access control lists maintained in OpenLDAP MUST be factored in correctly when using OpenLDAP. Database directives MUST take precedence over global directives.

APP.2.3.A6 Secure Authentication for OpenLDAP (B)

If the directory service is to distinguish between different users, they MUST authenticate themselves appropriately. The authentication between the slapd server and communication partners MUST be encrypted. If passwords are to be stored on the clients and servers, hashed values only MUST be used. A suitable hashing algorithm MUST be used.

3.2. Standard Requirements

For module APP.2.3 *OpenLDAP*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.2.3.A7 ELIMINATED (S)

This requirement has been eliminated.

APP.2.3.A8 Restrictions on Attributes in OpenLDAP (S)

The attributes in OpenLDAP SHOULD be restricted using overlays. OpenLDAP SHOULD be modified so that values in the directory service only correspond to a specific regular expression. In addition, it SHOULD be ensured with the help of overlays that selected values only exist once in the directory tree. Such restrictions SHOULD only be applied to user data.

APP.2.3.A9 Partitioning and Replication in OpenLDAP (S)

OpenLDAP SHOULD be partitioned into subtrees on different servers. In such configurations, changes made to data on one server SHOULD be replicated to the other servers. The replication mode SHOULD be selected based on the network connections and availability requirements at hand.

APP.2.3.A10 Secure Updating of OpenLDAP (S)

When performing updates, particular attention SHOULD be paid to whether the changes relate to the back ends or overlays used, or to software dependencies. If administrators use their own scripts, they SHOULD be checked to see if they work with the updated version of OpenLDAP without any problems. The configuration and access rights SHOULD be carefully checked after an update.

APP.2.3.A11 Restriction of the OpenLDAP Runtime Environment (S)

The slapd server SHOULD be restricted to a runtime directory. This directory SHOULD contain all configuration files and databases.

APP.2.3.A12 ELIMINATED (S)

This requirement has been eliminated.

APP.2.3.A13 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

No requirements for increased protection needs have been defined for module APP.2.3 *OpenLDAP*.

4. Additional Information

4.1. Useful Resources

No further information is available for module APP.2.3 *OpenLDAP*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.2.3 *OpenLDAP*.

G 0.11 Failure or Disruption of Service Providers

G 0.15 Eavesdropping

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.38 Misuse of Personal Information

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

APP.3.1 Web Applications and Web Services

1. Description

1.1. Introduction

Web applications provide users with particular functions and dynamic (changing) content. For this purpose, such applications use the Internet protocols HTTP (Hypertext Transfer Protocol) or HTTPS. With HTTPS, connections are cryptographically secured by the TLS (Transport Layer Security) protocol. Web applications make documents and user interfaces available on a server (in the form of input masks, for example) and deliver them on request to corresponding programs on clients such as web browsers.

Web services are applications that use the HTTP(S) protocol to provide data to other applications. As a rule, they are not directly controlled by users.

Several components are usually required to operate a web application or web service. Web servers are usually required to deliver data, as are application servers to run the actual application or service. Additional background systems are also needed, which are often connected as data sources via different interfaces (e.g. databases or directory services).

Web applications and web services are used in both public data networks and organisations' local networks (intranets) to provide data and further applications. As a rule, users must authenticate themselves in order to access a web application or a web service.

1.2. Objective

The aim of this module is to ensure the secure use of web applications and web services and to protect the information they process.

1.3. Scoping and Modelling

This module must be applied to every web application and web service that is used in the information domain in question.

It does not cover requirements for web servers or the editorial planning of a web presence. These can be found in module APP.3.2 *Web Servers*. The development of web applications is covered in module CON.10 *Development of Web Applications*.

Web service interfaces are often created using Representational State Transfer (REST) or Simple Object Access Protocol (SOAP). This module only considers REST-based web services. It focuses on the operational phase of the lifecycle. Security requirements resulting from planning and design or from decommissioning and business continuity planning are not considered in this module; these must be included in a separate risk analysis.

Finally, general requirements for the selection of software are covered in module APP.6 *General Software*.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate/evaluate the threat landscape. For module APP.3.1 *Web Applications and Web Services*, the following specific threats and vulnerabilities are of particular importance.

2.1. Insufficient Logging of Security-Relevant events

If security-relevant events are insufficiently logged by a web application or a web service, they may be difficult to trace at a later time. This may make it impossible to ascertain the causes of an event. For example, critical errors or unauthorised changes in the configuration of a web application may be overlooked.

2.2. Disclosure of Security-Relevant Information in Web Applications and Web Services

Websites and data generated and delivered by a web application or web service can contain information on related background systems, such as IT components and versions of frameworks. This information can make it easier for an attacker to target the web application or web service.

2.3. Misuse of a Web Application Due to Automated Use

If attackers use the functions of a web application or a web service in an automated way, they can perform numerous processes in a short time. Using a repeated login process, an attacker can, for example, attempt to determine valid combinations of user names and passwords (brute force) or generate lists of valid user names (enumeration) if the web application or service returns information about existing users. In addition, calling up resource-intensive functions repeatedly (e.g. complex database queries) can be misused for denial-of-service attacks at the application level.

2.4. Insufficient Authentication

Special functions of a web application or web service are often reserved for certain user groups. The corresponding users then receive user accounts that are exclusively equipped with the necessary access rights (for example). Using these accounts, the users authenticate themselves to the web application or service (e.g. with a user name and password) at the beginning of each session. If this authentication is not configured correctly, it may be possible for an attacker to bypass it. In addition, a web application or web service can be configured in such a way that access data will be stored insecurely on the web server. In the event of a successful incursion, an attacker will then be able to obtain large amounts of access data that can be used elsewhere.

3. Requirements

The specific requirements of module APP.3.1 *Web Applications and Web Services* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Procurement Department

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

APP.3.1.A1 Authentication (B)

The IT Operation Department MUST configure web applications and web services in such a way that users have to authenticate themselves to access protected resources. An appropriate authentication method MUST be selected for this purpose. The selection process SHOULD be documented.

The IT Operation Department MUST define appropriate thresholds for failed login attempts.

APP.3.1.A2 ELIMINATED (B)

This requirement has been eliminated.

APP.3.1.A3 ELIMINATED (B)

This requirement has been eliminated.

APP.3.1.A4 Controlled Integration of Files and Content (B)

If a web application or web service offers an upload function for files, this function MUST be restricted as far as possible by the IT Operation Department. In particular, the allowed file size, file types, and storage locations MUST be defined. The users allowed to use the upload function MUST be defined. Access and execution rights MUST also be set restrictively. Furthermore, it MUST be ensured that a user can save files only in the specified storage location.

APP.3.1.A5 ELIMINATED (B)

This requirement has been eliminated.

APP.3.1.A6 ELIMINATED (B)

This requirement has been eliminated.

APP.3.1.A7 Protection Against Unauthorised Automated Use (B)

The IT Operation Department MUST ensure that web applications and web services are protected against unauthorised automated use. However, these efforts MUST take into account the impact that the protection mechanisms will have on the ability of authorised users to use each application and service. If a web application contains RSS feeds or other functions explicitly intended for automated use, this MUST also be taken into account when configuring the protection mechanisms.

APP.3.1.A14 Protection of Confidential Data (B)

The IT Operation Department MUST ensure that access data for a web application or service is protected from unauthorised access on the server side using secure cryptographic algorithms. Salted hash methods MUST be used for this purpose.

The files containing the source code of a web application or service MUST be protected against unauthorised retrieval.

APP.3.1.A16 ELIMINATED (B)

This requirement has been eliminated.

APP.3.1.A19 ELIMINATED (B)

This requirement has been eliminated.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be implemented as a matter of principle.

APP.3.1.A8 System Architecture [Procurement Department] (S)

Security aspects SHOULD be considered early on in the planning of web applications and web services. It SHOULD also be ensured that the architecture of a web application or service maps the exact business logic of the relevant organisation and implements it correctly.

APP.3.1.A9 Web Application and Web Service Procurement (S)

In addition to the general aspects of software procurement, an organisation SHOULD, at minimum, consider the following when procuring web applications and web services:

- Secure input validation and output encoding
- Secure session management
- Secure cryptographic procedures
- Secure authentication procedures
- Secure procedures for server-side storage of credentials
- Appropriate access management
- Sufficient logging capabilities
- Regular security updates from the software developer
- Protection mechanisms against widespread attacks on web applications and web services
- Access to the source code of the web application or web service

APP.3.1.A10 ELIMINATED (S)

This requirement has been eliminated.

APP.3.1.A11 Secure Integration of Background Systems (S)

Access to background systems to which functions and data are outsourced SHOULD only be possible from defined IT systems via defined interfaces. When communicating across network and site boundaries, data traffic SHOULD be authenticated and encrypted.

APP.3.1.A12 Secure Configuration (S)

Web applications and web services SHOULD be configured in such a way that their resources and functions can only be accessed using the secured communication paths specified for this purpose. Access to resources and functions that are not required SHOULD be disabled. If this is not possible, such access SHOULD be restricted as far as possible. The following actions SHOULD be taken when configuring web applications and web services:

- Disabling unnecessary HTTP methods
- Configuring character encoding
- Removing security-related information from error messages and responses
- Storing configuration files outside of the web root directory
- Defining thresholds for access attempts

APP.3.1.A13 ELIMINATED (S)

This requirement has been eliminated.

APP.3.1.A15 ELIMINATED (S)

This requirement has been eliminated.

APP.3.1.A17 ELIMINATED (S)

This requirement has been eliminated.

APP.3.1.A18 ELIMINATED (S)

This requirement has been eliminated.

APP.3.1.A21 Secure HTTP Configuration of Web Applications (S)

To protect against clickjacking, cross-site scripting, and other attacks, the IT Operation Department SHOULD set appropriate HTTP response headers. At minimum, the following HTTP headers SHOULD be used:

- Content-Security-Policy
- Strict-Transport-Security
- Content-Type
- X-Content-Type-Options
- Cache-Control

The HTTP headers used SHOULD be as restrictive as possible.

Cookies SHOULD always be set with the attributes *secure*, *SameSite*, and *httponly*.

APP.3.1.A22 Penetration Testing and Auditing (S)

Web applications and web services SHOULD be checked for security issues at regular intervals. In particular, audits SHOULD be performed regularly. The results SHOULD be documented transparently, protected adequately, and handled confidentially. Deviations SHOULD be investigated. The results SHOULD be presented to the CISO.

APP.3.1.A23 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

APP.3.1 A20Use of Web Application Firewalls (H)

Organisations SHOULD use web application firewalls (WAF). The configuration of a given WAF should be adapted to the web application or service it is meant to protect. The WAF's configuration SHOULD be checked after each web application or web service update.

APP.3.1.A24 ELIMINATED (H)

This requirement has been eliminated.

APP.3.1.A25 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

On its website, the Open Web Application Security Project (OWASP) provides guidance on securing web applications and web services.

The Federal Office for Information Security (BSI) provides guidance on the use of cryptographic procedures in the document “Cryptographic Mechanisms: Recommendations and Key Lengths: BSI TR-02102”.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module APP.3.1 *Web Applications and Web Services*.

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.43 Attack with Specially Crafted Messages

G 0.46 Loss of Integrity of Sensitive Information

APP.3.2 Web Servers

1. Description

1.1. Introduction

A web server is a key component of any website. It accepts requests from clients and delivers the corresponding content back to them. The data is typically transmitted via the Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS), which is a version encrypted with Transport Layer Security (TLS). Since web servers offer a simple interface between server applications and users, they are also frequently used for internal information and applications in organisations' own networks (intranets).

Web servers are usually available directly on the Internet and are thus exposed to attacks. That is why they must be protected by appropriate security safeguards.

1.2. Objective

The aim of this module is to protect web servers and the information they provide and process.

1.3. Scoping and Modelling

This module must be applied to all web servers in the information domain in question.

The term “web server” is used for both the software that responds to HTTP requests and the IT systems used to run such software. This module mainly addresses web server software. Security aspects of the IT systems on which web server software is installed are addressed in the corresponding modules of the SYS *IT Systems* layer (see SYS.1.1 *General Server*, as well as SYS.1.3 *Linux and Unix Servers* and SYS.1.2.2 *Windows Server 2012*).

Recommendations for integrating web servers into network architecture and protecting them with firewalls are included in modules NET.1.1 *Network Architecture and Design* and NET.3.2 *Firewall*.

The present module covers fundamental aspects that are important for the provision of web content. It does not address dynamic content provided by web applications or web services. This is dealt with in module APP.3.1 *Web Applications and Web Services*.

This also applies to web browsers; corresponding requirements are included in module APP.1.2 *Web Browsers*.

Connections to web servers are usually encrypted. Module CON.1 *Crypto Concept* describes how cryptographic keys can be managed in a secure manner.

In cases in which web servers are managed by a hosting provider instead of being operated in-house, module OPS.2.1 *Outsourcing for Customers* must be observed.

Authentication mechanisms are often used for web servers. Additional requirements for these mechanisms can be found in module ORP.4 *Identity and Access Management*.

2. Threat Landscape

For module APP.3.2 *Web Servers*, the following specific threats and vulnerabilities are of particular importance.

2.1. Loss of Reputation

If attackers manage to access a web server with administrative rights, they can use it to publish a manipulated website (defacement). This can damage an organisation's reputation. Similarly, publishing incorrect information (such as faulty product descriptions) can cause an organisation's public image to suffer. An organisation may also receive an official reprimand if content is published on its website that violates certain legal provisions. In addition, an organisation may suffer losses if its website is not available and potential customers switch to competitors as a result.

2.2. Web Server Manipulation

An attacker may gain access to a web server and manipulate its data. For example, the attacker could change the web server's configuration, distribute malware, or modify web content.

2.3. Denial of Service (DoS)

DoS attacks can be used to specifically impair the availability of a website, for example by blocking individual accounts through incorrect logins. An attacker could, for example, ensure that user accounts are blocked by invalid login attempts.

DDoS (distributed denial of service) attacks may result in the partial or total failure of a web server. In such case, users’ access to corresponding web offerings will be very slow or not available at all. For many organisations, such failures can quickly become business-critical (when they affect online shops, for example).

2.4. Loss of Confidential Data

Many web servers still use outdated cryptographic methods such as RC4 or SSL. Insufficient authentication or inappropriate encryption may result in attackers being able to read or change communications between web servers and clients. The same applies to communications between a web server and other servers, such as load balancers.

2.5. Violation of Laws or Regulations

There are various regulatory requirements regarding the publication of web content. In addition to the regulations of telecommunications and data protection laws, the rules of copyright law must also be observed. Violations of these laws can have legal consequences.

2.6. Insufficient Troubleshooting

If errors occur during web server operations, this may impact the server's availability (for example). The content it displays may also be incomplete, or security mechanisms may fail. If errors are not handled correctly both the operation and the protection of the functions and data of a web server will no longer be ensured.

3. Requirements

The specific requirements of module APP.3.2 *Web Servers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner, Compliance Manager, Central Administration

3.1. Basic Requirements

For module APP.3.2 *Web Servers*, the following requirements MUST be implemented as a matter of priority:

APP.3.2.A1 Secure Web Server Configuration (B)

After the IT Operation Department has installed a web server, it MUST perform a secure basic configuration. To that end, it MUST specifically assign the web server process to a user account with minimal rights. The web server MUST also be executed in an encapsulated environment whenever this is supported by the operating system. If this is not possible, each web server SHOULD run on its own physical or virtual server.

The web server service MUST be stripped of all unnecessary write permissions. Modules and functions of the web server that are not required MUST be deactivated.

APP.3.2.A2 Protection of Web Server Files (B)

The IT Operation Department MUST protect all files on the web server (including scripts and configuration files in particular) so that they cannot be read or changed without authorisation.

It MUST be ensured that web applications can only access a defined directory tree (the WWW root directory). The web server MUST be configured to serve only files located within the WWW root directory.

The IT Operation Department MUST disable all unnecessary functions that list directories. Confidential data MUST be protected against unauthorised access. In particular, the IT Operation Department MUST ensure that confidential files are not located in public directories of the web server. The IT Operation Department MUST regularly check whether confidential files have been stored in public directories.

APP.3.2.A3 Protecting File Uploads and Downloads (B)

All files published using the web server MUST be checked in advance for malware. A maximum size for file uploads MUST be specified. Sufficient storage space MUST be reserved for uploads.

APP.3.2.A4 Logging of Events (B)

The web server MUST log at least the following events:

- successful attempts to access resources
- failed attempts to access resources due to a lack of authorisations, unavailable resources, or server errors
- general error messages

The log data SHOULD be analysed regularly.

APP.3.2.A5 Authentication (B)

When clients authenticate themselves to a web server using passwords, these passwords MUST be stored in a way that is cryptographically secured and protected from unauthorised access.

APP.3.2.A6 ELIMINATED (B)

This requirement has been eliminated.

APP.3.2.A7 Legal Framework Conditions for Websites [Process Owner, Central Administration, Compliance Manager] (B)

If web servers publish content or offer services for third parties, the relevant legal framework conditions MUST be observed. The organisation MUST observe the applicable telecommunication, data protection, and copyright laws.

APP.3.2.A11 Encryption via TLS (B)

The web server MUST provide secure encryption via TLS (HTTPS) for all connections that pass through untrusted networks. If it is necessary to use obsolete procedures for compatibility reasons, these SHOULD be limited to as few cases as possible.

If an HTTPS connection is used, all content MUST be delivered via HTTPS. Mixed content MUST NOT be used.

3.2. Standard Requirements

For module APP.3.2 *Web Servers*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.3.2.A8 Planning the Use of a Web Server (S)

The purpose of a web server and the content it provides SHOULD be planned and documented. The documentation SHOULD also describe the information or services included in the web offerings in question, along with the corresponding target groups. Appropriate persons SHOULD be put in charge of technical operations and web content.

APP.3.2.A9 Defining a Web Server Security Policy (S)

A security policy stating the required safeguards and responsibilities SHOULD be drawn up. An approach to obtaining information on current security vulnerabilities SHOULD also be defined. Furthermore, the manner in which security safeguards are to be implemented and the steps to be taken in the event of a security incident SHOULD be defined.

APP.3.2.A10 Selecting an Appropriate Web Host (S)

If an organisation opts to use an external webhosting provider instead of operating its web server itself, the organisation SHOULD pay attention to the following points when selecting a suitable provider:

- The manner in which the services are to be rendered SHOULD be contractually agreed. Security aspects SHOULD be included in writing in a service level agreement (SLA) as part of the contract.
- The service provider SHOULD regularly check and service the IT systems used. The service provider SHOULD be obligated to respond promptly in case of technical problems or compromised customer systems.
- The service provider SHOULD implement basic technical and organisational safeguards to protect its information domain.

APP.3.2.A12 Suitable Handling of Errors and Error Messages (S)

HTTP information and displayed error messages SHOULD not show the product name or the version of the web server used. Error messages SHOULD not reveal details regarding system information or configurations. The IT Operation Department SHOULD ensure that the web server only outputs general error messages that inform the user that an error has occurred. Each error message SHOULD contain a unique characteristic that allows administrators to

trace the error. In the case of unexpected errors, it SHOULD be ensured that the web server will not remain in a state where it is vulnerable to attack.

APP.3.2.A13 Access Control for Web Crawlers (S)

Web crawler access SHOULD be regulated in accordance with the robots exclusion standard. Content SHOULD be provided with access protection to safeguard it against web crawlers that do not comply with this standard.

APP.3.2.A14 Integrity Checks and Protection Against Malware (S)

The IT Operation Department SHOULD regularly check the integrity of the configurations of the web server and the files it provides and ensure they have not been modified by attackers. The files intended for publication SHOULD be regularly checked for malware.

APP.3.2.A16 Penetration Testing and Auditing (S)

Web servers SHOULD be checked for security issues at regular intervals. Audits SHOULD also be performed regularly. The results SHOULD be documented transparently, protected adequately, and handled confidentially. Deviations SHOULD be investigated. The results SHOULD be presented to the CISO.

APP.3.2.A20 Appointing Contact Persons [Central Administration] (S)

An organisation that maintains extensive websites SHOULD designate a contact person for them. Processes, procedures, and persons responsible for problems or security incidents SHOULD be specified.

The organisation SHOULD post a contact option on its website that enables external parties to report security issues to the organisation. The organisation SHOULD define processes for handling external security reports.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.3.2 *Web Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.3.2.A15 Redundancy (H)

Web servers SHOULD be designed to be redundant. The Internet connection of a web server and other IT systems (such as the web application server) SHOULD also be designed with redundancy.

APP.3.2.A17 ELIMINATED (H)

This requirement has been eliminated.

APP.3.2.A18 Protection Against Denial-of-Service Attacks (H)

A web server SHOULD be monitored continuously. Furthermore, safeguards that prevent or at least mitigate DDoS attacks SHOULD be defined and implemented.

APP.3.2.A19 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

The Federal Office for Information Security has published the following additional documents that may be relevant for the operation of web servers:

- “Migration auf TLS 1.2 – Handlungsleitfaden” [Migration to TLS 1.2 – BSI Action Guidelines]
- “Sicheres Webhosting: Handlungsempfehlung für Webhoster” [Secure Web Hosting: Recommendations for Web Hosts]
- “Sicheres Bereitstellen von Webangeboten (ISi-Webserver)” [Secure Provisioning of Websites (ISi Series for Web Servers)]

In the document “Guidelines on Securing Public Web Servers", the National Institute of Standards and Technology (NIST) also provides advice on web server security.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.3.2 *Web Servers*.

G 0.11 Failure or Disruption of Service Providers

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.39 Malware

G 0.40 Denial of Service

G 0.46 Loss of Integrity of Sensitive Information

APP.3.3 File Servers

1. Description

1.1. Introduction

A file server is a network server that provides files centrally from internal or networked hard drives for all users or clients with corresponding access authorisation. Authorised users can thus share data without having to transport it to removable media or distribute it by e-mail, for example. Because the data is stored centrally, it can be structured and provided in various directories and files. With file servers, access rights to files can also be assigned centrally. Furthermore, storing all data in a central location simplifies the creation of backups.

A file server mainly manages mass-storage devices connected via interfaces such as SCSI (Small Computer System Interface) or SAS (Serial Attached SCSI). The storage memory itself is either located directly within the server's casing or connected externally. The latter is often referred to as 'directly attached storage' (DAS). A file server can be operated on conventional server hardware or a dedicated appliance. For large data volumes, central storage area network (SAN) devices can also be connected via host bus adapters (HBA) in the server, as well as to SAN switches.

1.2. Objective

This module describes the main threats specific to file servers and the resulting requirements for the secure operation of such servers.

1.3. Scoping and Modelling

Module APP.3.3 *File Servers* must be applied once to each file server in the information domain in question.

This module includes basic specifications which must be observed and met when operating file servers. The general and operating-system-specific aspects of a server are not included in this module. These aspects are addressed in module SYS1.1 *General Server* and in the relevant operating-system-specific modules of the IT Systems layer, e.g. SYS.1.3 *Linux and Unix Servers* or SYS.1.2.2 *Windows Server 2012*. Requirements for network-based storage systems or storage

networks are not described. These are discussed in module SYS.1.8 *Storage Solutions*. Dedicated services for operating a file server (e.g. Samba) are also not addressed. The Samba service is covered in module APP.3.4 *Samba*.

When securing a file server, it is important to assign rights to files in a restrictive manner. Further requirements in this regard can be found in module ORP.4 *Identity and Access Management*. Furthermore, this module does not cover methods of securing the information stored on a file server. On this topic, the requirements of module CON.3 *Backup Concept* must be met.

2. Threat Landscape

For module APP.3.3 *File Servers*, the following specific threats and vulnerabilities are of particular importance:

2.1. File Server Failure

If a file server fails, the entire surrounding information domain may be affected, including important business processes and specialised tasks within the organisation. In addition to users, applications may depend on data from the file server to function properly. If data and services are not available, it may not be possible to meet deadlines and essential business processes may fail. Meanwhile, if there is no corresponding business continuity management concept, the time required to bring the systems affected back online may increase further. This can lead to financial losses in many cases. A file server failure can also have an impact on other organisations.

2.2. Insufficient File Server Characteristics

If the line connection or storage capacity of a file server is not sufficient, this may lead to increased access times or storage bottlenecks. This can result, for example, in employees becoming frustrated and starting to store data locally due to long waiting times, which means it will no longer be possible to trace who has certain data and where it is stored. Applications that rely on correct (intermediate) storage of information can also no longer function reliably.

2.3. Insufficient Checking of Stored Files

If a file server is not sufficiently included in an organisation's malware protection concept, attackers may place malware on the file server unnoticed. All IT systems and applications that access the file server's data could be infected with the malware, causing it to spread very quickly throughout the organisation.

2.4. Insufficient Access Authorisation Concept

If access authorisations and approvals are not designed and assigned properly, unauthorised third parties might access data. Attackers or unauthorised users could thus change, delete, or copy data.

2.5. Unstructured Data Storage

If the storage structure is not specified or employees do not comply with it, data can be stored on a file server in a confusing and uncoordinated manner. This leads to various problems, such as wasted disk space due to the same files being stored multiple times. Different versions of a file can also be stored. In addition, unauthorised access is possible if, for example, files are located in directories or file systems that are made accessible to third parties.

2.6. Loss of Data Stored on File Servers

If a file server fails completely or individual components prove defective, important data can be lost in the absence of a functioning backup or data synchronisation. The same applies when employees delete files inadvertently. Further problems can follow if sufficient redundancy has also not been ensured by means of a RAID array, for example. The failure of individual storage media will then have a direct impact on operations because files will no longer be available.

2.7. Ransomware

Ransomware is a special form of malware that encrypts data on infected IT systems. Attackers subsequently demand payment of a ransom, claiming that they will then enable the victim to decrypt the data again. Even after the ransom is paid, however, there is no guarantee that the data can be recovered.

Encryption is not restricted to the local data of the infected IT system. Many forms of ransomware look for network drives with write access in order to encrypt all their data, as well.

This means that all encrypted information dating back to the most recent backup can be lost, even if a ransom is paid. Along with the IT system originally infected, this may affect the centrally stored information accessed by multiple IT systems.

3. Requirements

The specific requirements of module APP.3.3 *File Servers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	User

3.1. Basic Requirements

For module APP.3.3 *File Servers*, the following requirements MUST be implemented as a matter of priority:

APP.3.3.A1 ELIMINATED (B)

This requirement has been eliminated.

APP.3.3.A2 Use of RAID Systems (B)

The IT Operation Department MUST define whether a RAID system should be used on a file server. Any decision against such a system MUST be documented in a transparent manner. If a RAID system is to be used, the IT Operation Department MUST decide:

- what RAID level should be used
- what length of time will be allowed for a RAID rebuild process
- whether to use a software or a hardware RAID

Hot spare hard disks SHOULD be available in a RAID.

APP.3.3.A3 Use of Anti-Virus Programs (B)

All data MUST be scanned for malware by a virus protection programme before being stored on the file server.

APP.3.3.A4 ELIMINATED (B)

This requirement has been eliminated.

APP.3.3.A5 ELIMINATED (B)

This requirement has been eliminated.

APP.3.3.A15 Planning File Servers (B)

Before an organisation introduces one or more file servers, it SHOULD decide what the file servers will be used for and what information will be processed on them. The organisation SHOULD plan each file server function to be used, including its security aspects. Personal computers MUST NOT be used as file servers.

File server storage space MUST be adequately sized. Sufficient storage reserves SHOULD also be kept available. Only mass storage designed for continuous operation SHOULD be used. The speed and connections of mass storage MUST be appropriate for its intended use.

3.2. Standard Requirements

For module APP.3.3 *File Servers*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.3.3.A6 Acquiring a File Server and Selecting a Service (S)

Appropriate file server software SHOULD be selected. The file server service SHOULD support the intended use of the file server—for example, the integration of network drives on clients,

streaming of multimedia content, the transfer of boot images from diskless IT systems, or simple file transfers via FTP. Performance, storage capacity, bandwidth, and the number of people who will be using it SHOULD be considered when purchasing a file server.

APP.3.3.A7 Selecting a File System (S)

The IT Operation Department SHOULD create a requirements list and use it as a basis for evaluating the file systems of different file servers. The file system selected SHOULD meet the organisation's standards. The file system SHOULD also provide a journaling function. Moreover, it SHOULD have a mechanism that prevents several users or applications from accessing a file with write permissions at the same time.

APP.3.3.A8 Structured Data Storage [User] (S)

A structure for storing data SHOULD be specified. Users SHOULD be informed regularly of the requirements of structured data storage. Files SHOULD only be stored on a file server in a structured manner. The types of data that can be stored locally those that can be kept on a file server SHOULD be specified in writing. Program and work files SHOULD be stored in separate directories. The organisation SHOULD regularly check compliance with the requirements for structured data storage.

APP.3.3.A9 Secure Storage Management (S)

The IT Operation Department SHOULD regularly check whether the mass storage of file servers is still working as intended. Suitable backup storage SHOULD be kept available.

If a storage hierarchy (primary, secondary and tertiary storage) has been established, (partially) automated storage management SHOULD be used. If data is distributed automatically, the proper functioning of the distribution method used SHOULD be checked manually at regular intervals.

At minimum, unauthorised attempts to access files and changes in access rights SHOULD be logged.

APP.3.3.A10 ELIMINATED (S)

This requirement has been eliminated.

APP.3.3.A11 Using Storage Restrictions (S)

The IT Operation Department SHOULD consider setting limits (quotas) on storage space for individual users if there are multiple users on a file server. As an alternative, mechanisms of the file or operating system in question SHOULD be used that warn users or only grant write privileges to the system administrator if the hard drive capacity reaches a specific level.

APP.3.3.A14 Using Error Correction Codes (S)

The IT Operation Department SHOULD use an error-detecting or error-correcting file system. Sufficient storage space SHOULD be provided for this purpose. The IT Operation Department SHOULD take into account that, depending on the method used, errors can only be detected with a certain probability and can only be removed to a limited extent.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.3.3 *File Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.3.3.A12 Data Encryption (H)

The mass storage devices of a file server SHOULD be encrypted at the file system or hardware level. If hardware encryption is used, products with a certified encryption function SHOULD be used. It SHOULD be ensured that the virus protection program in use can scan encrypted data for malware.

APP.3.3.A13 Replicating Between Locations (H)

For high-availability file servers, data SHOULD be replicated appropriately across several mass storage devices. Data SHOULD also be replicated between independent file servers located at independent sites. To this end, a suitable replication mechanism SHOULD be selected by the IT Operation Department. Sufficiently accurate time services SHOULD be used and operated so that the replication can work as intended.

4. Additional Information

4.1. Useful Resources

No further information is available for module APP.3.3 *File Servers*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.3.3 *File Servers*.

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.3.4 Samba

1. Description

1.1. Introduction

Samba is a freely available and full-featured Active Directory Domain Controller (ADDC) that is able to provide authentication, file, and print services as a means of facilitating interoperability between Windows and Unix. Samba combines many different protocols and technologies, including the Server Message Block (SMB) protocol. The term “Samba server” refers to servers running Samba. These are usually Unix servers.

If the use of Samba is designed properly and suitably configured, it will interact with a Windows client or server as if it were a Windows system itself.

1.2. Objective

The aim of this module is to show how organisations can use Samba in a secure manner and how information provided by Samba can be protected.

1.3. Scoping and Modelling

Module APP.3.4 *Samba* must be applied to every Samba server within the information domain under consideration.

This module deals with Samba as an authentication, file, and print service. As Samba is usually used on Unix servers, where it provides familiar services from the world of Windows servers, the security aspects of the modules SYS.1.1 *General Server* and SYS.1.3 *Linux and Unix Servers* must be considered.

When securing a Samba server, it is important to assign rights to files in a restrictive manner. More detailed information on identity and access management is provided in module ORP.4 *Identity and Access Management*.

General security requirements for printers, file servers, or directory services are also not part of this module. These are described in the modules SYS.4.1 *Printers, Copiers, and All-in-One Devices*, APP.3.3 *File Servers,* APP.2.1 *General Directory Service*, and APP.2.3 *OpenLDAP*.

2. Threat Landscape

For module APP.3.4 *Samba*, the following specific threats and vulnerabilities are of particular importance:

2.1. Eavesdropping on Unprotected Samba Communication Links

If attackers eavesdrop on unprotected Samba communication links, confidential information can be intercepted and misused. Protocols without comprehensive security characteristics are often used for data transfers between Unix servers, Windows servers, and clients. This makes both authentication data and payloads accessible to third parties, which can lead to misuse by unauthorised persons. This in turn can result in an organisation's sensitive information falling into the wrong hands.

2.2. Insecure Default Settings on Samba Servers

To demonstrate some of the capabilities of the Samba server and provide administrators with a quick introduction, the smb.conf configuration file is created with default settings during the server's installation. The default options in this file can be used to start the Samba server. If the file is used without caution or further adjustments, this may result in significant vulnerabilities. If file shares used as an example are not commented out, it will be possible to read any sensitive information stored on these unwanted shares.

2.3. Unauthorised Use or Administration of Samba

Using applications or IT systems, unauthorised persons may obtain confidential information, carry out manipulations or cause disruptions. They could then can administrate Samba without authorisation. The use of configuration tools that are outdated and no longer updated (such as the Samba Web Administration Tool, SWAT) is particularly problematic in this regard.

2.4. Incorrect Administration of Samba

If the administrators are not sufficiently familiar with the extensive functions, components, options, and configuration settings of Samba, this may result in serious complications. For example, incorrect configurations of DNS or user and rights management may allow unauthorised persons to access resources. This may result in operational interruptions or the disclosure of sensitive information.

2.5. Data Loss in Samba Environments

Data loss can have a significant impact on the use of IT. When information required by an organisation is destroyed or corrupted, this can cause delays in business processes and specialised tasks, or even prevent their execution. In the case of Samba, it should be considered that the properties of the file systems in Windows and Unix differ significantly. There is no universal guarantee that access rights will be maintained in Windows; under certain

circumstances, important file properties can be lost. This may also result in the loss of information on alternate data streams (ADS) and DOS attributes.

2.6. Loss of Integrity of Sensitive Information in Samba Environments

Samba stores important operating data in databases in the Trivial Database (TDB) format. If these databases are not handled with sufficient performance and consistency by the operating system, they can cause problems when Samba services are used.

3. Requirements

The specific requirements of module APP.3.4 *Samba* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module APP.3.4 *Samba*, the following requirements MUST be met as a matter of priority:

APP.3.4.A1 Planning the Use of a Samba Server (B)

The IT Operation Department MUST carefully plan and regulate the introduction of a Samba server. Depending on the operational scenario, it MUST define the operating mode of the Samba server and the tasks it will perform. It MUST also define which Samba components and other components are required for these purposes.

If the CTDB (Clustered Trivial Database) solution is to be used, the IT Operation Department MUST design it with care. If Samba is also meant to provide Active Directory (AD) services for Linux and Unix systems, these services MUST be planned carefully and tested. Furthermore, the authentication procedure for AD MUST be designed and implemented carefully. The implementation and the order in which stackable Virtual File System (VFS) modules are executed MUST be designed carefully. This implementation SHOULD be documented.

If IPv6 is to be used under Samba, this MUST also be carefully planned. In addition, whether the integration works without errors MUST be checked in a near-operational test environment.

APP.3.4.A2 Secure Basic Configuration of a Samba Server (B)

The IT Operation Department MUST configure the Samba server securely. Among other things, the access control settings MUST be adjusted. The same SHOULD apply to settings that affect the performance of the server.

The IT Operation Department MUST configure Samba to only accept connections from secure hosts and networks. Changes to the configuration SHOULD be documented carefully so that it is possible at any time to determine who made which changes and for what reasons. In such cases, the syntax of the configuration file MUST be checked for correctness after every change.

Additional software modules such as SWAT MUST NOT be installed.

3.2. Standard Requirements

For module APP.3.4 *Samba*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.3.4.A3 Secure Configuration of a Samba Server (S)

Databases in the Trivial Database (TDB) format SHOULD NOT be stored on a partition that uses ReiserFS as its file system. If a netlogon share is configured, unauthorised users SHOULD NOT be able to modify any files on the share.

The operating system of a Samba server SHOULD support access control lists (ACLs) in connection with the file system used. In addition, it SHOULD be ensured that the file system is integrated with the appropriate parameters.

The default settings of SMB Message Signing SHOULD be maintained unless they are contrary to the existing security policies in the information domain in question.

APP.3.4.A4 Avoiding NTFS File Properties on a Samba Server (S)

If a version of Samba is used that cannot map ADS in the New Technology File System (NTFS) and file system objects are to be copied or moved across system boundaries, file system objects SHOULD NOT contain ADS with important information.

APP.3.4.A5 Secure Configuration of a Samba Server's Access Controls (S)

The default parameters used by Samba to map DOS attributes to the Unix file system SHOULD NOT be used. Instead, Samba should be configured to save DOS attributes and inheritance flags in extended attributes. Shares SHOULD only be managed via the Samba registry.

In addition, the effective access authorisations for the shares of a Samba server SHOULD be checked regularly.

APP.3.4.A6 Secure Configuration of Winbind in Samba (S)

The operating system of the server SHOULD include a user account with all necessary group memberships for each Windows domain user. If this is not possible, Winbind SHOULD be used to convert domain user names into unique Unix user names. When using Winbind, it SHOULD be ensured that conflicts between local Unix users and domain users are prevented.

Furthermore, the pluggable authentication modules (PAMs) SHOULD be integrated.

APP.3.4.A7 Secure DNS Configuration in Samba (S)

If Samba is to be used as a DNS server, this implementation SHOULD be planned carefully and tested in advance. Since Samba supports various AD integration modes, the IT Operation Department SHOULD set the DNS settings in accordance with the Samba application scenario at hand.

APP.3.4.A8 Secure LDAP Configuration in Samba (S)

If users are managed with LDAP in Samba, the IT Operation Department SHOULD plan and document this configuration carefully. The access authorisations for LDAP SHOULD be controlled by means of ACLs.

APP.3.4.A9 Secure Configuration of Kerberos in Samba (S)

The Heimdal Kerberos Key Distribution Center (KDC) implemented by Samba SHOULD be used for authentication. It SHOULD be ensured that the Kerberos configuration file specified by Samba is used. Only secure encryption methods SHOULD be used for Kerberos tickets.

If Kerberos is used for authentication, the central time server SHOULD be installed locally on the Samba server. The NTP service SHOULD be configured so that only authorised clients can request the time.

APP.3.4.A10 Secure Use of External Programs on a Samba Server (S)

The IT Operation Department SHOULD ensure that Samba only calls trustworthy external programs that have been checked for malicious functions.

APP.3.4.A11 ELIMINATED (S)

This requirement has been eliminated.

APP.3.4.A12 Training Samba Server Administrators (S)

Administrators SHOULD be trained on the specific areas of Samba that are in use—user authentication and rights models for Windows and Unix, for example, but also on ACLs and ADS for NTFS.

APP.3.4.A13 Regular Backups of Important Samba Server Components (S)

All the system components required to recover a Samba server SHOULD be included in the organisation-wide backup concept. The account information of all the back ends in use SHOULD also be considered. In addition, all TDB files should be backed up. Furthermore, the Samba registry SHOULD be backed up if it has been used for shares.

APP.3.4.A14 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.3.4 *Samba* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.3.4.A15 Encryption of Data Packets in Samba (H)

To ensure their security while in transit, data packets SHOULD be encrypted using the methods integrated from SMB version 3.

4. Additional Information

4.1. Useful Resources

No further information is available for module APP.3.4 *Samba*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.3.4 *Samba*.

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.23 Unauthorised Access to IT Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.3.6 DNS Servers

1. Description

1.1. Introduction

A domain name system (DNS) is a network service used to resolve the host names of IT systems into IP addresses. A DNS can be compared to a telephone book that resolves names into IP addresses rather than telephone numbers. A DNS usually searches for the IP address that corresponds to a given host name (forward resolution). Searching for a host name based on a known IP address, on the other hand, is referred to as reverse resolution.

The associations between host names and IP addresses are managed in the domain name space. The domain name space has a hierarchical structure and is provided by DNS servers. While the term “DNS server” actually refers to the software used, it is mostly also used as a synonym for the IT system on which this software is run.

DNS servers manage the domain name space on the Internet, but are often also used within an organisation’s internal network. Resolvers are installed as standard components on users’ IT systems. Requests are made to DNS servers via the resolver. In response, the DNS servers return information about the domain namespace.

DNS servers can be differentiated by the tasks they perform. There are basically two different types: advertising DNS servers and resolving DNS servers. Advertising DNS servers are usually responsible for processing requests from the Internet. Resolving DNS servers process requests from an organisation's internal network.

A DNS server failure may have severe consequences for the operation of IT infrastructure. While a failed DNS system is not a major problem in itself, it does result in restricted DNS-based services. Web servers or e-mail servers may no longer be available, or remote maintenance may no longer function. Since DNS is required by a very large number of network applications, RFC 1034 specifies that at least two authoritative DNS servers (advertising DNS servers) must be operated for every zone.

1.2. Objective

This module describes the threats specific to DNS servers and the related requirements that ensure their secure operation.

1.3. Scoping and Modelling

Module APP.3.6 *DNS Servers* must be applied to each DNS server used in the information domain under consideration.

This module includes basic specifications to be considered and met when an organisation uses a DNS server. The focus here is on the availability of DNS servers and the integrity of the information transferred. This module also covers problems that can occur in the use of DNS servers.

General and operating-system-specific aspects of a server are not included in this module. These are covered in module SYS1.1 *General Server* and in the corresponding operating-system-specific modules of the SYS *IT Systems* layer, e.g. SYS.1.3 *Linux and Unix Servers* or SYS.1.2.2 *Windows Server 2012*.

2. Threat Landscape

For module APP.3.6 *DNS Servers*, the following specific threats and vulnerabilities are of particular importance.

2.1. DNS Server Failure

If a DNS server fails, it may affect all of an organisation's IT operations. Since clients and other servers in the organisation will no longer be able to resolve internal and external addresses on the basis of host names, establishing further data connections will be impossible. The external IT systems used by mobile employees, customers, and business partners (for example) will also be unable to access the organisation’s servers. This usually disrupts essential business processes.

2.2. Inadequate Line Bandwidth

If the available bandwidth is insufficient for a DNS server, the times required to access internal and external services may be prolonged. As a consequence, these services may be limited or entirely inaccessible. Attackers may also find it easier to overload the DNS server by means of a denial of service (DoS) attack.

2.3. Inadequate planning of DNS usage

Planning errors often turn out to be particularly serious because they can easily create extensive vulnerabilities. If the use of DNS is insufficiently planned, this may result in problems and vulnerabilities during live operations. If, for example, the firewall rules that control DNS traffic are defined in too lax a manner, this might result in an attack under certain

circumstances. On the other hand, overly restrictive rules may prevent legitimate clients from sending requests to DNS servers and hinder them when using services such as e-mail or FTP.

2.4. Incorrect Domain Information

Even if the use of DNS has been planned carefully and all the security-relevant aspects have been taken into consideration, this will not be sufficient if semantically and syntactically incorrect domain information is created. This includes the incorrect assignment of IP addresses to host names, missing data, the use of forbidden characters, and inconsistent forward and reverse resolution. If the domain information contains errors, the services that use this information will only be able function to a limited extent.

2.5. Incorrect Configuration of a DNS Server

Default, self-configured, and incorrect configuration settings may cause a DNS server to function improperly. For example, if a resolving DNS server has been configured to accept recursive requests without any limitations (i.e. from both the internal data network and the Internet), the availability of the server may be significantly impaired due to the increased load. Additionally, the server might become susceptible to DNS reflection attacks as a consequence.

Incorrectly configured DNS servers are also subject to the threat of zone transfers not being limited to authorised DNS servers. This means that every host capable of sending a request to DNS servers can obtain all the domain information of these servers. Data obtained in this way may facilitate future attacks.

2.6. DNS Manipulation

A DNS cache poisoning attack aims to store falsely assigned IP addresses and names on the target IT system. It exploits the fact that DNS servers cache the domain information they receive for a certain period of time, which can facilitate the widespread dissemination of fake data. If corresponding requests are then sent to a manipulated DNS server, this server will return falsified data. The receiver of the response caches the falsified data, and in doing so “poisons” its own cache, as well. The length of time after which stored data expires (time to live, or TTL) can be configured. If a manipulated address is requested from a resolving DNS server, it will not send a request to a different DNS server until the set length of time has expired. Manipulated DNS information can thus persist for a long time, even if it has already been corrected on the DNS server originally attacked. If, for example, an attacker is able to take over the name resolution for a domain by manipulating the entries in such a way that requests will be sent to the attacker's DNS servers, all the respective sub-domains will automatically be affected, as well. DNS cache poisoning attacks are often performed with the objective of diverting requests to malicious servers.

2.7. DNS Hijacking

DNS hijacking is a type of attack used to route the communications between advertising DNS servers and resolvers through the attacker's IT system. Using this man-in-the-middle attack, the attacker can intercept and record communications between the servers. The far greater threat, however, is that a successful attacker may be able to manipulate any data traffic

between two communication partners in any number of ways. If a request is sent by the resolver of a client IT system to a DNS server after a successful DNS hijacking attack, the attacker can, for example, modify the assignment of IP addresses to names. DNS hijacking can also be combined with other attacks, such as phishing.

2.8. DNS DoS

When a DoS attack is carried out on a DNS server, the number of requests sent to the server is so high that it overloads the network connection to the DNS server or the DNS server itself. In general, the requests are sent using bot networks to achieve the required data rate. A DNS server that has become overloaded in this manner can no longer respond to any legitimate requests.

2.9. DNS Reflection

A DNS reflection attack is a DoS attack that does not target the DNS server to which the requests are sent, but the receiver of the responses. It takes advantage of the fact that certain requests generate a relatively large amount of response data. Here, it is possible to achieve an amplification factor of 100 or higher. This means that the response, measured in bytes, is at least a hundred times larger than the request. Due to the number and size of the responses, the bandwidth of the target network or the receiver's IT system will become overloaded beyond its capacity. Thus, any technical IT component can be the target of this type of attack. Finally, DNS reflection attacks benefit from open resolvers.

3. Requirements

The specific requirements of module APP.3.6 *DNS Servers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Central Administration

3.1. Basic Requirements

The following requirements MUST be met for module APP.3.6 DNS Servers as a matter of priority:

APP.3.6.A1 Planning the Use of VPNs (B)

The use of DNS servers MUST be planned carefully. The manner in which the DNS network service should be set up MUST be determined first. Sensitive domain information MUST also

be identified. The manner in which DNS servers are to be incorporated into the network of the information domain in question MUST be planned. All decisions MUST be documented appropriately.

APP.3.6.A2 Deployment of Redundant DNS Servers (B)

Advertising DNS servers MUST be designed for redundancy. There MUST be at least one additional secondary DNS server for every advertising DNS server.

APP.3.6.A3 Use of Separate DNS Servers for Internal and External Requests (B)

Advertising DNS servers and resolving DNS servers MUST be separated on the server side. The resolvers of internal IT systems MUST ONLY use internal resolving DNS servers.

APP.3.6.A4 Secure Basic Configuration of a DNS Server (B)

A resolving DNS server MUST be configured to only accept requests from the internal network. If a resolving DNS server sends requests, it MUST use random source ports. If DNS servers delivering forged domain information are known, the resolving DNS server MUST be prevented from sending requests to these DNS servers. An advertising DNS server MUST be configured to always handle requests from the Internet iteratively.

It MUST be ensured that DNS zone transfers between primary and secondary DNS servers function appropriately. Zone transfers MUST be configured so that they are only possible between primary and secondary DNS servers. Zone transfers MUST be limited to certain IP addresses. The version of the DNS server product used MUST be hidden.

APP.3.6.A5 ELIMINATED (B)

This requirement has been eliminated.

APP.3.6.A6 Securing Dynamic DNS Updates (B)

It MUST be ensured that only legitimate IT systems are allowed to modify domain information. The domain information that can be changed by the IT systems MUST be specified.

APP.3.6.A7 Monitoring of DNS Servers (B)

DNS servers must be monitored continuously. In particular, DNS server load MUST be monitored in order adapt the performance capacity of the hardware in good time. DNS servers MUST be configured in such a way that at least the following security-relevant events are logged:

- number of DNS requests
- number of errors in DNS requests
- errors in extension mechanisms for DNS (EDNS)
- expiring zones
- failed zone transfers

APP.3.6.A8 Administration of Domain Names [Central Administration] (B)

It MUST be ensured that the registrations for all of the domains that an organisation uses are extended regularly and in good time. An employee MUST be assigned responsibility for the administration of Internet domain names. If an organisation commissions an Internet service provider to handle domain administration, it MUST be ensured that the organisation retains control of the domains.

APP.3.6.A9 Creation of a Business Continuity Plan for DNS Servers (B)

A business continuity plan MUST be drawn up for DNS servers. This business continuity plan MUST be integrated into the existing business continuity plans of the organisation in question. The DNS server business continuity plan MUST describe a data backup concept for the zone and configuration files. The business continuity plan for the zone and configuration files MUST be integrated into the organisation's existing backup plan. The contingency plan for DNS servers MUST include a plan to restore all the DNS servers in the information domain under consideration.

3.2. Standard Requirements

For module APP.3.6 *DNS Servers*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.3.6.A10 Selection of a Suitable DNS Server Product (S)

If a DNS server product is procured, care SHOULD be taken to ensure that it has proven itself sufficiently in practice. The DNS server product SHOULD support the current RFC standards. Furthermore, the DNS server product SHOULD support the person in charge in creating syntactically correct master files.

APP.3.6.A11 Sufficient Capacity of DNS Servers (S)

The hardware of a DNS server SHOULD have sufficient capacity. A DNS server's hardware SHOULD be used exclusively to operate the server. The network connections of all the DNS servers in the information domain under consideration SHOULD be dimensioned sufficiently.

APP.3.6.A12 ELIMINATED (S)

This requirement has been eliminated.

APP.3.6.A13 Limited Visibility of Domain Information (S)

An information domain's name space should be divided into a public and an organisation-internal area. The public part SHOULD only include the domain information required by services that are to be accessible from external sources. IT systems in the internal network SHOULD not be assigned any DNS names that may be resolved from external sources if they have a public IP address.

APP.3.6.A14 Location of Name Servers (S)

Primary and secondary advertising DNS servers SHOULD be located in different network segments.

APP.3.6.A15 Analysis of Log Data (S)

DNS server log data SHOULD be checked regularly. The DNS server log data SHOULD be evaluated regularly. At a minimum, the following security-relevant events SHOULD be evaluated:

- number of DNS requests
- number of errors in DNS requests
- errors in extension mechanisms for DNS (EDNS)
- expiring zones
- failed zone transfers
- changes in the ratio of errors to DNS requests

APP.3.6.A16 Integrating a DNS Server into a "P-A-P" Structure (S)

DNS servers SHOULD be integrated into a "packet filter—application level gateway—packet filter" (P-A-P) structure (see also NET.1.1 *Network Architecture and Design*). In the process, the advertising DNS server SHOULD be placed in a demilitarised zone (DMZ) of the outer packet filter. The resolving DNS server SHOULD be installed in a DMZ of the internal packet filter.

APP.3.6.A17 Use of DNSSEC (S)

The DNS protocol extension DNSSEC SHOULD be enabled on both resolving DNS servers and advertising DNS servers. The key signing keys (KSK) and zone signing keys (ZSK) used for this SHOULD be changed at regular intervals.

APP.3.6.A18 Advanced Securing of Zone Transfers (S)

Transaction signatures (TSIG) SHOULD be used additionally to achieve stronger security of zone transfers.

APP.3.6.A19 Disposal of DNS Servers (S)

A DNS server SHOULD be deleted from both the domain name space and the network system.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.3.6 *DNS Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.3.6.A20 Feasibility Reviews of Business Continuity Plans (H)

An organisation SHOULD check the feasibility of its business continuity plan for DNS servers on a regular basis.

APP.3.6.A21 Hidden Master (H)

In order to make attacks on a primary advertising DNS server more difficult, a hidden master configuration SHOULD be established.

APP.3.6.A22 Connecting DNS Servers via Different Providers (H)

Externally available DNS servers SHOULD be connected using different providers.

4. Additional Information

4.1. Useful Resources

The BSI has published the following additional documents related to DNS:

- BSI publication on cyber security BSI-CS 055: “Sichere Bereitstellung von DNS-Diensten: Handlungsempfehlungen für Internet-Service-Provider (ISP) und große Unternehmen” [Secure Provision of DNS Services: Recommendations for Internet Service Providers (ISPs) and Large Companies]
- BSI publication on cyber security BSI-CS 121: “Umsetzung von DNSSEC: Handlungsempfehlungen zur Einrichtung und zum Betrieb der Domain Name Security Extensions” [Use of DNSSEC: Recommendations for Setting up and Operating the Domain Name Security Extensions]
- Secure connection of local networks to the Internet (ISi-LANA)

The National Institute of Standards and Technology (NIST) provides recommendations on using DNS in the NIST Special Publication 800-81-2, “Secure Domain Name System (DNS)—Deployment Guide”.

RFC 1034, “Domain Names—Concepts and Facilities”, provides additional information on DNS.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.3.6 *DNS Servers*.

G 0.9 Failure or Disruption of Communication Networks

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.4.2 SAP ERP Systems

1. Description

1.1. Introduction

Enterprise resource planning systems from SAP are used to automate and technically support internal and external business processes. SAP ERP systems typically process confidential information, which means that all their components and data must be appropriately protected.

SAP ERP systems are currently available under the product names SAP Business Suite and SAP S/4HANA. An SAP ERP system is made up of various modules that can be used to map the structure of an organisation. The modules of a given SAP ERP system may cover areas such as accounting, human resources, and logistics. The core components of the SAP ERP system are SAP NetWeaver (application server middleware) and SAP HANA (application server and database). SAP NetWeaver enables clients to integrate SAP ABAP and SAP Java applications and control processes throughout the system. SAP HANA can analyse large amounts of data for all business units in real time.

1.2. Objective

This module describes the risks to be considered with regard to SAP ERP systems and how these systems can be securely installed, configured, and operated. It is geared towards Chief Information Security Officers and administrators who are in charge of planning and implementing SAP ERP systems.

1.3. Scoping and Modelling

Module APP.4.2 *SAP ERP Systems* must be applied to every SAP ERP system.

This module is limited to the core installation of an SAP ERP system and focuses on the specific characteristics of the underlying SAP NetWeaver application server. It does not describe all the available SAP products in detail. The following descriptions are limited to the configuration of the SAP Basis and do not address the configuration of modules or applications.

Requirements for developing ABAP programs can be found in module APP.4.6 *SAP ABAP Programming*. No adjacent IT systems, operating systems, or databases are considered in detail. On these subjects, specific modules such as SYS1.2.2 *Windows Server 2012*, SYS.1.3 *Linux and Unix Servers*, APP.4.3 *Relational Database Systems* should be applied. This module also does not deal with SAP HANA. Current product names are deliberately omitted, as these change frequently.

2. Threat Landscape

For module APP.4.2 *SAP ERP Systems*, the following specific threats and vulnerabilities are of particular importance:

2.1. Lack of Consideration of SAP Security Recommendations

If an SAP ERP system is set up without taking SAP's recommended security guides into account, this can lead to serious security problems in the system. For example, SAP recommendations on user and authorisation management may not be implemented correctly. Ignoring such SAP recommendations, which protect communications or interface operations that use RFC and web services, can lead to vulnerabilities. This can leave an entire system open to attacks.

2.2. Insufficient Application of Patches and SAP Security Notes

SAP ERP systems are complex and consist of different modules and components that usually process sensitive data. SAP therefore regularly publishes patches and Security Notes to correct software errors and known vulnerabilities. If new patches or SAP security notes are not applied promptly or at all, open vulnerabilities could be exploited by attackers. This could then allow them to manipulate SAP ERP systems. This could compromise confidential data, cause services to fail, or bring entire business processes to a standstill.

2.3. Lack of Planning, Implementation, and Documentation of an SAP Access Control Policy

SAP access control policies are functionally and technically complex. As a result of these high demands, many organisations fail to adequately plan and implement such policies. However, the lack of a well thought-out access control policy can often result in users receiving more authorisations than necessary. These users could then deliberately manipulate or accidentally damage an SAP ERP system and put its integrity, confidentiality, and availability at risk.

In addition, the design of authorisations in S/4HANA systems must be precisely mapped and synchronised among the integrated ABAP, HANA, and NetWeaver Gateway components (for Fiori applications); otherwise, contradictory authorisations could be assigned.

If an SAP access control policy is not sufficiently documented, assigned authorisations cannot be traced and maintained. Among other possible consequences, employees who have left a given organisation or have been assigned new tasks may retain the ability to access the organisation's SAP ERP systems.

2.4. Lack of SAP Documentation and Contingency Concepts

If there is no documentation for an SAP ERP system or such documentation is not kept up to date, it will not be possible to determine how the system was initially set up. This could delay the restoration of service in an emergency or cause business-critical processes to fail completely. This threat also applies if there are no contingency plans that describe in detail how the persons in charge should proceed in the event of an emergency.

3. Requirements

The specific requirements of module APP.4.2 *SAP ERP Systems* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Department, BCM Officer, Developer

3.1. Basic Requirements

For module APP.4.2 *SAP ERP Systems*, the following requirements MUST be implemented as a matter of priority:

APP.4.2.A1 Secure Configuration of the SAP Java Stack (B)

The SAP ABAP stack MUST be configured securely. For this purpose, the respective profile parameters MUST be set (e.g. for password security, authentication, and encryption). The system change option and the clients MUST also be configured, IMG customising carried out, and the operating system commands saved.

APP.4.2.A2 Secure Configuration of the SAP Java Stack (B)

The SAP Java stack MUST be configured securely if it is used. Security mechanisms and concepts that are different from the SAP ABAP stack MUST be created for this. Administrators MUST therefore know the architecture of the Java stack and how it is administered. In addition, unnecessary services MUST be shut down, standard content removed, HTTP services protected, and access to administration interfaces restricted.

APP.4.2.A3 Network Security (B)

To guarantee network security, appropriate concepts MUST be created that factor in the SAP ERP system and the settings made therein.

Furthermore, the SAP router and SAP Web Dispatcher SHOULD be used to implement and maintain a secure SAP network.

In order to avoid vulnerabilities due to misinterpretations or misunderstandings, the IT Operation Department, firewall operations, portal operations, and SAP operations MUST be coordinated.

APP.4.2.A4 Protection of Standard SAP User IDs (B)

Immediately after installing an SAP ERP system, the default passwords for the standard user IDs MUST be changed. Suitable safeguards MUST also be taken to secure the standard SAP user IDs that have been set up. Certain standard user IDs MUST NOT be used (e.g. for RFC connections and background jobs).

APP.4.2.A5 Configuration and Protection of SAP User Administration (B)

SAP user administration for ABAP systems MUST be undertaken in a secure and careful manner. Activities such as creating, changing, and deleting users; resetting and unlocking passwords; and assigning roles and profiles MUST be part of user administration.

APP.4.2.A6 Creation and Implementation of a User and Access Control Policy [Department, Developer] (B)

A user and access control policy MUST be developed and implemented for SAP ERP systems. The following points MUST be considered:

- the identity principle, minimum principle, job principle, document principle of accounting, document principle of authorisation administration, segregation of duties principle (SoD), approval principle, standard principle, written form principle, and control principle MUST be taken into account.
- User, authorisation, and profile administrators MUST have separate responsibilities and authorisations.
- Procedures MUST be defined within authorisation administration for *creating, changing, deleting, and transporting roles, as well as for transporting SU24 default values*. Authorisation roles SHOULD be created and maintained in the development system. They SHOULD be transported using the Transport Management System (TMS). Authorisations SHOULD be created, saved, and assigned to the users in authorisation roles (PFCG roles) in a role-based access control policy. Since individual critical actions in the roles cannot always be avoided, they SHOULD be covered by mitigation controls.
- Within the framework of the access control policy, procedures MUST be defined for the *request, approval, modification, and deletion of users and authorisations*.
- Naming conventions MUST be defined for user IDs and technical role names.
- Default values and check indicators SHOULD be maintained in transaction SU24. The corresponding procedure SHOULD be described in the user and access control policy.
- Legal and internal framework conditions such as the German Generally Accepted Accounting Principles (German GAAP), the German Commercial Code (HGB), and the organisation's internal specifications MUST be taken into account. The user and access control policy SHOULD also cover the operation of technical accounts, including the authorisation of background and interface users.

Appropriate control mechanisms SHOULD be applied to check for SoD conflicts in roles and monitor the assignment of critical authorisations to users.

If components such as SAP HANA and SAP NetWeaver Gateway (for Fiori applications) are used in addition to the ABAP back end, the design of the authorisations among the components MUST be coordinated and synchronised.

APP.4.2.A7 Protection of SAP Databases (B)

Access to SAP databases MUST be secured. Whenever feasible, administrators SHOULD only be able to access the databases with SAP tools. If third-party software is used for this purpose, additional security safeguards MUST be implemented. The users *SAPR3* or *SAP<SID>* MUST NOT be used to connect to databases. In addition, the default passwords (e.g. for *SAPR3* or *SAP<SID>*) MUST be changed and certain database tables (such as USR* tables) placed under special protection.

APP.4.2.A8 Protection of the SAP RFC Interface (B)

To protect the Remote Function Call (RFC) interface, RFC connections, RFC authorisations, and RFC gateways MUST be configured securely.

Uniform administrative guidelines MUST be created and implemented for all RFC connections. For this purpose, the required RFC connections SHOULD be defined and documented. Connections with a stored password SHOULD not be configured from lower- to higher-privileged systems (e.g. from *Dev* to *Prod*). RFC connections that are no longer used MUST be deleted.

All RFC gateways MUST be securely administered and suitable profile parameters MUST be set (e.g. *gw/monitor, gw/reg_no_conn_info* and *snc/permit_insecure_start*). All connections that are established via a gateway MUST be analysed and evaluated in terms of their security. Furthermore, logging MUST be enabled. Access control lists (ACLs) MUST be defined.

APP.4.2.A9 Protecting and Monitoring the Message Server (B)

The message server MUST be secured by appropriate settings in the profile parameters. Among other things, it MUST be decided whether ACLs are to be set up for the internal message server. The message server MUST be monitored using appropriate mechanisms so that system failures on the message server are detected quickly (for example).

APP.4.2.A10 ELIMINATED (B)

This requirement has been eliminated.

3.2. Standard Requirements

For module APP.4.2 *SAP ERP Systems*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements They SHOULD be met as a matter of principle.

APP.4.2.A11 Secure Installation of an SAP ERP System (S)

When installing an SAP ERP system, current SAP security guides and documentation SHOULD be taken into account. In addition, the security policy of the organisation at hand SHOULD be observed. It SHOULD also be ensured that the SAP ERP system is to be installed on a secure operating system.

APP.4.2.A12 SAP Authorisation Development [Department, Developer] (S)

Technical authorisations SHOULD be developed on the basis of technical specifications. Furthermore, SAP authorisations SHOULD be adapted or created anew on the development system of the SAP landscape under consideration. In cases involving S/4HANA, this SHOULD also include authorisation development on HANA databases. Repository roles SHOULD be set up and transported, as well. Database privileges SHOULD NOT be assigned directly to users.

For software developed in-house (e.g. for transactions or authorisation objects), transaction SU24 SHOULD be maintained (assignments of authorisation objects to transactions). Full authorisation (*) or intervals in object values SHOULD be avoided.

Authorisation development SHOULD be carried out as part of change management.

It SHOULD be ensured that the production system in question is adequately protected against authorisation changes and that no developer keys are assigned. The respective quality assurance system SHOULD be operated in the same way as the production system when assigning authorisations and adding settings.

APP.4.2.A13 SAP Password Security (S)

To ensure secure logins to an SAP ERP system, profile parameters, customising switches, or a security policy SHOULD be configured appropriately.

The hash algorithms used for the stored hash values of the passwords in an SAP ERP system SHOULD comply with the current security standards. Access to tables with hash values SHOULD be restricted.

APP.4.2.A14 Identification of Critical SAP Authorisations [Department] (S)

The handling of critical authorisations SHOULD be strictly controlled. These authorisations, roles, and profiles SHOULD be assigned restrictively. This SHOULD also be ensured for critical role combinations and additive effects, such as cross authorisations.

Critical authorisations SHOULD be regularly identified, reviewed, and evaluated. The SAP profiles *SAP_ALL* and *SAP_NEW** and the SAP authorisation object *S_DEVELOP* (with change authorisations *ACTVT 01* and *02*) SHOULD not be assigned in a production system. Emergency users SHOULD be excluded from this requirement.

APP.4.2.A15 Secure Configuration of the SAP Router (S)

The SAP router SHOULD regulate access to the network and complement the existing firewall architecture appropriately. It SHOULD also control access to the SAP ERP system.

APP.4.2.A16 Implementation of Security Requirements for the Windows Operating System (S)

The SAP ERP system SHOULD NOT be installed on a Windows domain controller. The SAP-specific users, such as *<sid>adm* or *SAPService <sid>*, SHOULD be secured. After installation, the user *<db><sid>* SHOULD be locked.

The user SAPService *<sid>* SHOULD NOT have any interactive login rights. With respect to these authorisations, the system resources associated with the SAP ERP system (such as files, processes, and shared memory) SHOULD be protected.

Appropriate settings SHOULD be used to secure the specific authorisations of the users *Guest, System, SAP system users = <sapsid>adm, SAPService<SAPSID>* and *Database users = <database-specific users>*, as well as user groups created by the SAP ERP system.

APP.4.2.A17 Implementation of Security Requirements for the Unix Operating System (S)

Access authorisations SHOULD be defined for the SAP ERP system directories in Unix. The passwords of the system-specific users *<sid>adm* and *<db><sid>* SHOULD also be changed. After installation, the user *<db><sid>* SHOULD be locked.

APP.4.2.A18 Disabling Insecure Communications (S)

Communications with and among SAP ERP systems SHOULD be secured with SNC. If the database and the SAP application server are operated on different systems, the database connection SHOULD be encrypted appropriately. The internal services of the SAP application server SHOULD ONLY communicate with each other using TLS.

APP.4.2.A19 Definition of Security Policies for Users (S)

Specific security policies for passwords and login restrictions SHOULD be created for specific users and user groups. For example, users with critical authorisations SHOULD be protected by strong password rules (SECPOL transaction). Security policies SHOULD be correctly assigned to users and checked regularly.

APP.4.2.A20 Secure SAP GUI Settings (S)

SAP GUI SHOULD be installed on all clients and updated regularly. SAP GUI ACLs SHOULD also be activated and appropriate administration rules distributed and activated.

APP.4.2.A21 ELIMINATED (S)

This requirement has been eliminated.

APP.4.2.A22 Protection of the Spool in the SAP ERP System [Developer] (S)

It SHOULD be ensured that data from sequential data processing such as spool or print can only be accessed to a limited extent. Unauthorised users SHOULD also be prevented from accessing the TemSe data store used by the SAP spool system. The authorisations granted SHOULD be checked regularly.

APP.4.2.A23 Protection of SAP Background Processing [Developer] (S)

SAP background processing SHOULD be protected against unauthorised access. For batch jobs, various system user IDs SHOULD be defined and created according to their functional areas. Dialogue users SHOULD NEVER be authorised for this purpose.

APP.4.2.A24 Activation and Protection of the Internet Communication Framework (S)

It SHOULD be ensured that only necessary ICF services are activated. All ICF services that are under an ICF object SHOULD only be activated individually. Authorisations SHOULD be assigned restrictively. Communications SHOULD be encrypted.

APP.4.2.A25 Secure Configuration of the SAP Web Dispatcher (S)

The SAP Web Dispatcher SHOULD not be the first entry point from the Internet into an SAP ERP system. The SAP Web Dispatcher SHOULD always be up to date. It SHOULD be configured securely.

APP.4.2.A26 Protection of Customers' Own Code in the SAP ERP System (S)

A custom code management process SHOULD be defined so that a customer's own code is removed if it can be replaced by standard SAP code or is no longer used. The requirements from the guideline for the development of ABAP programs SHOULD also be taken into account.

APP.4.2.A27 Auditing the SAP ERP System [Department] (S)

To ensure that all internal and external guidelines and requirements are being met, all SAP ERP systems SHOULD be audited regularly. The Security Optimization Service in SAP Solution Manager SHOULD be used for this purpose. The results of audits SHOULD be evaluated and documented.

APP.4.2.A28 Creation of a Contingency Concept [BCM Officer] (S)

A contingency concept SHOULD be created and followed for SAP ERP systems. It SHOULD secure business activities and meet the requirements of crisis management or business continuity management. The following points SHOULD be described and defined in the contingency concept:

- Incident detection and response
- Data backup and recovery
- Business continuity management

The contingency concept SHOULD be updated at regular intervals.

APP.4.2.A29 Setting Up Emergency Users (S)

User IDs SHOULD be created for emergency users. The IDs and authorisations that have been set up SHOULD be strictly controlled and precisely documented. In addition, all activities performed by emergency users SHOULD be logged.

APP.4.2.A30 Implementation of Continuous Monitoring of Security Settings (S)

The correctness of all SAP ERP system security settings SHOULD be constantly monitored. The proper application of all patches and updates SHOULD also be monitored. SAP monitoring SHOULD be integrated into an organisation's general system monitoring.

APP.4.2.A31 Configuration of SAP Single Sign-On (S)

If multiple SAP ERP systems exist, users SHOULD access the systems with SAP Single Sign-On (SAP SSO). The SAP ERP systems that will be included in the SSO mechanism SHOULD be determined in the planning phase. SSO SHOULD be configured and operated securely.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.4.2 *SAP ERP Systems* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.4.2.A32 Real-Time Detection and Alerts for Irregular Processes (H)

The most important security recording functions in SAP ERP systems, such as the security audit log or system log, SHOULD be continuously monitored. An employee in charge SHOULD be automatically alerted in the event of suspicious transactions. To analyse SAP-specific security incidents and differentiate false reports from actual security incidents, employees SHOULD either be trained or third-party services should be used.

4. Additional Information

4.1. Useful Resources

The SAP Help Portal (https://www.help.sap.com/viewer/index) is the central entry point to support from SAP. It offers extensive information and instructions on a wide range of subjects. A selection of topics of interest in the context of SAP ERP systems is listed below:

- SAP Audit Management, https://help.sap.com/saphelp_fra110/helpdata/de/ab/ce1b52bd543c3ae10000000a441470/frameset.htm und https://help.sap.com/saphel_erp60_sp/helpdata/de/f9/558f40f3b19920e10000000a1550b0/content.htm
- User Management of SAP NetWeaver AS for Java, https://help.sap.com/saphelp_nw73/helpdata/de/45/b90177cf2252f8e10000000a1553f7/content.htm?no_cache=true
- Central User Administration, https://help.sap.com/doc/erp2005_ehp_07/6.07/de-DE/8d/270bea613d2443bad6ce0524f08ca0/frameset.htm

Detailed best-practice recommendations on audits of SAP ERP systems are provided in the auditing guide SAP ERP 6.0: Best Practice—Recommendations of the German-speaking SAP User Group (DSAG).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the

second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.4.2 *SAP ERP Systems*.

G 0.14 Interception of Information / Espionage

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.4.3 Relational Database Systems

1. Description

1.1. Introduction

Database systems (DBS) are often used as auxiliary resources in organising, creating, modifying, and managing large data collections with the help of IT. A DBS consists of a database management system (DBMS) and one or more databases. A database is a collection of data and corresponding descriptions (metadata) that is continuously stored in a database system. Since database systems often play a central role in IT infrastructure, they have to meet essential security requirements. The core processes of an organisation typically depend on information from databases. This results in corresponding availability requirements. Additionally, there are often high requirements regarding the confidentiality and integrity of the information stored in databases.

1.2. Objective

The objective of this module is to demonstrate the secure operation of relational database systems and the appropriate protection of the information processed and stored in databases. It thus describes requirements that can be used to securely plan, implement, and operate database systems and reduce threats.

1.3. Scoping and Modelling

APP.4.3 *Relational Database Systems* must be applied once to each relational database system in use.

This module describes requirements for relational database systems. Security requirements for non-relational database systems are not covered here.

In order to continuously protect the information in databases, security requirements for the design of database tables and access to databases should have been considered during the corresponding application development process. However, this module does not cover these issues.

It also does not address the threats and requirements that affect the operating system and hardware on which a database system is installed. These aspects are covered in the corresponding operating system-specific modules of the IT Systems layer, e.g. SYS.1.3 *Linux and Unix Servers* or SYS.1.2.2 *Windows Server 2012*.

Relational database systems should always be considered as part of modules OPR.4 *Identity and Access Management*, OPS.1.1.3 *Patch and Change Management*, CON.3 *Backup Concept*, OPS.1.2.2 *Archiving*, OPS.1.1.5 *Logging*, and OPS.1.1.2 *Proper IT Administration*.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module APP.4.3 *Relational Database Systems*, the following specific threats and vulnerabilities are of particular importance.

2.1. Insufficient System Resources

If the hardware of a database system does not have sufficient system resources at its disposal, the database may work improperly or fail completely. One consequence is that it may not be possible to store data. Resources can also be heavily utilised at peak times, which can lead to a deterioration in performance. This in turn may cause applications to be executed improperly, or not at all.

2.2. Enabled Default User Accounts

Upon initial installation or in the delivered configurations of a database management system, user and administration accounts are frequently not protected or only protected with publicly known passwords. This means these accounts can be misused. For example, an attacker may use publicly known login data to access a database management system as a user—or even as an administrator. The attacker will then be able to read, manipulate, or delete the configuration or the data stored.

2.3. Unencrypted Database Connections

In their default configuration, many database management systems establish unencrypted connections to applications. If the communication between applications and database management systems is not encrypted, third parties may access information or manipulate it during transmission.

2.4. Data Loss in a Database

Data may be lost in a database due to hardware or software flaws or human error. Since important information for applications is stored in databases in most cases, services may then be unavailable or entire production processes may come to a halt.

2.5. Loss of Integrity of Stored Data

Incorrect database configurations, software errors, or manipulated data may compromise the integrity of the information contained in a database. If this is only detected later on or not at all, an organisation's core processes may be strongly impaired. For example, if the integrity relationships (referential integrity) between tables are not defined correctly, this may result in incorrect data in the database. If such an error is only detected during production operations or not detected at all, the inconsistent data is not the only thing that will require time-consuming cleansing and reconstruction. Considerable damage can also occur over time—for example, when the data in question relates to critical areas such as taxes, accounting, or even the control of entire production systems.

2.6. SQL Injections

SQL injections are frequently used to attack database systems. When an application accesses the data of an SQL database, SQL commands are transmitted to the DBMS. If input data within the application is not validated sufficiently, attackers can import their own SQL commands into the application that can then be edited with the authorisation of the application’s service account. This way, an attacker may read, manipulate, or delete data; add new data; or even call system commands. Although SQL injections primarily affect front-end applications, they can also have a significant impact on the database system itself and the related infrastructure.

2.7. Insecure Configuration of the Database Management System

Frequently, functions that are not required are enabled in the default configuration of a database management system, which makes it easier for potential attackers to read or manipulate information in the adjacent database. In order to administer a DBMS without having to provide any authentication, an attacker may, for example, be able to establish a connection to an unused programming interface because the corresponding organisation has not changed the default installation. As a consequence, they may access the organisation's databases without authorisation.

2.8. Malware and Insecure Database Scripts

In many database management systems, it is possible to automate certain actions. To this end, scripts are executed in the context of a database, including with the help of the Procedural Language/Structured Query Language (PL/SQL). This also includes database triggers. However, if these are not checked by the process owner before they are used, the database scripts may not meet the software development requirements of the respective organisation.

An attacker may also manipulate data dictionary tables or other core functions of a database with the help of malware or database scripts, for example. Detecting this kind of attack is very hard. Malware and low-quality scripts can endanger the confidentiality, integrity, and availability of the data stored in databases.

3. Requirements

The specific requirements of module APP.4.3 *Relational Database Systems* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner, Developer

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

APP.4.3.A1 Creation of a Security Policy for Database Systems (B)

Based on its general security policy, an organisation MUST draw up a security policy specific to database systems. This MUST describe requirements and specifications for the secure operation of database systems in a comprehensible manner. The guideline MUST be familiar to all employees responsible for database systems. It MUST be integral to their work. If the policy is changed or deviations from the requirements are allowed, this MUST be coordinated with the CISO and documented. The correct implementation of the policy MUST be reviewed on a regular basis. The results MUST be documented in an appropriate manner.

APP.4.3.A2 ELIMINATED (B)

This requirement has been eliminated.

APP.4.3.A3 Basic Hardening of Database Management Systems (B)

Database management systems MUST be hardened. To this end, a checklist of the steps to be performed MUST be compiled and completed. Passwords MUST NOT be stored in plain text. Basic hardening MUST be reviewed and adapted as required at regular intervals.

APP.4.3.A4 Controlled Creation of New Databases (B)

New databases MUST be created in accordance with a defined process. When a new database is created, basic information on the database MUST be documented in a comprehensible manner.

APP.4.3.A5 ELIMINATED (B)

This requirement has been eliminated.

APP.4.3.A6 ELIMINATED (B)

This requirement has been eliminated.

APP.4.3.A7 ELIMINATED (B)

This requirement has been eliminated.

APP.4.3.A8 ELIMINATED (B)

This requirement has been eliminated.

APP.4.3.A9 Backing Up a Database System (B)

System backups of a DBMS and its data MUST be performed at regular intervals. The database system MUST also be backed up before a new database is created. The service programs permitted for this purpose SHOULD be used.

All transactions SHOULD be backed up in such a way that they can be recovered at any time. If the backup process would exceed the available capacity, an extended concept SHOULD be created to back up the database (e.g. incremental backups). The recovery parameters SHOULD be specified based on the protection needs of the data (see CON.3 *Backup Concept)*.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

APP.4.3.A10 ELIMINATED (S)

This requirement has been eliminated.

APP.4.3.A11 Sufficient Hardware Capacity [Process Owner] (S)

Database management systems SHOULD be installed on sufficiently sized hardware. The hardware SHOULD have sufficient reserves in order to meet potentially increasing requirements. If resource bottlenecks become apparent during operations, these SHOULD be eliminated at an early stage. When sizing hardware, the growth expected for the scheduled deployment period SHOULD be taken into account.

APP.4.3.A12 Uniform Configuration Standard for Database Management Systems (S)

A uniform configuration standard SHOULD be defined for all the database management systems deployed. All database management systems SHOULD be configured and operated in the same manner according to this standard. If an installation requires a deviation from the configuration standard, all steps SHOULD be approved by the CISO and documented in a comprehensible manner. The configuration standard SHOULD be reviewed and adapted as required at regular intervals.

APP.4.3.A13 Restrictive Utilisation of Database Links (S)

It SHOULD be ensured that only persons accountable are authorised to create database links (DB links). If such links are created, private DB links MUST be preferred to public DB links. All DB links created by the persons accountable SHOULD be documented and reviewed at regular

intervals. Additionally, DB links SHOULD be taken into account when the database system is backed up (see APP.4.3.A9 *Backing Up a Database System*).

APP.4.3.A14 ELIMINATED (S)

This requirement has been eliminated.

APP.4.3.A15 ELIMINATED (S)

This requirement has been eliminated.

APP.4.3.A16 Encryption of Database Connections (S)

A database management system SHOULD be configured in such a way that database communications are always encrypted. The cryptographic methods and protocols used to this end SHOULD comply with the internal specifications of the respective organisation (see CON.1 *Crypto Concept*).

APP.4.3.A17 Data Transfer or Migration [Process Owner] (S)

The manner in which data should be transferred to a database initially or regularly SHOULD be defined in advance. After data is transferred, checks SHOULD be performed to ensure that it is complete and has not been changed.

APP.4.3.A18 Database Management System Monitoring (S)

The parameters, events, and operating states of a database management system that are critical for secure operations SHOULD be defined. These SHOULD be monitored using a corresponding system. Threshold values SHOULD be defined for all critical parameters, events, and operating states. If these values are exceeded, appropriate action MUST be taken. The responsible staff members SHOULD be alerted. Application-specific parameters, events, operating states, and their threshold values SHOULD be coordinated with the persons accountable for the specialised applications in use.

APP.4.3.A19 Protection Against Malicious Database Scripts [Developer] (S)

When database scripts are developed, binding quality criteria SHOULD be defined for them (see CON.8 *Software Development*). Database scripts SHOULD be subjected to extensive functional tests on separate test systems before they are used in production environments. The results SHOULD be documented.

APP.4.3.A20 Regular Audits (S)

All the components of a database system SHOULD be checked regularly in terms of whether all the specified security safeguards have been implemented and are configured correctly. This SHOULD include checks of whether the documented status corresponds to the actual status and whether the configuration of the database management system corresponds to the documented standard configuration. In addition, it SHOULD be determined whether all the database scripts at hand are actually needed. Whether they meet the quality standards of the respective organisation SHOULD also be checked. Furthermore, the log files of the database system and the operating system SHOULD be checked for irregularities (see DER.1 *Detecting Security-Relevant Events*). The audit results SHOULD be documented in a transparent manner. They SHOULD be compared against the target status. Deviations SHOULD be investigated.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

APP.4.3.A21 Use of Database Security Tools (H)

Information security products SHOULD be used for databases. The products used SHOULD provide the following functions:

- Creation of an overview of all database systems
- Extended configuration options and rights management for databases
- Detection and prevention of possible attacks (e.g. brute force attacks on a user account or SQL injections)
- Audit functions (e.g. checking configuration requirements)

APP.4.3.A22 Contingency Planning (H)

A business continuity plan that includes information on how emergency operations can be carried out SHOULD be prepared for the database management system in use. The resources required for the business continuity plan SHOULD be identified. Additionally, the business continuity plan SHOULD define how the respective organisation can return from emergency operations to regular operations. The business continuity plan SHOULD define the necessary reporting channels, response routes, resources, and response times for the Process Owners. Based on a coordination plan for the restoration of service, all IT systems that depend on the database in question SHOULD be identified in advance and taken into consideration.

APP.4.3.A23 Archiving (H)

If the data of a database system needs to be archived, a corresponding archiving concept SHOULD be drawn up. It SHOULD be ensured that the existing data will be available at a later point in time in a complete and consistent manner.

The archiving concept SHOULD define both archiving intervals and the storage period of the archived data. Additionally, the technology used to archive the database SHOULD be documented. The archived data SHOULD be used for regular recovery tests. The results SHOULD be documented.

APP.4.3.A24 Data Encryption in Databases (H)

The data stored in databases SHOULD be encrypted. In this process, the following factors (among others) SHOULD be considered beforehand:

- Effects on performance
- Key management processes and methods, including separate key storage and security
- Effects on backup recovery concepts
- Functional impact on the database (regarding sorting options, for example)

APP.4.3.A25 Security Audits of Database Systems (H)

Security audits SHOULD be carried out on database systems at regular intervals. The systemic and manufacturer-specific aspects of the database infrastructure (e.g. directory services) used and the database management system deployed SHOULD be considered within the framework of security audits.

4. Additional Information

4.1. Useful Resources

The BSI has published the following partner contributions on the topic of database security within the framework of the Alliance for Cyber Security:

- Oracle: Datenbank-Sicherheit – Grundüberlegungen [Oracle: Database Security – Basic Considerations]
- McAfee: Datenbanksicherheit in Virtualisierungs- und Cloud-Computing-Umgebungen [McAfee: Database Security in Virtualisation and Cloud Computing Environments]

The Deutsche Telekom Group has published the document "Sicherheitsanforderung Datenbanksysteme" [Security Requirements for Database Systems] as part of its Privacy and Security Assessment (PSA) process.

Section BA2.3, "Protection of Databases" of “The Standard of Good Practice for Information Security” (published by the Information Security Forum, ISF) provides guidelines for the protection of relational database systems.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module APP.4.3 *Relational Database Systems*.

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.4.4 Kubernetes

1. Description

1.1. Introduction

Kubernetes has established itself as the de facto standard for the orchestration of containers in public and private clouds. Kubernetes is also used for IoT and other applications; with K3S, for example, there is an edition that is intended for very small servers such as single-board computers. The cloud native stack, which consists of many different components, is also built on the standard established by Kubernetes.

The term "container" refers to a technique in which a host system runs applications in parallel in separate environments (virtualisation at the operating system level). In most cases, the monitoring, starting and stopping, and further administration of containers is carried out by management software, which thus takes over the *orchestration*. Kubernetes combines one or more related containers in a *pod*. Since the focus of this module is Kubernetes, it only considers pods and not individual containers. The orchestration is mostly carried out in groups of jointly managed Kubernetes nodes in one or more “clusters”.

Several products that have established themselves as ways to operate and manage the orchestration of pods make it possible to manage very large environments, as well. At their core, however, they are all based on Kubernetes. When considering such products, a distinction must be made between the *runtime*, which runs the processes on Kubernetes nodes, and the *orchestration*, which controls the runtimes on multiple Kubernetes nodes.

In addition to these two central components, the operation of Kubernetes usually consists of a specialised infrastructure that includes things like registries, code versioning and storage, automation tools, management servers, storage systems, or virtual networks.

The terms below are defined as follows for this module:

- *Application* means a collection of multiple programs that perform a task together
- *Cluster* means operating environments for containers with multiple nodes
- *Containers* are processes started from an image that run within operating system namespaces

- *Container Network Interface* (*CNI*) is the interface for managing the virtual networks in a cluster
- *Container Storage Interface* (*CSI*) is the interface to the mostly external storage systems that Kubernetes can provide to pods
- *Control plane* refers to all applications used for the management (i.e. orchestration) of nodes, runtimes, and clusters
- *Images* are all software packages that comply with the Open Container Initiative (OCI); these include both base images for custom images and images that are used unchanged
- *Node* refers to a server that is installed and optimised for the operation of a runtime
- *Pod* refers to a collection of several containers running within the same operating system namespace
- *Registry* is the generic term for code management and image storage
- *Runtime* is the software that runs the software in an image as a container

1.2. Objective

The objective of this module is to protect information that is processed, provided, or transmitted via Kubernetes clusters.

1.3. Scoping and Modelling

APP.4.4 *Kubernetes* should always be used in conjunction with module SYS.1.6 *Containerisation*. In terms of the focus of this module, the container runtime used or the additional applications that are part of the control plane are not relevant.

The module contains basic requirements for setting up, operating, and orchestrating with Kubernetes, as well as for the specialised infrastructure required for related operations. The latter includes registries, CSI/CNI, nodes, and automation software insofar as they interact directly with the cluster. The requirements for these applications mostly relate to the interfaces, but also include requirements that affect the operation of the applications to the extent that they directly affect the security of the respective cluster. Other services common in the Kubernetes environment, such as automation for CI/CD pipelines and code management (e.g. in Git) are not covered in depth in this module.

This module provides comprehensive modelling of a cluster. In this context, the applications of the control plane, services for automation, and nodes should be seen and treated as one group.

Security requirements for services operated in Kubernetes clusters, such as web servers (APP.3.2 *Web Servers*) or e-mail servers (see APP.5.3 *General E-Mail Clients and Servers*), are the subject of separate modules.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module APP.4.4 *Kubernetes*, the following specific threats and vulnerabilities are of particular importance.

2.1. Poor Authentication and Authorisation in the Control Plane

To manage runtimes, nodes, and Kubernetes itself, there needs to be administrative access for administrators and tool-based deployment. Such access is implemented in the form of either Unix sockets or network ports. Mechanisms for the authentication and encryption of administrative access are often present, but not activated by default in all products.

If unauthorised persons access a data network or its nodes, they can execute commands via unprotected administrative access points and impair the availability, confidentiality, and integrity of the data processed there.

2.2. Loss of Confidentiality of Access Data

Pods often require access data (access tokens) for Kubernetes. Through an attack on a pod, this access data can fall into unauthorised hands. With these credentials, it is possible for an attacker to interact with the control plane in an authenticated manner. With sufficient permissions, they can also make changes to the orchestration.

2.3. Resource Conflicts on Nodes

Individual pods can overload a node or its orchestration and thus jeopardise the availability of all other pods on the node, or the operation of the node itself.

2.4. Unauthorised Changes to Clusters

Automation with CI/CD and the consequent need to grant privileged access to tools carries the risk of unauthorised changes being made to clusters. For example, a developer may apply a new version of an application to a cluster that has not been sufficiently tested or has not gone through a release process. If there are errors in authorisations in a CI/CD environment, malware may be able to penetrate the clusters and read, delete, or change data there.

2.5. Unauthorised Communication

All the pods in a cluster are essentially able to communicate with each other, with the nodes in their own cluster, and with any other IT systems. If this communication is not restricted, malware or an attacker can exploit this to attack the control plane, other pods, or the nodes, for example.

There is also a risk that pods in the cluster will be unintentionally accessible from the outside. This would allow an external attack against services that should only be accessible within the cluster. This threat is exacerbated by the fact that less attention is often paid to internal

services. If a vulnerability is tolerated in a service that is only used internally but is also accessible from the outside, this puts the entire cluster at considerable risk.

3. Requirements

The specific requirements of module APP.4.4 *Kubernetes* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	None

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

APP.4.4.A1 Planning the Separation of the Applications (B)

Before going live, the manner in which the applications running in the pods in question and their different test and production operating environments will be separated MUST be planned. Based on the protection needs of the applications, the planning MUST determine which architecture of namespaces, meta tags, clusters, and networks adequately addresses the risks at hand and whether virtualised servers and networks should also be used.

The planning MUST include provisions separating for networks, CPUs, and persistent volumes. The separation SHOULD also take into account and be aligned with the network zone concept and the protection requirements at hand.

Each application SHOULD run in a separate Kubernetes namespace that includes all the programs of the application. Only applications with similar protection needs and similar possible attack vectors SHOULD share a Kubernetes cluster.

APP.4.4.A2 Planning Automation with CI/CD (B)

Automating the operation of applications in Kubernetes using CI/CD MUST ONLY take place after appropriate planning. The planning MUST cover the entire lifecycle from commissioning to decommissioning, including development, testing, operation, monitoring, and updates. A roles and rights concept and the securing of Kubernetes Secrets MUST be part of the planning.

APP.4.4.A3 Identity and Access Management for Kubernetes (B)

Kubernetes and all other control plane applications MUST authenticate and authorise each action taken by a user or, in automated mode, corresponding software. This applies whether

the actions are taken via a client, a web interface, or a corresponding API. Administrative actions MUST NOT be performed anonymously.

Each user MUST ONLY be granted the permissions they absolutely require. Unlimited access rights MUST be granted in a very restrictive manner.

Only a small group of people SHOULD be authorised to define automation processes. Only selected administrators SHOULD be given the right to create or change shares for persistent volumes in Kubernetes.

APP.4.4.A4 Separation of Pods (B)

The operating system kernel of nodes MUST have isolation mechanisms to restrict visibility and resource usage among the corresponding pods (cf. Linux namespaces and cgroups). At minimum, this isolation MUST include process IDs, inter-process communication, user IDs, the file system, and the network (including the hostname).

APP.4.4.A5 Backup in the Cluster (B)

A cluster MUST have a backup. The backup MUST include:

- Persistent volumes
- Configuration files for Kubernetes and the other programs of the control plane
- The current state of the Kubernetes cluster, including extensions
- Databases of the configuration (namely *etcd* in this case)
- All infrastructure applications required to operate the cluster and the services within it
- The data storage of the code and image registries

Snapshots for the operation of the applications SHOULD also be considered. Snapshots MUST NOT be considered a substitute for backups.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

APP.4.4.A6 Initialisation of Pods (S)

If an initialisation (e.g. of an application) takes place in a pod at start-up, this SHOULD take place in a separate Init container. It SHOULD be ensured that the initialisation terminates all processes that are already running. Kubernetes SHOULD ONLY start the other containers if the initialisation is successful.

APP.4.4.A7 Separation of Networks for Kubernetes (S)

Networks for the administration of nodes, the control plane, and the individual networks of application services SHOULD be separated.

Only the network ports of the pods necessary for operation SHOULD be released into the designated networks. If a Kubernetes cluster contains multiple applications, all the network connections between the Kubernetes namespaces SHOULD first be prohibited and only required network connections permitted (whitelisting). The network ports necessary for the

administration of the nodes, the runtime, and Kubernetes (including its extensions) SHOULD ONLY be accessible from the corresponding administration network and from pods that need them.

Only selected administrators SHOULD be authorised in Kubernetes to manage the CNI and create or change rules for the network.

APP.4.4.A8 Securing Configuration Files on Kubernetes (S)

The configuration files of a Kubernetes cluster, including all its extensions and applications, SHOULD be versioned and annotated.

Access rights to configuration file management software SHOULD be granted in a restrictive manner. Read and write access rights to the configuration files of the control plane SHOULD be assigned and restricted with particular care.

APP.4.4.A9 Use of Kubernetes Service Accounts (S)

Pods SHOULD NOT use the "default" service account. Rights SHOULD NOT be granted to the "default" service account. Pods for different applications SHOULD run under their own service accounts. Access rights for the service accounts of the applications' pods SHOULD be limited to those that are strictly necessary.

Pods that do not require a service account SHOULD not be able to view it or have access to corresponding tokens.

Only control plane pods and pods that absolutely need them SHOULD use privileged service accounts.

Automation programs SHOULD each receive their own tokens, even if they share a common service account due to similar tasks.

APP.4.4.A10 Securing Automation Processes (S)

All automation software processes, such as CI/CD and their pipelines, SHOULD only operate with the rights that are strictly necessary. If different user groups can change configurations or start pods via automation software, this SHOULD be done for each group through separate processes that only have the rights necessary for the respective user group.

APP.4.4.A11 Container Monitoring (S)

In pods, each container SHOULD define a health check for start-up and operation ("readiness" and "liveness"). These checks SHOULD provide information about the availability of the software running in a pod. The checks SHOULD fail if the monitored software cannot perform its tasks properly. For each of these checks, a time period SHOULD be defined that is appropriate for the service running in the pod. Based on these checks, Kubernetes SHOULD delete or restart the pods.

APP.4.4.A12 Securing Infrastructure Applications (S)

If a separate registry for images or automation software, persistent volume management, configuration file storage, or similar is in use, its protection SHOULD at least consider:

- Use of personal and service accounts for access

- Encrypted communication on all network ports
- Restrictive assignment of permissions to user and service accounts
- Logging of changes
- Regular data backups

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

APP.4.4.A13 Automated Configuration Auditing (H)

There SHOULD be an automated audit that checks the settings of nodes, of Kubernetes, and of the pods of applications against a defined list of allowed settings and standardised benchmarks.

Kubernetes SHOULD enforce these established rules in each cluster by connecting appropriate tools.

APP.4.4.A14 Use of Dedicated Nodes (H)

In a Kubernetes cluster, nodes SHOULD be assigned dedicated tasks and only run pods that are assigned to each task.

Bastion nodes SHOULD handle all incoming and outgoing data connections of between applications and other networks.

Management nodes SHOULD operate control plane pods and only handle control plane data connections.

If deployed, storage nodes SHOULD only operate the fixed persistent volume services pods in a cluster.

APP.4.4.A15 Separation of Applications at Node and Cluster Level (H)

Applications with very high protection needs SHOULD each use their own Kubernetes clusters or dedicated nodes that are not available for other applications.

APP.4.4.A16 Use of Operators (H)

The automation of operational tasks in operators SHOULD be used for particularly critical applications and control plane programs.

APP.4.4.A17 Attestation of Nodes (H)

Nodes SHOULD send a cryptographically secured (and, if possible, TPM-verified) status message to the control plane. The control plane SHOULD ONLY accept nodes into a cluster that have successfully proven their integrity.

APP.4.4.A18 Use of Micro-Segmentation (H)

Pods SHOULD ONLY be able to communicate with each other through the necessary network ports, even within a Kubernetes namespace. There SHOULD be rules within the CNI that disallow all but the necessary network connections within the Kubernetes namespace. These rules SHOULD precisely define the source and destination of the allowed connections using at least one of the following criteria: service name, metadata ("labels"), Kubernetes service accounts, or certificate-based authentication.

All the criteria used as labels for a connection SHOULD be secured in such a way that they can only be changed by authorised persons and management services.

APP.4.4.A19 High Availability of Kubernetes (H)

A Kubernetes operation SHOULD be set up in such a way that if a site fails, the clusters (and thus the applications in the pods) either continue to run without interruption or can be restarted in a short time at another site.

Should a restart be required, all the necessary configuration files, images, user data, network connections, and other resources required for operation (including the necessary hardware) SHOULD already be available at the alternative site.

For the uninterrupted operation of clusters, the control plane of Kubernetes, the infrastructure applications of the clusters, and the pods of the applications SHOULD be distributed across several fire zones based on the location data of the corresponding nodes so that the failure of a fire zone will not lead to the failure of an application.

APP.4.4.A20 Encrypted Data Storage for Pods (H)

The file systems containing the persistent data of the control plane (etcd in particular in this context) and the application services SHOULD be encrypted.

APP.4.4.A21 Regular Restart of Pods (H)

Pods SHOULD be stopped and restarted regularly if there is an increased risk of external interference and a very high need for protection. No pod SHOULD run for more than 24 hours. The availability of the applications in a pod SHOULD be ensured.

4. Additional Information

4.1. Useful Resources

For more information about threats and security safeguards with regard to containers, see the following publications, among others:

- NIST 800-190
  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf
- CIS Benchmark Kubernetes
  https://www.cisecurity.org/benchmark/kubernetes/

- OCI – Open Container Initiative
  https://www.opencontainers.org/
- CNCF – Cloud Native Computing Foundation
  https://www.cncf.io/

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module APP.4.4 *Kubernetes*:

G 0.14 Interception of Information / Espionage

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.4.6 SAP ABAP Programming

1. Description

1.1. Introduction

In-house or custom software development are often programmed in SAP systems. Such developments enable an organisation to adapt individual business processes or reporting requirements to its needs, for example. It is also possible to create special functions that are not available out-of-the-box.

Custom developments may be programmed by an organisation's in-house developers or by those it commissions. ABAP (Advanced Business Application Programming) is often used for this in the SAP environment.

ABAP is a proprietary, platform-independent programming language from the company SAP. It was developed for programming commercial applications in the SAP environment, and its basic structure bears a slight resemblance to the COBOL language. Its important features are:

- Integration of an authentication, role, and authorisation concept
- Use of a proprietary, database-agnostic SQL derivative (Open SQL)
- Support for communications among different SAP systems
- Integration of audit options

1.2. Objective

This module shows ABAP developers and security testers the relevant technical risks that can result from in-house or custom ABAP development. It also defines requirements that show how ABAP programs can be securely developed and used.

This module requires basic knowledge of ABAP and in-house or custom ABAP development tools.

1.3. Scoping and Modelling

Module APP.4.6 *SAP ABAP Programming* must be applied once to each SAP system that involves in-house or custom development created in the ABAP programming language.

This module supplements the modules CON.8 *Software Development*, APP.6 *General Software* and APP.7 *Development of Individual Software* with specific aspects of developing ABAP programs.

It describes the general risks of the ABAP programming language and is not a complete guide to developing ABAP programs. The module defines requirements that should be met from a security point of view when developing ABAP programs.

As web applications only make up a very small proportion of all ABAP applications in SAP implementations, web vulnerabilities are not the focus of this document.

2. Threat Landscape

For module APP.4.6 *SAP ABAP Programming*, the following specific threats and vulnerabilities are of particular importance:

2.1. Lack of Authorisation Checks

In SAP, authorisations are only checked in a given program if a corresponding authorisation check has been implemented by the developer. Without a check like this in the program code, no test is carried out to see if the user is actually authorised to carry out an action. Nevertheless, authorisation checks are frequently forgotten in custom-developed program code. This often renders the entire authorisation concept at hand ineffective and allows unauthorised persons to access the data stored in the respective SAP system. This can also lead to violations of compliance requirements, which can have serious consequences, especially with regard to audits.

2.2. Loss of Confidentiality or Integrity of Critical Data

SAP systems contain a significant amount of information critical to the organisations that run them. The SAP standard provides for various mechanisms to protect this data. However, information critical to an organisation could still be accessed without permission through faulty in-house or custom ABAP development. Employees or attackers could thus transfer data into an environment that can no longer be controlled. Critical data can also be manipulated through the use of ABAP programs in bypassing the standard SAP security mechanisms.

2.3. Injection Vulnerabilities

Injection vulnerabilities relate to an attacker's ability to insert control characters or commands into an application via an input field. A successful attack can disrupt the planned program sequence with unexpected commands.

Injection vulnerabilities represent the greatest security risk for in-house or custom development. Incorrect code in an ABAP application can sometimes allow an attacker to completely control an SAP system. Since such attacks are very complex and come in many variants, they are very difficult to detect and resolve without special training.

2.4. Bypassing Existing SAP Security Mechanisms

The SAP standard provides various protection mechanisms for data. They include client separation, identify management, roles, and authorisations. However, these security mechanisms can be deliberately bypassed or unintentionally omitted in code.

3. Requirements

The specific requirements of module APP.4.6 *SAP ABAP Programming* are listed below. As a matter of principle, the Developer is responsible for meeting the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Developer
Further responsibilities	

3.1. Basic Requirements

For module APP.4.6 *SAP ABAP Programming*, the following requirements MUST be MET as a matter of priority:

APP.4.6.A1 Protecting Reports with Authorisation Checks (B)

It MUST be ensured that only authorised users can start self-programmed evaluations (reports). Therefore, each report MUST perform explicit authorisation checks appropriate to the context at hand.

APP.4.6.A2 Formally Correct Evaluation of Authorisation Checks (B)

Each authorisation check in code MUST be evaluated by querying the return value *SY-SUBRC*.

APP.4.6.A3 Authorisation Check Before Starting a Transaction (B)

If developers use the *CALL TRANSACTION* command, a start authorisation check MUST always be performed before the command is executed.

APP.4.6.A4 No Proprietary Authorisation Checks (B)

Each authorisation check MUST be carried out using the *AUTHORITY CHECK* command provided for this purpose. Proprietary authorisation checks (e.g. based on user names) MUST NOT be used.

3.2. Standard Requirements

For module APP.4.6 *SAP ABAP Programming*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

APP.4.6.A5 Drawing Up a Policy for ABAP Development (S)

A policy SHOULD be drawn up for the development of ABAP programs. In addition to naming conventions, the policy SHOULD contain specifications for ABAP elements that may or may not be used. The requirements from this module SHOULD be included in the policy. The policy SHOULD be binding for Developers.

APP.4.6.A6 Complete Execution of Authorisation Checks (S)

During an authorisation check in ABAP code (*AUTHORITY-CHECK <OBJECT>*), it SHOULD be ensured that all fields are checked for the relevant authorisation object. If individual fields are not actually required, they SHOULD be marked as *DUMMY*. The reason for the exception SHOULD also be documented in the field.

APP.4.6.A7 Authorisation Check During Input Processing (S)

The function codes and screen elements of ABAP Dynpro applications SHOULD be consistent. If a screen element has been deactivated, an application SHOULD NOT react to the events of this element without adequate authorisation checks. If certain entries in a Dynpro menu are hidden or individual buttons are disabled, the corresponding function codes SHOULD also not be executed.

APP.4.6.A8 Protection Against Unauthorised or Manipulative Access to the File System (S)

If access to files on an SAP server depends on user input, this input SHOULD be validated before access is granted.

APP.4.6.A9 Authorisation Check in Remote-Enabled Function Modules (S)

It SHOULD be ensured that all remote-enabled function modules in program code explicitly check whether the initiator is authorised to execute the corresponding business logic.

APP.4.6.A10 Execution of Operating System Commands (S)

Each call of a permitted operating system command SHOULD be preceded by a corresponding authorisation check (authorisation object *S_LOG_COM*). User input SHOULD NOT be part of a command. For this reason, operating system calls SHOULD only be executed using standard SAP function modules intended for this purpose.

APP.4.6.A11 Avoiding Planted Malicious Code (S)

The ABAP commands *INSERT REPORT* and *GENERATE SUBROUTINE POOL* SHOULD NOT be used.

APP.4.6.A12 Avoiding Generic Module Execution (S)

Transactions, programs, function modules, and methods SHOULD NOT be generically executable. If there are important reasons for a generic execution, where and why this is

happening SHOULD be documented in detail. In addition, a whitelist SHOULD be defined that contains all the permitted modules. Before a module is called, the user's input SHOULD be compared against the whitelist.

APP.4.6.A13 Avoiding Generic Access to Table Contents (S)

Table contents SHOULD NOT be read generically. If there are important reasons for doing this, where and why this is happening SHOULD be documented in detail. It SHOULD also be ensured that the dynamic table name is restricted to a controllable list of values.

APP.4.6.A14 Avoiding Native SQL Statements (S)

The ABAP Database Connectivity (ADBC) interface SHOULD NOT be used. User input SHOULD NOT be part of ADBC commands.

APP.4.6.A15 Avoiding Data Leaks (S)

A sufficiently secure authorisation check SHOULD be performed before business-critical data is displayed, transmitted, or exported. Planned (intended) export options SHOULD be documented.

APP.4.6.A16 No System-Dependent Execution of Functions (S)

ABAP programs SHOULD NOT be programmed in a system-dependent manner—that is, so that they can only be executed on a particular SAP system. Should this be absolutely necessary, however, it SHOULD be documented in detail. In addition, the code SHOULD then be checked manually.

APP.4.6.A17 No Client-Dependent Execution of Functions (S)

ABAP programs SHOULD NOT be programmed in a client-dependent manner—that is, so that they can only be executed by a particular client. Should this be absolutely necessary, however, it SHOULD be documented in detail. In addition, further security measures SHOULD then be taken, such as a manual code review or quality assurance on the corresponding client.

APP.4.6.A18 Avoiding Open SQL Injection Vulnerabilities (S)

Dynamic Open SQL SHOULD NOT be used. If database access with dynamic SQL conditions is necessary, user input SHOULD NOT be transferred in the respective query. If this is nevertheless the case, the user input MUST be checked (output encoding).

APP.4.6.A19 Protection Against Cross-Site Scripting (S)

Custom-developed HTML in Business Server Page (*BSP*) applications or HTTP handlers SHOULD be avoided whenever possible.

APP.4.6.A20 No Access to Data from Another Client (S)

Automatic client separation SHOULD NOT be bypassed. Data from other clients SHOULD NOT be accessed using *EXEC SQL* or the Open SQL option *CLIENT SPECIFIED*.

APP.4.6.A21 Ban on Hidden ABAP Source Code (S)

The source code of an ABAP program created in-house SHOULD always be readable. Techniques that prevent this (obfuscation) SHOULD NOT be used.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.4.6 *SAP ABAP Programming* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.4.6.A22 Use of ABAP Code Analysis Tools (H)

An ABAP code analysis tool SHOULD be used to automatically check ABAP code for security-relevant programming errors, functional and technical errors, and quality vulnerabilities.

4. Additional Information

4.1. Useful Resources

The “Best Practice Guidelines for Development – Useful Tips for ABAP Development” published by the German-speaking SAP User Group (DSAG) contains more detailed information on ABAP programming.

Further information and best practices on secure ABAP programming is available in *Sichere ABAP-Programmierung* [Secure ABAP Programming] by Wiegenstein, Schumacher, Schinzel, and Weidemann, which is published by SAP Press.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.4.6 *SAP ABAP Programming*.

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.28 Software Vulnerabilities or Errors

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.5.2 Microsoft Exchange and Outlook

1. Description

1.1. Introduction

Microsoft Exchange Server (hereinafter “Exchange”) is a groupware solution for medium-sized to large organisations. It can be used to electronically transmit messages and is equipped with additional services for supporting workflows. Exchange can be used to centrally manage, deliver, filter, and send messages such as e-mails. It also provides and manages typical groupware applications such as notes, contact lists, calendars, and task lists. In addition to the server service itself, client software or a web browser is necessary in order to use the functions of Exchange.

Microsoft Outlook (hereinafter “Outlook”) is a client for Exchange that is made directly available by installing the Office package from Microsoft or by integrating it into the operating systems of mobile devices. Furthermore, the “Outlook on the web” application (previously the “Outlook Web App”) makes it possible to access e-mails, contacts, the calendar, and more via a browser. This function is already included in Exchange.

The combination of Exchange servers and Outlook clients is referred to in this module as the Exchange system.

1.2. Objective

The objective of this module is to provide information on typical threats to Exchange and Outlook and show how Exchange and Outlook can be used securely in organisations.

1.3. Scoping and Modelling

The module must be applied for all Exchange systems in the information domain under consideration.

General requirements for the security of e-mail systems are included in module APP.5.3 *General E-Mail Clients and Servers*. This module must also be applied to any e-mail system based on Exchange or Outlook.

It includes specific threats and requirements regarding Exchange systems. Specific requirements for server platforms and operating systems are not part of this module. These can be found in the modules SYS.1.1 *General Server* and SYS.2.1 *General Client*, as well as in the respective operating-system-specific modules.

2. Threat Landscape

For module APP.5.2 *Microsoft Exchange and Outlook*, the following specific threats and vulnerabilities are of particular importance.

2.1. Insufficient Rules for Exchange and Outlook

Comprehensive rules and specifications for Exchange and Outlook are necessary in order to ensure the security of the information they are used to process. For example, data may be lost, changed, or deleted accidentally if Exchange is incorporated into Active Directory in an incorrect and uncontrolled manner. The situation is similar if mailbox databases are depublished in an unregulated manner and Exchange is not sufficiently considered in the security policy. The same holds true when the Outlook clients can access the Exchange servers without any controls.

2.2. Incorrect Migration of Exchange

In practice, Exchange systems are more frequently migrated than installed anew. In order to migrate to a new version of Exchange Server, it is sometimes necessary to update the operating system to a later version. New versions of operating systems often include requirements regarding the existing domain concept and the existing directory services.

If a migration is not planned and performed carefully, internal communications using Exchange may be disrupted dramatically within the organisation in question, which could subsequently reduce productivity. During migration, configuration problems may occur for reasons such as changes in the configuration settings for the different versions at hand or the options for connecting to directory services. Furthermore, incorrect protocol settings may cause abnormalities related to information transfer, authentication, or encryption.

2.3. Inadmissible Browser Access to Exchange

Exchange allows users to access their own e-mail accounts via a browser. This involves the use of the Internet Information Services (IIS), which are an integral part of the Windows operating system. If this functionality is planned poorly and configured improperly, it may allow uncontrolled access to the internal network from the outside.

If e-mails are accessed via the Internet with a browser, this poses very significant risks. Despite not having direct access to an organisation’s network, attackers may access e-mails and

thereby gain access to e-mail addresses and content, misuse e-mail features, send spam e-mails, or gain access to the organisation's internal information.

2.4. Unauthorised Connection of Other Systems to Exchange

Exchange systems are tightly intertwined with the Windows operating system and only cooperate with third-party systems using connectors that enable other systems to retrieve e-mails from Exchange servers using certain protocols (e.g. POP3).

If the connectors are not taken into consideration in the installation or migration of Exchange, they may be incompatible with the migrated version of Exchange. As a consequence, e-mails may be lost or accidentally changed.

Outside the homogeneous Microsoft environment, security settings related to the Exchange system are invalid.

If different sub-systems are administered separately, inconsistencies may occur at any time. Improperly connected third-party systems may also cause data to be lost or the system to be blocked.

2.5. Improper Administration of Site and Data Access Rights in Exchange and Outlook

Vulnerabilities may arise if access rights to an Outlook client or data stored within Exchange and Outlook are not created and administered properly. This can occur, for example, if rights exceeding those actually necessary are assigned, enabling unauthorised persons to access confidential information.

2.6. Incorrect Configuration of Exchange

Successful attacks on services such as Exchange are frequently made possible by incorrectly configured systems. Since an Exchange system is very complex, diverse configuration settings and interdependent parameters may cause numerous security issues. Possible incorrect configurations range from the installation and operation of the Exchange components on inappropriate systems, the absence of encryptions, and insufficient access restrictions on Exchange servers to the incorrect assignment of rights when creating or initialising an Exchange database.

2.7. Improper Configuration of Outlook

The e-mail client Outlook is an important part of the Exchange system. For the overall security of the system, it is important that Outlook clients be properly configured. The communication protocol selected may already entail specific security issues. Private keys that are used to encrypt and sign e-mails may also be compromised. If network-level encryption is used (based on IPSec or TLS, for example), the encryption mechanism may become ineffective due to an incorrectly configured client. Incorrect configurations may cause security issues such as a loss of confidentiality due to unauthorised access.

2.8. Malfunction and Misuse of In-House Macros and Programming Interfaces in Outlook

Many software manufacturers equip their tools and applications with application programming interfaces (APIs). These make it possible to use certain functions of other programs or extend an application's own range of functions. Functions like these can be misused in Outlook to spread malware. The malware variants include malicious tools and macros that directly exploit Outlook and its related e-mail features in order to obtain, change, or delete information. Macros can also be used to forward or relocate messages, dates, or tasks. Errors in macros may constitute an increased risk in this regard. Index errors in macros may produce incorrect results that cause an organisation to take poor business decisions. The specific consequences may include unnecessary costs or automated data leaks.

3. Requirements

The specific requirements of module APP.5.2 *Microsoft Exchange and Outlook* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module APP.5.2 *Microsoft Exchange and Outlook*, the following requirements MUST be met as a matter of priority:

APP.5.2.A1 Planning the Use of Exchange and Outlook (B)

Before implementing Exchange and Outlook, an organisation MUST plan their use carefully. It MUST consider at least the following points:

- design of the e-mail infrastructure
- clients and/or server systems to be connected
- use of functional extensions
- the protocols to be used

APP.5.2.A2 Selecting an Exchange Infrastructure (B)

Based on the planning of the deployment of Exchange, the IT Operation Department MUST decide on the systems, application components, and hierarchical gradation with which the

Exchange infrastructure will be realised. When selecting an infrastructure, it MUST also be decided whether the systems are to be operated in the cloud or as a local service.

APP.5.2.A3 Access Management and Access Rights (B)

In addition to its general access control policy, an organisation MUST create, adequately document, and apply an access control policy for the systems in its Exchange infrastructure.

The IT Operation Department MUST use server-side user profiles for computer-independent user access to Exchange data. It MUST adapt the default NTFS authorisations for the Exchange directory so that only authorised administrators and system accounts are allowed to access the data in this directory.

APP.5.2.A4 ELIMINATED (B)

This requirement has been eliminated.

APP.5.2.A5 Backing Up Exchange (B)

Exchange servers MUST be backed up prior to any installations and configuration changes, as well as at cyclical intervals. In particular, the Exchange server databases MUST be backed up.

Deleted Exchange objects SHOULD only be removed from the database after some time.

3.2. Standard Requirements

For module APP.5.2 *Microsoft Exchange and Outlook*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.5.2.A6 ELIMINATED (S)

This requirement has been eliminated.

APP.5.2.A7 Migration of Exchange Systems (S)

The IT Operation Department SHOULD thoroughly plan and document all migration steps. The IT Operation Department SHOULD consider mailboxes, objects, security policies, Active Directory concepts, and connections to other e-mail systems. It SHOULD also take into account the functional differences between different versions of Exchange. The new system SHOULD be tested in a separate testing network prior to being installed.

APP.5.2.A8 ELIMINATED (S)

This requirement has been eliminated.

APP.5.2.A9 Secure Configuration of Exchange Servers (S)

The IT Operation Department SHOULD install and configure Exchange servers as specified in the respective organisation's security policy. Connectors SHOULD be configured securely. The IT Operation Department SHOULD enable logging of the Exchange system. A corresponding concept SHOULD be created for existing user-specific customisations.

When using functional extensions, it SHOULD be ensured that the requirements defined to maintain confidentiality, integrity, and availability are still being met.

APP.5.2.A10 Secure Configuration of Outlook (S)

The IT Operation Department SHOULD create a separate Outlook profile with user-specific settings for each user.

The IT Operation Department SHOULD configure Outlook so that only necessary information is transmitted to other users. The IT Operation Department SHOULD inform users regarding information that is automatically transmitted to other users. Read receipts and information that offers insights into the internal structure of the organisation at hand SHOULD NOT be transmitted to external users.

APP.5.2.A11 Protection of Communications Between Exchange Systems (S)

The IT Operation Department SHOULD decide on the protection mechanisms that are to be used to secure communications between Exchange systems in a comprehensible way. In particular, the IT Operation Department SHOULD determine how communication to the following interfaces is secured:

- administration interfaces
- client-server communications
- existing interfaces for web-based distributed authoring and versioning (WebDAV)
- server-to-server communication
- public key infrastructure on which Outlook's e-mail encryption is based

APP.5.2.A12 Using Outlook Anywhere, MAPI over HTTP, and Outlook on the Web (S)

The IT Operation Department SHOULD configure Outlook Anywhere, MAPI over HTTP, and Outlook on the Web in line with its organisation’s security requirements. Access to Exchange through the Internet SHOULD be restricted to the necessary users.

APP.5.2.A13 ELIMINATED (S)

This requirement has been eliminated.

APP.5.2.A14 ELIMINATED (S)

This requirement has been eliminated.

APP.5.2.A15 ELIMINATED (S)

This requirement has been eliminated.

APP.5.2.A16 ELIMINATED (S)

This requirement has been eliminated.

APP.5.2.A19 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.5.2 *Microsoft Exchange and Outlook* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.5.2.A17 Encryption of Exchange Database Files (H)

The IT Operation Department SHOULD create a concept for encrypting PST and Information Store files. The organisation in question SHOULD inform users about the protection mechanisms used to encrypt PST files and how these mechanisms work. Additional aspects of local PST files that SHOULD be taken into consideration when encrypting Exchange system databases include:

- proprietary encryption functions
- degrees of encryption
- mechanisms for securing the data in a PST file

mechanisms such as the Encrypting File System or Windows BitLocker drive encryption SHOULD be used to secure PST files.

APP.5.2.A18 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

Microsoft provides comprehensive information on the administration of Microsoft Exchange on the website “Microsoft Technet” (https://technet.microsoft.com/de-de).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.5.2 *Microsoft Exchange and Outlook*.

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.36 Identity Theft

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.5.3 General E-Mail Clients and Servers

1. Description

1.1. Introduction

E-mail is one of the oldest and commonly used Internet applications. E-mails are used to send text and attached files to other people. Users require an e-mail address for this purpose.

E-mail applications require e-mail servers that can send and receive electronic messages. As a rule, e-mail clients retrieve messages intended for them from an e-mail server using the POP3 or IMAP protocols and send messages to the e-mail server using the SMTP protocol, which forwards them to another e-mail server if necessary.

Since e-mail is widely used, especially at companies and public authorities, e-mail servers are often targeted by attackers.

E-mail clients are often also a focus of attack: sending malware via e-mail is a common strategy. In addition, e-mails are often used as a tool for social engineering attacks.

For these reasons, the secure operation and use of e-mail applications is of particular importance.

1.2. Objective

The objective of this module is to protect information that is processed with e-mail clients or on e-mail servers.

1.3. Scoping and Modelling

Module APP.5.3 *General E-Mail Clients and Servers* must be applied to each e-mail client and server in the information domain under consideration.

The module includes requirements for general e-mail servers and clients. Requirements for server platforms, operating systems, and clients are not covered. These can be found in the

modules SYS.1.1 *General Server* and SYS.2.1 *General Client*, as well as in the respective operating-system-specific modules.

Within the context of an information domain, module APP.5.3 *General E-Mail Clients and Servers* is mostly used in combination with another specific module of layer APP.5 *E-Mail/Groupware/Communication*. These must also be implemented separately. Among others, these modules include APP.5.2 *Microsoft Exchange and Outlook*.

Requirements for logging and backup are included in the modules OPS.1.1.5 *Logging* and CON.3 *Backup Concept*.

Groupware functions that offer features such as the administration of contact details and calendars in addition to e-mail are not covered in this module. Pure cloud solutions such as those that are part of Microsoft 365 or Google's G Suite are also not included. General requirements for this are included in module OPS.2.2 *Cloud Usage*.

2. Threat Landscape

For module APP.5.3 *General E-Mail Clients and Servers*, the following specific threats and vulnerabilities are of particular importance.

2.1. Insufficient Planning of E-Mail Use

E-mail cannot be used securely without appropriately documented rules and a defined security process within the organisation in question. If procedural, organisational, and technical rules are neglected in the planning of e-mail systems, this could result in incorrect settings and both internal and external attacks.

For example, an insufficiently sized e-mail server can fail due to a large number of incoming e-mails. If sufficient security safeguards are not planned, e-mail clients will also be more susceptible to e-mails containing malware.

2.2. Incorrect Configuration of E-Mail Clients and Servers

Since e-mail infrastructures can be highly complex, the many possible settings and interdependent parameters involved may cause numerous security issues.

For example, an e-mail server may reject legitimate e-mails from other servers due to a faulty configuration. Essential settings (e.g. transport encryption of e-mails) can also be ignored or disregarded.

Furthermore, incorrect configurations in e-mail clients can lead to them executing malicious code in e-mails. These vulnerabilities can significantly impact the availability, integrity, and confidentiality of information.

Many organisations fail to use security mechanisms that enable e-mail servers in other organisations to check whether an e-mail is actually from the specified sender. An incorrectly set e-mail server can also be misused by attackers to send spam e-mails.

2.3. E-mail Unreliability

E-mail is a quick and convenient way to exchange data, but it is not always reliable. Messages can be lost due to faulty e-mail servers or disrupted transmission paths, for example. The causes for this can include spam filters that filter out and discard legitimate messages. E-mails can also be lost when the recipient's address is not correctly entered. In the worst case, confidential information may be sent to the wrong recipients.

2.4. Malware in E-Mails

There are several ways in which attackers can spread malware using e-mails. Malicious code can be contained directly in an e-mail, for example. If an e-mail client is not configured correctly, it may execute the code when the e-mail is opened.

Files containing malware can also be sent as attachments to e-mails. If such e-mails are not sorted out by spam or virus filters and users open the attachments, the malware is executed. This can lead to extensive damage to other IT systems, as well—for example, if ransomware (also known as extortion trojans) is executed.

2.5. Social engineering

E-mails are often used by attackers to obtain confidential information or to trick users into other harmful behaviour. For example, an attacker may send an e-mail purporting to be from a manager that instructs the recipient to carry out actions that will harm the corresponding organisation (known as CEO fraud). This often involves instructions to transfer money to accounts abroad.

A fake e-mail from a real and trustworthy provider may also request that access data be entered on a website (phishing). The access data thus obtained can then be used by the attacker to take further action.

The danger of social engineering increases if users are not regularly trained and made aware of these threats.

2.6. Reading and Manipulating E-Mails

E-mails are usually sent unencrypted and without a signature, which allows attackers to read and even change them at will. They can then disclose confidential information or distribute false information. Attackers can also install malware this way.

3. Requirements

The specific requirements of module APP.5.3 *General E-Mail Clients and Servers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles

with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	User, Supervisor

3.1. Basic Requirements

For module APP.5.3 *General E-Mail Clients and Servers*, the following requirements MUST be met as a matter of priority:

APP.5.3.A1 Secure Configuration of E-Mail Clients (B)

An organisation MUST specify a secure configuration for its e-mail clients. The e-mail clients MUST be pre-configured when they are handed over to the users.

The organisation MUST ensure that the security-relevant aspects of the configuration cannot be changed by users. If this is not possible, the organisation MUST inform the users that they are not permitted to change the configuration on their own.

Before file attachments from e-mails are opened, they MUST be checked for malware by a protection program on the client, if this is not already done on the e-mail server. E-mail clients MUST be configured in such a way that they do not automatically interpret any HTML code or other active content in e-mails. Preview functions for file attachments MUST be configured so that they do not automatically interpret files. E-mail filtering rules and uncontrolled automatic forwarding of e-mails MUST be limited to necessary application scenarios.

E-mail clients MUST use secure transport encryption for communications with e-mail servers across untrusted networks.

APP.5.3.A2 Secure Operation of E-Mail Servers (B)

The IT Operation Department MUST implement protection mechanisms against denial-of-service (DoS) attacks. E-mail servers MUST offer secure transport encryption for receiving e-mails and accessing e-mail clients via public data networks. If e-mail servers send e-mails on their own, they SHOULD also use secure transport encryption for this purpose.

An organisation MUST specify all the e-mail protocols and services it permits. In addition, the IT Operation Department MUST configure e-mail servers so that they cannot be misused as spam relays.

If messages are stored on an e-mail server, the IT Operation Department MUST configure and document an appropriate size limit for the server-side mailbox.

APP.5.3.A3 Data Backup and Archiving of E-Mails (B)

The IT Operation Department MUST back up its e-mail servers regularly. To this end, the corresponding organisation MUST regulate how the sent and received e-mails of e-mail clients and the e-mails on the servers are backed up. With regard to archiving, the organisation SHOULD also consider that e-mails may only be stored locally on clients.

APP.5.3.A4 Spam and Virus Protection on E-Mail Servers (B)

The IT Operation Department MUST ensure that incoming and outgoing e-mails on e-mail servers, and particularly their attachments, are checked for spam characteristics and harmful content. The introduction and use of e-mail filtering programs MUST be coordinated with the Data Protection Officer, Employee Representatives, and Users.

The organisation MUST specify how encrypted e-mails are to be dealt with if they cannot be decrypted by the virus protection program in use.

3.2. Standard Requirements

For module APP.5.3 *General E-Mail Clients and Servers*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.5.3.A5 Establishing Deputising Rules for E-Mail Use [Supervisor] (S)

An organisation should establish deputising rules for the handling of e-mails. If e-mails are forwarded, the deputising users SHOULD at least be informed. Data protection aspects MUST be taken into account when forwarding e-mails. An organisation SHOULD establish regulations for autoreply functions in e-mail programs that describe how these functions can be used securely. When employees use the autoreply functions, no internal information SHOULD be forwarded.

APP.5.3.A6 Defining a Security Policy for E-Mail (S)

An organisation SHOULD establish and regularly update a security policy for the use of e-mail. The organisation SHOULD inform all users and administrators of new or changed security requirements for e-mail applications. The organisation's e-mail security policy SHOULD comply with its generally applicable security policies. The organisation SHOULD check that the security policy is being applied correctly.

The e-mail security policy for users SHOULD specify the following:

- how these communications can be secured
- what user access rights exist
- how e-mails are checked for forged senders
- how to secure transmitted information
- how to check the integrity of e-mails
- which open e-mail distribution lists may be used
- whether private e-mail use is permitted
- how to deal with e-mails and mailboxes of employees who leave the company
- whether and how webmail services may be used
- who is responsible for group mailboxes
- how file attachments should be handled
- how e-mails in HTML format should be handled by users

The e-mail security policy SHOULD also include the configuration options of the e-mail applications for administrators, as well as the specifications for possible access to an e-mail server from other servers. Information on authorised points from which an e-mail server may be accessed SHOULD also be included in the policy.

The e-mail security policy SHOULD regulate the handling of newsgroups and mailing lists.

APP.5.3.A7 User Training on the Security Mechanisms of E-Mail Clients (S)

An organisation SHOULD educate users on the risks of using e-mail applications and how to use e-mail safely. This SHOULD take place in addition to general training and awareness raising.

The organisation SHOULD make users aware of the possible dangers of opening e-mail attachments. Training SHOULD also address how users can recognise e-mails from fake senders.

The organisation SHOULD warn users not to participate in e-mail chain letters or subscribe to a large number of mailing lists.

APP.5.3.A8 Training Users to Deal with Spam [User] (S)

As a matter of principle, all users SHOULD ignore and delete all spam e-mails. Users SHOULD NOT answer unsolicited e-mails. They SHOULD NOT click links in these e-mails. If an organisation has a central spam management solution, users SHOULD forward spam e-mails to it and then delete them.

APP.5.3.A9 Extended Security Safeguards on E-Mail Servers (S)

An organisation's e-mail servers SHOULD check incoming e-mails using the Sender Policy Framework (SPF) and DomainKeys. The organisation SHOULD use DomainKeys and the SPF to authenticate e-mails it sends.

If SPF is used, it SHOULD be clearly specified how e-mails are to be handled. The softfail parameter ("~") SHOULD only be used for testing purposes.

The organisation SHOULD use Domain-based Message Authentication, Reporting and Conformance (DMARC) to specify how the e-mails it sends should be verified by the receiving e-mail server. DMARC reports SHOULD be evaluated regularly. The organisation SHOULD determine whether DMARC reports on received e-mails are sent to other organisations.

The organisation SHOULD secure its e-mail communications via DANE and MTA-STS.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.5.3 *General E-Mail Clients and Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.5.3.A10 End-to-End Encryption (H)

An organisation SHOULD use end-to-end encryption and signatures for e-mails. Only protocols that comply with the current state of the art SHOULD be used for encryption and signatures.

APP.5.3.A11 Deployment of Redundant E-Mail Servers (H)

An organisation SHOULD operate several redundant e-mail servers. The redundant e-mail servers SHOULD be stored with appropriate priority in the DNS information of the domains concerned. The organisation SHOULD determine how e-mails are to be synchronised among its e-mail servers.

APP.5.3.A12 Monitoring Public Blacklists (H)

The IT Operation Department SHOULD regularly check if its organisation's e-mail servers are listed on public spam or blacklists.

APP.5.3.A13 TLS Reporting (H)

An organisation SHOULD use TLS reporting. It SHOULD be determined whether TLS reports are to be sent to other organisations.

4. Additional Information

4.1. Useful Resources

In the ISO/IEC 27001:2013 standard, the International Organization for Standardization (ISO) specifies requirements for the operation of e-mail services in section 13.2.3.

Section CF2.3.3 of “The Standard of Good Practice for Information Security” published by the Information Security Forum (ISF) provides guidelines for operating e-mail services.

In its “Guidelines on Electronic Mail Security”, the National Institute of Standards and Technology (NIST) describes how e-mail applications can be run securely.

In “BSI TR-03108 Secure E-Mail Transport”, the Federal Office for Information Security (BSI) provides information on sending e-mails securely.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security

objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.5.3 *General E-Mail Clients and Servers*.

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.33 Shortage of Personnel

G 0.36 Identity Theft

G 0.39 Malware

G 0.40 Denial of Service

G 0.42 Social Engineering

G 0.45 Data Loss

G 0.25 Failure of Devices or Systems

APP.6 General Software

1. Description

1.1. Introduction

In this module, the term "general software" includes all software regardless of whether it relates to word processing, an operating system, a mobile communication app, custom-developed software, or a distributed content management system.

As a rule, all software has a lifecycle that includes planning, requirements analysis, procurement, testing (including release), installation in a production environment, training, operation, updates and change management, and decommissioning (including uninstallation). This lifecycle can vary depending on the application context at hand. As a result, specific applications can involve further individual steps, and the scope of these steps can also vary.

In the intermediate steps covered herein, however, there are recurring aspects of information security that can be applied to any type of software.

1.2. Objective

This module illustrates the security requirements that must be met to ensure that general software can be used securely throughout its lifecycle. The primary objective is to protect software and the information it processes.

1.3. Scoping and Modelling

Module APP.6 *General Software* must be applied to all software used in the information domain under consideration. This does not include operating systems that run on closed systems such as IoT devices, routers, printers, or embedded systems. Software is often delivered in a bundled manner (e.g. in office suites or operating systems with extensively integrated tools) or extended by things like plug-ins or add-ons. In such cases, this module can be applied once to the entire software bundle in question.

This module only deals with standardised and generic procedures in the lifecycle of software. No specific recommendations are given on the detailed configuration of software or securing

it by means of individual protection mechanisms on the IT systems used. The specific modules in the APP layer should be used for these purposes.

The intermediate steps of release (including software tests) and patch and change management are also not covered in this module. They are dealt with in OPS.1.1.6 *Software Tests and Approvals* and OPS.1.1.3 *Patch and Change Management*.

If certain requirements cannot be met by a finished, ready-to-use software product (e.g. by adapting its configuration) and a custom-developed product is needed, this module should be supplemented by APP.7 *Development of Individual Software*.

Software and the data associated with it often need to be available in emergencies. Initial considerations in this regard are covered in module DER.4 *Business Continuity Management*.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module APP.6 *General Software*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inappropriate Selection of Software

A wide variety of software solutions are available on the market for numerous purposes and uses. Operations can be significantly disrupted if unsuitable software is selected that fails to meet an organisation's requirements. For example, file formats can be incompatible with programs already in use or new products may lack the required functional scope. This may result in declining performance, malfunctions, or errors within business processes.

In particular, if the software does not meet the organisation's security requirements, data processed with the software could be disclosed or manipulated (e.g. if the login functions of applications have not been designed for the planned operational environment in an open data network).

2.2. Disclosure of Sensitive Information Due to Incorrect Configuration

Software that is incorrectly configured can lead to the exposure of sensitive information. For example, unnecessary functions may still be enabled, such as backup functions that inadvertently synchronise data to a cloud. This could result in sensitive data being viewed and disclosed by unauthorised third parties.

The possible consequences include financial losses and damage to an organisation's reputation. In addition, the organisation could find itself in violation of applicable laws (e.g. by disclosing personal data).

2.3. Purchasing Software from Unreliable Sources

If software is procured from an unreliable source, there is no guarantee that it will be an unmodified original version of the software. Instead, a defective or compromised version of the software may have been obtained. This also applies to extensions such as plug-ins or add-ons. The installation of compromised software can lead to the distribution of malware within an organisation. There is also the possibility that the software will not function as intended. Moreover, the integrity and availability of IT systems can be impaired.

2.4. Security Vulnerabilities Due to Inadequate Maintenance

In principle, vulnerabilities and security flaws can occur throughout the whole period of use of a given piece of software. For example, if login functions are bypassed or encryption is broken, this puts the information security of the data processed with the software at risk.

Vulnerabilities and security flaws cannot be remedied promptly in some situations, especially if no suitable maintenance contract has been concluded with the software manufacturer or provider or the software is simply used beyond the respective maintenance period. Violations of licence conditions can also lead to update mechanisms (including those that are automatic) being disabled, for example, which can result in software no longer being maintained.

2.5. Data Loss Due to Incorrect Use of Software

Incorrect use of software may result in employees inadvertently deleting or changing data and rendering it unusable. This may bring entire business processes to a halt. If encryption functions are used incorrectly, the affected data may still exist, but decrypting it may no longer be possible. Increased effort will then be required to recover the data, if it is recoverable at all.

2.6. Insufficient Resources for Running Software

If IT systems have insufficient resources to run software, this may significantly increase the processing and response times for users. In the worst case, it will not be possible to run the software on the systems in question. This can significantly disrupt business processes.

2.7. Failure to Meet User Requirements

Even if software meets the functional requirements at hand, it may be rejected by users if, for example, it is cumbersome and not user-friendly. This can lead to users resorting to alternative forms of processing and misappropriating other IT systems or software for this purpose. For example, private IT systems can be used without consultation with the IT Operation Department. These alternative forms of processing are rarely considered from an information security perspective and thus pose an increased risk.

3. Requirements

The specific requirements of module APP.6 *General Software* are listed below. The IT Operation Department is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner, Procurement Department

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

APP.6.A1 Planning Software Use [Process Owner] (B)

Before an organisation introduces (new) software, it MUST determine the following:

- What the software will be used for and what information it will process
- How users should be involved in the requirements analysis and supported in the implementation process
- How the software will be connected to other applications and IT systems, and via which interfaces
- The IT systems on which the software is to be run and what resources are required
- Whether the organisation will become dependent on a manufacturer if it uses the software in question

Security aspects MUST be considered in this process. In addition, the organisation MUST clarify and define the responsibilities for technical supervision, approval, and operational administration in advance. The responsibilities MUST be documented and updated as needed.

APP.6.A2 Drawing Up a Requirements Catalogue for Software [Process Owner] (B)

Based on the results of corresponding planning, the software requirements at hand MUST be collated in a requirements catalogue. The requirements catalogue MUST include the basic functional requirements. In addition, the non-functional requirements, and particularly the security requirements, MUST be integrated into the requirements catalogue.

In doing so, the requirements of both the Process Owners and the IT Operation Department MUST be taken into account. In particular, the legal requirements arising from the context of the data to be processed MUST also be considered.

The requirements catalogue SHOULD be finalised in consultation with all the departments involved.

APP.6.A3 Secure Procurement of Software [Procurement Department] (B)

During the procurement process, suitable software MUST be selected based on the requirements catalogue. The selected software MUST be procured from a trusted source. The trusted source SHOULD provide a means of verifying the integrity of the software.

Furthermore, the software SHOULD be procured with a suitable maintenance contract or a comparable commitment from the manufacturer or software provider. In particular, these contracts or commitments SHOULD guarantee that any vulnerabilities or security flaws that emerge in the software will be promptly remedied throughout the period of use.

APP.6.A4 Regulation of Software Installation and Configuration [Process Owner] (B)

The installation and configuration of software MUST be regulated by the IT Operation Department in order to ensure the following:

- The software is installed and executed with the smallest functional scope necessary
- The software is executed with the fewest authorisations possible
- Settings pertaining to the processing of personal data are configured to store as little data as possible
- All relevant security updates and patches are installed before the software is used productively

Dependent components (including runtime environments, libraries, interfaces, and other programs) MUST also be considered. In coordination with the Process Owner, the IT Operation Department MUST determine who is allowed to install the software and how. Ideally, software SHOULD always be installed centrally by the IT Operation Department. If it is necessary to install software (or parts thereof) manually, the IT Operation Department MUST create installation instructions that clearly regulate the intermediate steps required for installation and what configurations are to be made.

In addition, the IT Operation Department MUST define how the integrity of installation files is to be checked. If digital signatures or checksums are available for an installation package, they MUST be used to verify its integrity.

If required, the IT Operation Department SHOULD define a secure default configuration for the software in question. The default configuration SHOULD be documented.

APP.6.A5 Secure Installation of Software (B)

Software MUST be installed in line with the applicable rules on installations in IT systems. Unmodified versions of the approved software MUST be used.

If there is any deviation from these instructions, this MUST be approved by the Supervisor and IT Operation Department and documented accordingly.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

APP.6.A6 Consideration of Recommended Security Requirements (S)

An organisation SHOULD consider the following security requirements in the requirements catalogue for the software at hand:

- The software SHOULD include general security functions that are required in the application context in question, such as logging and authentication.
- The software SHOULD make it possible to use the hardening functions of the operational environment. In particular, the hardening capabilities of the intended operating system and execution environment SHOULD be considered.
- If the software transmits information over unsecured public networks, it SHOULD use secure encryption functions that reflect the current state of the art. In addition, the transmitted data SHOULD be checked for integrity using checksums or digital signatures.
- If the software uses certificates, it SHOULD offer the option to display the certificates transparently. It SHOULD also be possible to block certificates, withdraw trust from them, or add an organisation's own certificates.

The functions of the software that pertain to the security requirements at hand SHOULD be used in actual operations.

APP.6.A7 Selection and Assessment of Potential Software [Process Owner, Procurement Department] (S)

The requirements catalogue SHOULD be used to evaluate the products available on the market. These products SHOULD be compared using an assessment scale. Whether the products on the short list actually meet the requirements of the organisation in question SHOULD then be examined. If there are several product alternatives, user acceptance and the additional effort required for aspects such as training or migration SHOULD also be considered. The Process Owners SHOULD select a suitable software product together with the IT Operation Department based on the assessments and test results.

APP.6.A8 Regulation of the Availability of Installation Files (S)

The IT Operation Department SHOULD ensure the availability of installation files so that the installation process can be reproduced. In this regard, the IT Operation Department SHOULD:

- Secure the installation files appropriately
- Ensure that the installation files will continue to be available from the source in question (e.g. the corresponding app store)

In addition, it SHOULD be ensured that software can be configured in a reproducible manner. For this purpose, the configuration files SHOULD be backed up. Alternatively, there SHOULD be suitable documentation on how the software is configured.

This regulation SHOULD be integrated into the organisation's data backup concept.

APP.6.A9 Taking Inventory of Software (S)

Software SHOULD be inventoried. An inventory SHOULD document the systems on which software is used and under which licence. If necessary, the security-relevant settings SHOULD also be documented. Software SHOULD only be used with licences that correspond to the intended use and the respective contractual provisions. Each licence SHOULD cover the entire intended period of use of the corresponding software.

If there is a deviation from a default configuration, this SHOULD be documented. The inventory SHOULD be updated by the IT Operation Department as necessary, especially when software is installed.

The inventory SHOULD be structured to provide a quick overview of the necessary details in the event of a security incident.

APP.6.A10 Establishing a Security Policy for Software Use (S)

An organisation SHOULD establish a security policy that summarises the regulations that determine how software is to be used and operated. The policy SHOULD be known to all the relevant people in charge and employees of the organisation and SHOULD represent the basis for their actions and work. In terms of content, the policy SHOULD also include a manual that explains how software should be used and managed.

Employee compliance with the policy SHOULD be checked regularly and at random. The policy SHOULD be updated at regular intervals.

APP.6.A11 Using Plug-ins and Extensions (S)

Plug-ins and extensions SHOULD be restricted to those that are absolutely necessary. If extensions are used, the corresponding software SHOULD offer the option to configure and disable them.

APP.6.A12 Orderly Decommissioning of Software [Process Owner] (S)

If software is to be decommissioned, the IT Operation Department SHOULD regulate this procedure with the Process Owners. The process for informing users in this regard SHOULD also be regulated. In the process, the matter of whether the functional requirements in question still apply (e.g. for business processes) SHOULD be clarified. If they do, the manner in which the required functions of the software to be decommissioned will continue to be available SHOULD be regulated.

APP.6.A13 Uninstallation of Software (S)

If software is uninstalled, all files created and no longer needed SHOULD be removed. All entries in system files that were made for the software and are no longer needed SHOULD be reversed.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

APP.6.A14 Using Certified Software (H)

When purchasing software, it SHOULD be determined whether the assurances of the manufacturer, distributor, and provider regarding the security functions implemented can be considered to be sufficiently trustworthy. If this is not the case, certification of the application (e.g. according to Common Criteria) SHOULD be factored into the selection process. If several products are available, security certificates SHOULD be considered, particularly if the evaluated scope of functions includes the minimum functions (or most of them) and the strength of the corresponding mechanisms matches the protection needs at hand.

4. Additional Information

4.1. Useful Resources

In the ISO/IEC 27001:2013 standard (annex A.14, “Security Requirements of Information Systems”), the International Organization for Standardization (ISO) specifies requirements for the information security of IT systems that should also be taken into account when selecting and using software.

The Common Criteria for Information Technology Security Evaluation (CC) form the basis for internationally recognised product certifications. CC certification can therefore be used as evidence of a software product's information security.

The National Institute of Standardisation and Technology formulates requirements for the acquisition of IT products, including software, in NIST Special Publication 800-53 (appendix F, “Family System and Service Acquisition”).

In “The Standard of Good Practice for Information Security”, the Information Security Forum (ISF) presents best practices for securing software in the section “Business Application Management”.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module APP.6 *General Software*.

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

APP.7 Development of Individual Software

1. Description

1.1. Introduction

Many organisations faced challenges that they can no longer adequately solve with unadapted software. The tasks associated with these challenges often require software solutions that are tailored to an organisation's individual needs. In this module, these software solutions are referred to as individual software. One variant involves implementing basic solutions that comprise a set of typical functions and then customising them. The basic functions are adapted to an organisation's specific purposes and supplemented by individually required functions. Common examples of this involve IT applications such as enterprise resource planning (ERP) systems, content management systems (CMS), or identity management (IDM) systems. Individual software can also be developed entirely from scratch by an organisation or third parties. This includes applications for business process control or individually adapted specialised applications, such as personnel management software or procedures for managing social data or registration data.

It is essential that the required security functions be considered during the planning and design of individual software and that information security be taken into account throughout the entire lifecycle. It can take a great deal of additional effort (or be impossible) to compensate for planning errors or missing security functions during live operations.

Individual software is usually developed as part of a project. A wide variety of process and project management models have been established for this purpose. While classic, linear process models such as the waterfall process are very well suited to projects with fixed requirements at the beginning, agile procedure models such as Scrum enable individual software to be developed iteratively and incrementally. Agile procedure models can thus adapt better to changing circumstances, especially if not all requirements are fixed at the beginning. However, they do not offer the same costing certainty as linear procedure models and in some cases do not fit the classic structures of procurement processes, which are geared towards a linear approach.

1.2. Objective

The aim of this module is to cover the basic security requirements to be considered when planning and developing individual software.

1.3. Scoping and Modelling

Module APP.7 *Development of Individual Software* must be applied once to each development of individual software.

Aspects of planning, designing, and using individual software, such as defining required security functions or decommissioning such software, are covered in APP.6 *General Software*. It should therefore always be used in conjunction with this module.

Software development very often involves a client-contractor relationship. This situation is reflected in IT-Grundschutz in that the APP.7 *Development of Individual Software* module deals with the client side, while CON.8 *Software Development* module covers the contractor side.

The release and testing of individual software are covered in module OPS.1.1.6 *Software Tests and Approvals*.

2. Threat Landscape

For module APP.7 *Development of Individual Software*, the following specific threats and vulnerabilities are of particular importance.

2.1. Unsatisfactory Contractual Arrangements with External Service Providers

Unsatisfactory contractual arrangements with outsourcing service providers may result in a variety of severe security issues. This applies in particular to creating, implementing, and maintaining applications. If tasks, performance parameters, or the effort involved are insufficiently or misleadingly described, security safeguards may not be implemented due to ignorance or a lack of qualifications or resources. This can lead to multiple negative consequences—for example, if regulatory requirements and duties are not fulfilled, laws or obligations to provide information are not complied with, or no responsibility is taken because of missing monitoring and control options.

2.2. Software Design Errors

Security-relevant errors can occur in the design of applications, programs, and protocols. These often result from the fact that application modules and protocols intended for a specific purpose are reused in other deployment scenarios. If other security requirements are then relevant, this can lead to massive security problems—for example, if application modules and protocols that are actually intended for compartmentalised operational environments are connected to the Internet.

2.3. Undocumented Functions

Many applications contain undocumented functions built in by the manufacturer, often for the development or support of the application. Users are not usually aware of them. Undocumented functions are problematic if they make it possible to bypass essential security mechanisms (e.g. for access protection). This may impair the confidentiality, integrity, and availability of processed data.

2.4. Insufficient Security Safeguards in Applications

Security mechanisms or security functions in an application should ensure that confidentiality, integrity, and availability can be guaranteed to the required extent when processing information. When developing an application, however, the focus is often on technical functionality or time and cost considerations. This means that important security mechanisms may be missing or too weak, allowing them to be bypassed easily.

2.5. Inadequate Control of Software Development

If the software development process is not sufficiently controlled by the client, there are a number of dangers, such as:

- Required security functions that are missing or only insufficiently implemented. This can result in a variety of risks that jeopardise the availability, confidentiality, and integrity of the data processed with the customised software.
- The development project may be delayed so that the individual software is not available in time.
- Priorities can be set incorrectly; for example, less critical functions can be developed extensively while urgently needed security functions are only implemented in a rudimentary way. This can also lead to project delays and a variety of security risks.

2.6. Hiring Unsuitable Software Developers

Commissioning unsuitable software developers can lead to a variety of risks:

- A lack of technical expertise (e.g. in the programming language, frameworks, or planned technical operational environment) can lead to many avoidable software vulnerabilities.
- A lack of knowledge of project management and requirements engineering can lead to friction in coordination processes, and thus to considerable delays. This can also lead to focus in the wrong areas and essential security functions not being implemented with the required priority. Unsuitable software developers can be commissioned due to overly tight and unrealistic cost calculations, for example. Errors, misleading requirements, and incorrect objectives in tenders can also lead to this.

3. Requirements

The specific requirements of module APP.7 *Development of Individual Software* are listed below. As a matter of principle, the Process Owner is responsible for fulfilling the

requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	Process Owner
Further responsibilities	Procurement Department, IT Operation Department

3.1. Basic Requirements

For module APP.7 *Development of Individual Software*, the following requirements MUST be met as a matter of priority:

APP.7.A1 Including Aspects of Individual Software in Software Deployment Planning (B)

The planning of software deployment MUST be extended to include aspects of individual software by defining the following:

- Who is responsible for managing and coordinating the software development or the contractor
- The organisational framework in which the software is to be developed (project management model)

Individual software SHOULD be developed within the framework of a development project. A schedule SHOULD be drawn up to plan the approximate timing of the development project.

APP.7.A2 Defining Security Requirements for the Software Development Process (B)

An organisation MUST define clear requirements for the software development process. The requirements MUST specify the environment in which software may be developed and the technical and organisational safeguards to be implemented by contracted software developers.

APP.7.A3 Specification of Security Functions for System Integration [IT Operation Department] (B)

The IT Operation Department and Process Owners MUST establish requirements for the technical operational environment of planned individual software and coordinate them with software development. The requirements MUST clearly state the use of the application in question in terms of:

- type of hardware platform
- type of software platform (including the entire software stack)
- available resources (e.g. CPU cluster or RAM)
- interfaces with other systems
- security functions resulting from the above aspects

Interfaces with other IT systems SHOULD be modelled and defined in standardised technical formats.

APP.7.A4 Commissioning in Line with Requirements [Procurement Department] (B)

If individual software is developed by an organisation or commissioned externally, the following issues in particular MUST be used as a basis for software development in addition to the existing legal and organisational requirements:

- the catalogue of requirements (see APP.6 *General Software*)
- the security requirements for the software development process
- the security functions for system integration

3.2. Standard Requirements

For module APP.7 *Development of Individual Software*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

APP.7.A5 Appropriate Control of Application Development (S)

An appropriate control and project management model SHOULD be used when developing individual software. In this regard, the selected model SHOULD be agreed with the contractor and considered in terms of controlling.

Whether the required staff are adequately qualified SHOULD be considered in particular. All the relevant phases SHOULD be covered during the lifecycle of the software. It SHOULD also include an appropriate development model, risk management, and quality objectives.

APP.7.A6 Documentation of Individual Software Requirements (S)

The requirements from the requirements catalogue, the security requirements for the software development process, and the security functions for system integration SHOULD be comprehensively documented. In particular, a security profile SHOULD be created for the application in question. This SHOULD document the protection needs of the functions and data to be processed. The documentation, including the security profile, SHOULD be made available to the software developers.

The documentation SHOULD be updated in the event of changes to the individual software or related functional updates.

APP.7.A7 Secure Acquisition of Individual Software (S)

A development project SHOULD be commissioned within the framework of the most suitable project management model. Security aspects SHOULD be taken into account during the tendering and awarding process to ensure the following:

- only suitable contractors are commissioned
- no wide-ranging conclusions about the organisation's security architecture can be drawn from publicly available information

The organisation SHOULD have defined processes and specified contact persons to ensure that the relevant framework conditions are considered.

APP.7.A8 Early Involvement of the Process Owner in Development-Related Software Tests (S)

The Process Owner SHOULD be involved in the software developers' tests early on in the development process (before final acceptance). This SHOULD be agreed in the project schedule in coordination with the contractor from the start.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.7 *Development of Individual Software* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

APP.7.A9 Trusted Storage (H)

Checks SHOULD be carried out on whether business-critical applications are protected against manufacturer outages. For this purpose, materials and information not included in the scope of delivery of the application in question SHOULD be placed in trust—for example, with an escrow agency. Documented code, design plans, keys, and passwords SHOULD be included in this. The escrow agency's obligations regarding deposit and release SHOULD be contractually regulated. It SHOULD be clarified when deposits may be released and to whom.

APP.7.A10 Commissioning Certified Software Development Companies (H)

Certified software developers SHOULD be commissioned to develop any particularly security-critical applications. Their certification SHOULD include security considerations for relevant aspects of software development.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides the following:

- An overview of all components in the software lifecycle in the norm ISO/IEC 12207:2008, "System and Software Engineering – Software Life Cycle Process"
- An overview of the options for system security in the standard ISO/IEC 15408-2:2008, "Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security Functional Components"
- Requirements for system development and operation in the standard ISO/IEC 27001:2013, "Information Technology – Security Techniques – Information Security Management Systems – Requirements" (annex A, A.14, "System Acquisition, Development and Maintenance")

In its standard "The Standard of Good Practice for Information Security", the Information Security Forum (ISF) sets requirements for the management of business applications in "Area BA Business Application Management".

In “NIST Special Publication 800-53” (appendix F-SA, “Family: System and Services Acquisition, Family: System and Communications Protection, and Family: System and Information Integrity”), the National Institute of Standards and Technology specifies further requirements for handling individual software.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module APP.7 *Development of Individual Software*.

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.45 Data Loss

SYS.1.1 General Server

1. Description

1.1. Introduction

The term “general server” refers to IT systems running any operating system that provide services to users and other IT systems. These services can be basic services for a local or external network, for example, or those that facilitate the exchange of e-mails or make databases and printer services available. Server IT systems play a key role in information technology, and thus in the well-functioning workflows of an organisation. Servers often perform tasks in the background without direct user interaction. On the other hand, some server services interact directly with users and are not perceived as a server service at first glance. The X server on Unix is a well-known example.

1.2. Objective

The objective of this module is to protect information that is processed, offered, or transmitted by servers, along with associated services.

1.3. Scoping and Modelling

SYS.1.1 *General Server* must be applied to all server IT systems running any operating system.

Server systems usually run operating systems for which specific security requirements must be taken into consideration. For widely used server operating systems, separate modules that build on this module can be found in the IT-Grundschutz Compendium. SYS.1.1 *General Server* forms the basis for the modules on specific server systems. If a specific module exists for a given system, that module must be used in addition to SYS.1.1 *General Server*. If there is no specific module for the server systems in use in a particular case, the requirements of this module must be adapted in a suitable manner.

The specific services offered by a given server are not part of this module. For these server services, other modules will need to be implemented in addition to this module. These modules should be selected based on the results of the IT-Grundschutz modelling process. If

interactive use by users is also planned for a server system (e.g. a terminal server) in a particular case, the associated security aspects must also be considered.

It is essential that the requirements for role and access control policies described in module ORP.4 *Identity and Access Management* and the requirements of module DER.4 *Business Continuity Management* also be considered.

Furthermore, servers should always be considered in malware protection concepts. Corresponding requirements can be found in module OPS.1.1.4 *Protection Against Malware*.

For servers, there are special requirements for administrators and the handling of patches and changes. Therefore, the requirements of the modules OPS.1.1.2 *Proper IT Administration* and OPS.1.1.3 *Patch and Change Management* must be observed.

Servers frequently provide services to a large number of clients, often via the Internet. For this reason, it is particularly important that they be separated from the rest of an organisation's network. Requirements for this can be found in module NET.1.1 *Network Architecture and Design*.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module SYS.1.1 *General Server*, the following specific threats and vulnerabilities are of particular importance.

2.1. Data Loss

For servers in particular, the loss of data may seriously affect business processes or specialised tasks, which can in turn impact the entire surrounding organisation. A large number of IT systems, such as clients or other servers, generally depend on the constant availability of the data stored centrally on servers.

When any type of information that is relevant to an organisation is destroyed or corrupted, this can cause delays in business processes and specialised tasks, or even prevent their execution. Overall, the loss of stored data may lead to failures and additional costs in recovering the data, and especially to long-term consequences (e.g. a loss of trust among customers and partners, legal consequences, or a negative public image). Many organisations stipulate that no data may be stored on local clients; central storage on servers must be used for this purpose instead. In such cases, a loss of this centrally stored data would have serious consequences. The direct and indirect damage caused can even threaten the existence of an organisation.

2.2. Denial-of-Service Attacks

An attack on the availability of data resources ("denial of service") aims to prevent users from using necessary and normally available functions or devices. This type of attack is often connected to the use of distributed resources, with the attacker placing such high demands on these resources that other users can no longer access them. IT systems are typically highly

interdependent, as well. This means that a shortage of resources on one server will quickly affect others. Shortages of CPU time, storage space, or bandwidth, for example, can be artificially induced. This can lead to services or resources no longer being available.

2.3. Provision of Unnecessary Operating System Components and Applications

During the installation of a server operating system, it is possible to install applications and services supplied with it, some of which may not be used at all. Software that is tested briefly, but no longer needed afterwards is often installed during later operations, as well. Employees are frequently unaware that these unused applications and services are available. As a result, numerous unused applications and services may be placing an unnecessary load on a server.

In addition, these unused applications and services may contain vulnerabilities, such as when they are no longer updated. If the applications and services installed are not known, the organisation in question will not be aware of the fact that they must also be updated. This means they can easily become a gateway for attackers.

2.4. Server Overload

If servers do not have sufficient capacity, there will come a point when they no longer meet the requirements of the respective organisation. Depending on the type of systems affected, this may have numerous adverse effects. For example, servers or services may be temporarily unavailable, or data loss may occur. In complex IT landscapes, a single overloaded server can also lead to problems or failures on other servers.

Information systems may be overloaded by the following circumstances:

- Installed services or applications being configured incorrectly and taking up excessive memory as a result
- Available disk capacity being exceeded
- Numerous simultaneous requests
- Services requiring too much computing power
- A large number of simultaneous messages

3. Requirements

The specific requirements of module SYS.1.1 *General Server* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Building Services

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

SYS.1.1.A1 Appropriate Installation (B)

Servers MUST be operated in locations that may only be accessed by authorised persons. Servers MUST therefore be set up and installed in data centres, computer rooms, or lockable server rooms (see the corresponding modules in the INF *Infrastructure* layer). Servers MUST NOT be used as personal computers. IT systems used as workstations MUST NOT be used as servers.

SYS.1.1.A2 User Authentication on Servers (B)

Authentication methods adequate for the protection needs at hand MUST be used when users and services log into servers. This SHOULD be taken into account for administrative access in particular. Central, network-based authentication services SHOULD be used whenever possible.

SYS.1.1.A3 ELIMINATED (B)

This requirement has been eliminated.

SYS.1.1.A4 ELIMINATED (B)

This requirement has been eliminated.

SYS.1.1.A5 Protection of Interfaces (B)

It MUST be ensured that only specified removable storage media and other devices can be connected to servers. All interfaces that are no longer needed must be disabled.

SYS.1.1.A6 Disabling Unnecessary Services (B)

All unnecessary services and applications—particularly network services—MUST be disabled or uninstalled. All unused functions in firmware MUST also be disabled. On servers, the disk space allotted to both individual users and applications SHOULD be restricted appropriately.

The decisions taken in this regard SHOULD be documented in a way that makes it clear which configuration and software equipment was chosen for servers.

SYS.1.1.A7 ELIMINATED (B)

This requirement has been eliminated.

SYS.1.1.A8 ELIMINATED (B)

This requirement has been eliminated.

SYS.1.1.A9 Using Anti-Virus Programs on Servers (B)

Whether virus protection programs can and should be used MUST be checked depending on the operating system installed, the services provided, and other existing protection mechanisms of the server in question. Where available, concrete statements from the relevant operating system modules of the IT-Grundschutz Compendium on whether virus protection is necessary MUST be considered.

SYS.1.1.A10 Logging (B)

In general, all security-relevant system events MUST be logged, including the following at minimum:

- System starts and reboots
- Successful and failed login attempts (operating system and application software)
- Failed authorisation checks
- Blocked data flows (violations of ACLs or firewall rules)
- Creation of or changes to users, groups, and authorisations
- Security-relevant error messages (e.g. hardware defects, exceeded capacity limits)
- Warnings from security systems (e.g. virus protection)

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

SYS.1.1.A11 Defining a Security Policy for Servers (S)

Based on the general security policy of the organisation in question, the requirements for servers SHOULD be specified in a separate security policy. This policy SHOULD be known to all administrators and other persons involved in the procurement and operation of servers and be integral to their work. The implementation of the policy's requirements SHOULD be checked at regular intervals. The results SHOULD be appropriately documented.

SYS.1.1.A12 Planning the Use of Servers (S)

Each server system SHOULD be suitably planned. In this process, the following points SHOULD be taken into account at minimum:

- Selection of the hardware platform, operating system, and application software
- Hardware capacity (performance, memory, bandwidth, etc)
- Type and number of communication interfaces
- Power consumption, thermal load, space requirements, and structural shape
- Administrative access points (see SYS.1.1.A5 *Protection of Administration Interfaces*)
- User access
- Logging (see SYS.1.1.A10 *Logging*).
- Updates for operating systems and applications

- Integration into system and network management, backups, and protection systems (virus protection, IDS, etc)

All decisions taken in the planning phase SHOULD be documented in such a way that they can be understood at any future point in time.

SYS.1.1.A13 Procurement of Servers (S)

Prior to procuring one or more servers, a requirements list SHOULD be drawn up that can be used to evaluate the products available on the market.

SYS.1.1.A14 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.1.A15 Stable and Uninterruptible Power Supply [Building Services] (S)

Every server SHOULD be connected to an uninterruptible power supply (UPS).

SYS.1.1.A16 Secure Basic Configuration of Servers (S)

The basic settings of servers SHOULD be checked and, where necessary, adapted to the specifications of the security policy at hand. Clients SHOULD only be connected to the Internet after the installation and configuration have been completed.

SYS.1.1.A17 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.1.A18 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.1.A19 Configuring Local Packet Filters (S)

Based on a set of rules, existing local packet filters SHOULD be designed to limit incoming and outgoing communications to the necessary communication partners, communication protocols, ports, and interfaces. The identity of remote systems and the integrity of corresponding connections SHOULD be protected cryptographically.

SYS.1.1.A20 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.1.A21 Operational Documentation for Servers (S)

Operational tasks that are carried out on a server SHOULD be clearly documented in terms of what has been done, when, and by whom. In particular, the documentation SHOULD make configuration changes transparent. Security-relevant responsibilities, such as who is authorised to install new hard disks, SHOULD be documented. Everything that can be documented automatically SHOULD be documented automatically. The documentation SHOULD be protected against unauthorised access and loss.

SYS.1.1.A22 Integration into Contingency Planning (S)

Servers SHOULD be taken into account in business continuity management processes. To this end, the contingency requirements for the system in question SHOULD be determined and

appropriate contingency procedures implemented—for example, by drawing up recovery plans or securely storing passwords and cryptographic keys.

SYS.1.1.A23 Monitoring Systems and Servers (S)

Server systems SHOULD be integrated into an appropriate system monitoring concept. The status and functionality of these systems and the services operated on them SHOULD be continuously monitored. Error conditions and defined thresholds that are exceeded SHOULD be reported to the operating personnel.

SYS.1.1.A24 Security Checks for Servers (S)

Servers SHOULD be subjected to regular security tests to check their compliance with the applicable security requirements and identify possible vulnerabilities. In particular, these security tests SHOULD be performed on servers with external interfaces. To prevent indirect attacks via infected systems in an organisation's own network, internal server systems SHOULD also be checked accordingly at defined intervals. Whether the security checks can be realised automatically—by means of suitable scripts, for example—SHOULD be examined.

SYS.1.1.A25 Controlled Decommissioning of a Server (S)

When decommissioning a server, it SHOULD be ensured that no important data that might still be present on the storage media is lost and no sensitive data remains. There SHOULD be an overview of the data stored in each location on the server. Furthermore, it SHOULD be ensured that services offered by the server will be taken over by another server when necessary.

A checklist SHOULD be created that is to be completed when decommissioning a server. This checklist SHOULD at least include aspects related to backing up data, migrating services, and subsequently deleting all data in a secure manner.

SYS.1.1.A35 Drawing Up and Maintaining an Operating Manual (S)

An operating manual SHOULD be drawn up. It SHOULD document all the rules, requirements, and settings that are necessary in operating servers. There SHOULD be a specific operating manual for every type of server. Each operating manual SHOULD be updated at regular intervals. Operating manuals SHOULD be protected against unauthorised access. Operating manuals SHOULD be available in emergencies.

SYS.1.1.A37 Encapsulation of Security-Critical Applications and Operating System Components (S)

In order to prevent an attacker from accessing the operating system or other applications and prevent access from the operating system to files that are particularly sensitive, applications and operating system components (such as authentication or certificate verification) SHOULD be specially encapsulated according to their protection needs or isolated from other applications and operating system components. Particular attention SHOULD be paid to security-critical applications that work with data from insecure sources (e.g. web browsers and office communication applications).

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

SYS.1.1.A26 ELIMINATED (H)

This requirement has been eliminated.

SYS.1.1.A27 Host-Based Attack Detection (H)

Host-based attack detection systems (also referred to as host-based intrusion detection systems, IDS, or intrusion prevention systems, IPS) SHOULD be used to monitor system behaviour for abnormalities and misuse. The IDS/IPS mechanisms used SHOULD be appropriately selected, configured, and thoroughly tested. If an attack has been detected, the operating personnel SHOULD be alerted in an appropriate manner.

Using operating system mechanisms or suitable additional products, changes made to system files and configuration settings SHOULD be checked, restricted, and reported.

SYS.1.1.A28 Increasing Availability Through Redundancy (H)

Server systems with high availability requirements SHOULD be protected adequately against failures. At minimum, suitable redundancies SHOULD be available and maintenance contracts concluded with the respective suppliers. Whether high-availability architectures with automatic failover (across various sites, if necessary) are required in the case of very high requirements SHOULD be checked.

SYS.1.1.A29 ELIMINATED (H)

This requirement has been eliminated.

SYS.1.1.A30 One Service per Server (H)

Depending on the threat landscape at hand and the protection needs of services, only one service SHOULD be operated on each server.

SYS.1.1.A31 Using Execution Control (H)

Execution control SHOULD be used to ensure that only explicitly authorised programs and scripts can be executed. The rules SHOULD be set as restrictively as possible. If explicit specification of paths and hashes is not possible, certificate-based or path rules SHOULD be used as an alternative.

SYS.1.1.A32 ELIMINATED (H)

This requirement has been eliminated.

SYS.1.1.A33 Active Administration of Root Certificates (H)

As part of the procurement and installation of a server, the root certificates that are required to operate the server SHOULD be documented. Only the previously documented root certificates required for operation SHOULD be present on the server. Regular checks SHOULD be

performed as to whether existing root certificates still comply with the respective organisation’s requirements. All certificate stores on the IT system at hand SHOULD be included in these checks.

SYS.1.1.A34 Hard Disk Encryption (H)

In case of increased protection needs, a server's storage media should be encrypted using a product or procedure that is considered secure. This SHOULD also apply to virtual machines containing production data. Trusted Platform Module (TPM) SHOULD NOT be the only form of key protection used. Recovery passwords SHOULD be stored in an appropriate and secure location. In case of very high requirements (e.g. regarding confidentiality), full volume or full disk encryption SHOULD be used.

SYS.1.1.A36 Protecting the Boot Process (H)

A server's boot loader and operating system kernel SHOULD be checked by self-controlled key material that is signed upon system start in a trusted chain (secure boot). Unnecessary key material SHOULD be removed.

SYS.1.1.A38 Hardening of the Host System by Means of a Read-Only File System (H)

The integrity of the host system should be ensured by a read-only file system (an immutable OS).

4. Additional Information

4.1. Useful Resources

NIST Special Publication 800-123, "Guide to General Server Security" (July 2008), is offered by the National Institute of Standards and Technology.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module SYS.1.1 *General Server*:

G 0.8 Failure or Disruption of the Power Supply

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Federal Office
for Information Security

SYS.1.2.2 Windows Server 2012

1. Description

1.1. Introduction

In Windows Server 2012, Microsoft released an operating system for servers in September 2012 that featured several improvements in security compared to previous Windows versions (particularly Windows Server 2008 R2). Rather than the code base of its predecessor, Windows Server 2021 builds on that of the Windows 8 client operating system from a technical point of view. In the Windows Server 2012 R2 release in October 2013, the operating system was updated and extended to make it the server equivalent of the client-side Windows 8.1.

This module addresses the process of securing both Windows Server 2012 and Windows Server 2012 R2. If both versions are meant, the uniform term "Windows Server 2012" is used. Differences in the R2 version are mentioned separately. The expiration dates for mainstream and extended support (“end of life”, EoL) for both operating systems are 9 January 2018 and 10 January 2023, respectively.

1.2. Objective

The objective of this module is to protect information and processes that are processed and controlled on server systems running Windows Server 2012.

1.3. Scoping and Modelling

Module SYS.1.2.2 *Windows Server 2012* must be applied to all server systems on which the Microsoft Windows Server 2012 operating system is used.

This module specifies and adds specific features of Windows Server 2012 to the aspects included in module SYS.1.1 *General Server*. Accordingly, the two modules must always be used together.

Within the framework of this module, a default integration into an Active Directory domain is assumed, as is common in organisations. The particularities of stand-alone systems are only mentioned selectively where the differences appear to be particularly relevant. Requirements related to Active Directory are covered in module APP.2.2 *Active Directory*.

The security requirements of possible server roles and functions, such as file servers (APP.3.3 *File Servers*), web servers (APP.3.2 *Web Servers*), or Microsoft Exchange and Outlook (APP.5.2 *Microsoft Exchange and Outlook*), are covered in separate modules, as is the subject of virtualisation (SYS.1.5 *Virtualisation*). This module is about using built-in resources to achieve basic security at the operating system level regardless of the server's intended purpose.

2. Threat Landscape

For module SYS.1.2.2 *Windows Server 2012*, the following specific threats and vulnerabilities are of particular importance:

2.1. Poor Planning of Windows Server 2012

Windows Server 2012 is a complex operating system with a large number of functions and configuration options. There is also a great deal of freedom regarding integration into domains and networking with other IT systems and services. Even though state-of-the-art Windows versions include good default settings in many areas, the basic configuration is not always the most secure. Without sufficient planning, this can lead to a multitude of attack vectors that can be easily exploited by unauthorised third parties. Furthermore, if central decisions are not made prior to installation, Windows Server 2012 will run in an insecure and undefined state that is difficult to remedy afterwards.

2.2. Careless Cloud usage

Windows Server 2012 offers the use of cloud services at various points without the need to install third-party software. For example, this includes Microsoft Azure Online Backup or the online storage of BitLocker recovery keys. While cloud services can offer fundamental advantages (e.g. in terms of availability), using them carelessly can pose risks regarding confidentiality and dependency on service providers. This means that data can fall into the hands of unauthorised third parties via cloud services. These can be criminal attackers as well as state actors. If a provider stops offering a cloud service, this may have significant effects on an organisation’s own business processes.

2.3. Improper Administration of Windows Servers

Compared to previous versions, many new security-relevant features were added to Windows Server 2012 and Windows Server 2012 R2. In other (familiar) features, parameters, default configurations, and parts of functions were changed. If administrators have not been trained sufficiently in the particularities of the systems, configuration errors and human error can affect both the security and functionality of a system.

Non-uniform Windows Server security settings are a particular risk (e.g. for SMB, RPC, or LDAP). If configuration is not planned, documented, reviewed, and tracked systematically and in a centralised manner, it may lead to a configuration drift. The more the specific configurations of systems that are similar from a functional point of view differ for no reason and without any documentation, the more difficult it is to maintain an overview of the status quo and to maintain security in a holistic and consequent manner.

2.4. Improper Use of Group Policies (GPOs)

Group policies (Group Policy Objects, or GPOs) are a useful and powerful way to configure many (security) aspects of Windows Server 2012, particularly in a domain. Given the large number of possible settings, it is easy to accidentally set contradictory or incompatible settings or forget subject areas. A non-systematic approach in this regard will, at minimum, cause operational malfunctions that are sometimes difficult to remedy. In the worst case, severe vulnerabilities may arise on a server or connected client systems. In particular, improperly used inheritance rules and filters may result in GPOs not being applied to a system at all.

2.5. Loss of Integrity of Sensitive Information or Processes

Windows Server 2012 has numerous features that are designed to protect the integrity of information processed by the operating system. Each of these functions can contain vulnerabilities. Furthermore, they are often not configured thoroughly for reasons related to perceived user-friendliness or convenience. Information and processes may thus be falsified by unauthorised employees or external attackers, who are frequently able to cover their tracks in the process. In many cases, malware is also used to remotely manipulate information.

2.6. Unauthorised Acquisition or Misuse of Administrator Rights

Having administrators use standard user rights for their regular work is now common practice. Administrators must work with more extensive rights at certain points, however, which gives an attacker the opportunity to interfere and take control of such privileges. The misuse of rights by legitimate administrators is also a relevant damage scenario. Since these roles are often very powerful, the effects are typically significant, particularly in cases involving domain administrators. Even without guessing or breaking passwords, attackers can use pass-the-hash methods, for example, to read out and misuse appropriate credentials as a means of moving laterally within a network.

2.7. Compromised Remote Access

Windows Server 2012 has a large number of remote administration options that present general potential for misuse. Forms of remote access such as RDP user sessions may be available to third parties due to insecure or insecurely used protocols, weak authentication (e.g. weak passwords), or incorrect configuration. As a consequence, a server and the information it houses may be compromised to a critical extent. Additional IT systems connected to the server can also be compromised this way.

3. Requirements

The specific requirements of module SYS.1.2.2 *Windows Server 2012* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further

responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module SYS.1.2.2 *Windows Server 2012*, the following requirements MUST be met as a matter of priority:

SYS.1.2.2.A1 Planning of Windows Server 2012 (B)

The use of Windows Server 2012 MUST be planned carefully prior to installation. The hardware requirements MUST be checked prior to procurement. A justified and documented decision for an appropriate edition of Windows Server 2012 MUST be taken. The purpose of the server and its integration into Active Directory MUST be specified. The use of cloud services integrated into the operating system MUST be considered and planned as a matter of principle. If they are not required, the configuration of Microsoft accounts on the server MUST be blocked.

SYS.1.2.2.A2 Secure Installation of Windows Server 2012 (B)

Server roles, features, and functions beyond those required MUST NOT be installed. If it is sufficient from a functional scope perspective, the server core variant MUST be installed. Otherwise, reasons why the server core variant is not sufficient MUST be cited. Servers MUST already be updated to a current patch status during the installation.

SYS.1.2.2.A3 Secure Administration of Windows Server 2012 (B)

All administrators responsible for a server system MUST have training in the security-relevant aspects of administering Windows Server 2012. Web browsers on the server MUST NOT be used for surfing the Internet.

3.2. Standard Requirements

For module SYS.1.2.2 *Windows Server 2012*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

SYS.1.2.2.A4 Secure Configuration of Windows Server 2012 (S)

A single server SHOULD NOT fulfil several essential functions or roles; they should be suitably divided. Prior to commissioning, a system SHOULD be fundamentally hardened. To this end, function-specific security templates for the entire organisation in question SHOULD be created, maintained, and rolled out to the servers. Internet Explorer SHOULD only be used in its enhanced security configuration and enhanced protected mode on a server.

SYS.1.2.2.A5 Protection Against Malware on Windows Server 2012 (S)

Except for IT systems running Windows Server 2012 that are operated as stand-alone devices without any network connection or removable media, an anti-virus protection program SHOULD be installed prior to establishing an initial connection to the Internet or removable media. The applicable malware protection concept SHOULD call for full scans of all hard drives on a regular basis. Alarms SHOULD be configured that will alert the responsible administrators when viruses are found.

SYS.1.2.2.A6 Secure Authentication and Authorisation in Windows Server 2012 (S)

In Windows Server 2012 R2, all users SHOULD be members of the security group "Protected Users". Accounts for services and computers SHOULD NOT be members of the "Protected Users" group. Service accounts in Windows Server 2012 SHOULD be members of the "Managed Service Account" group. The PPL protection of the local security authority (LSA) SHOULD be activated. The use of dynamic access rules for resources SHOULD be preferred.

SYS.1.2.2.A7 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.2.2.A8 Protection of System Integrity (S)

AppLocker SHOULD be enabled and configured as stringently as possible.

SYS.1.2.2.A9 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.1.2.2 *Windows Server 2012* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.1.2.2.A10 ELIMINATED (H)

This requirement has been eliminated.

SYS.1.2.2.A11 Attack Detection in Windows Server 2012 (H)

Security-relevant events in Windows Server 2012 SHOULD be collected and analysed in a central location. Encrypted partitions SHOULD be blocked after a defined number of decryption attempts.

SYS.1.2.2.A12 Redundancy and High Availability in Windows Server 2012 (H)

The availability requirements that can be met or supported with the help of operating system functions such as Distributed File System (DFS), ReFS, failover clusters, network load balancing, or NIC teaming (LBFO) SHOULD be reviewed. For branch locations, BranchCache SHOULD be enabled.

SYS.1.2.2.A13 ELIMINATED (H)

This requirement has been eliminated.

SYS.1.2.2.A14 Shutting Down Encrypted Servers and Virtual Machines (H)

To protect encrypted data, servers that are not required (including virtual machines) SHOULD always be shut down. This SHOULD occur automatically whenever possible. Data encryption SHOULD require an interactive step or at least be documented in the security log.

4. Additional Information

4.1. Useful Resources

Microsoft provides the following additional information about Windows Server 2012:

- Secure Windows (for Windows 8/8.1, but largely also applicable to Windows Server 2012 / 2012 R2): https://technet.microsoft.com/en-us/library/hh832031.aspx
- Secure Windows Server 2012 R2 and Windows Server 2012: https://technet.microsoft.com/en-us/library/hh831360.aspx
- Security and Protection: https://technet.microsoft.com/en-us/library/hh831778.aspx
- List of security events on Windows 8.1 and Windows Server 2012: https://www.microsoft.com/en-us/download/confirmation.aspx?id=50034
- Configuring Additional LSA Protection: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
- Windows Server Guidance to Protect Against Speculative Execution: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-speculative-execution

The Information Security Forum (ISF) provides specifications for the use of servers in “The Standard of Good Practice for Information Security”, in particular in Area SY1.2 ("Server Configuration").

NIST Special Publication 800-123, "Guide to General Server Security" (July 2008), is offered by the National Institute of Standards and Technology (NIST).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security

objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.1.2.2 *Windows Server 2012*.

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.40 Denial of Service

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

SYS.1.3 Linux and Unix Servers

1. Description

1.1. Introduction

The operating systems Linux and Unix are often used on server systems. Examples of classic Unix systems include the BSD series (FreeBSD, OpenBSD, and NetBSD), Solaris, and AIX. Linux, on the other hand, is a functional Unix system rather than a classic Unix system. This means that the Linux kernel is not based on the original source code from which the various Unix derivatives developed. This module considers all the operating systems in the Unix family, including Linux as a functional Unix system. Since the configuration and operation of Linux and Unix servers are similar, Linux and Unix are jointly referred to in this module as "Unix servers" and "Unix-like".

Linux is free software that is developed by the open-source community. This means anyone can use, copy, distribute, or modify it. In addition, there are providers that compile and maintain the various software components for distribution and offer further services. For Linux servers, the distributions Debian, Red Hat Enterprise Linux / CentOS, SUSE Linux Enterprise / openSUSE, or Ubuntu Server are often used. In addition, there are Linux distributions tailored to special purposes and devices, such as OpenWRT for routers.

The services offered on a Unix server are often central, which means they are particularly exposed. For this reason, Unix servers are not only critical for business processes; they are also frequently the focus of attacks. As a result, the availability and protection of Unix servers is of particular importance.

1.2. Objective

The objective of this module is to protect information that is provided and processed by Unix servers. The requirements of the module mainly apply to Linux servers, but can be generally adapted to Unix servers. Requirements are formulated on how to configure and operate these operating systems independently of the intended purpose of the server in question.

1.3. Scoping and Modelling

Module SYS.1.3 *Linux and Unix Servers* must be applied to all servers on which Linux- or Unix-based operating systems are used.

The module contains basic specifications for creating and operating Unix servers. It specifies and adds specific features of Unix systems to the aspects included in module SYS.1.1 *General Server*.

Security requirements of possible server functions such as web servers (APP.3.2 *Web Servers*) or e-mail servers (see APP.5.3 *General E-Mail Clients and Servers*) are covered in separate modules; they are not addressed here. One exception is the Unix-specific server service SSH, which is also dealt with in this module. Similarly, the topic of virtualisation is not addressed in this module, but in SYS.1.5 *Virtualisation*.

2. Threat Landscape

For module SYS.1.3 *Linux and Unix Servers*, the following specific threats and vulnerabilities are of particular importance:

2.1. Unauthorised Collection of System and User Information

Using various UNIX programs, it is possible to capture data on users that is stored in an IT system. This includes data that can provide information on a user's activity profile. It can also contain information on other logged-in users, as well as technical information on the installation and configuration of the operating system.

For example, with a simple program that analyses information provided by the "who" command at certain intervals, any user can generate a precise utilisation profile for an account. It can then be determined, for instance, when the system administrator or administrators have been absent in order to exploit these patterns for unauthorised acts. The program also makes it possible to determine which terminals are approved for privileged access. Other programs with similar potential for data misuse are "finger" and "ruser".

2.2. Exploitability of the Script Environment

Script languages are often used in Unix operating systems. Scripts are lists of individual commands that are stored in text files and opened via the command line (for example). Due to the large scope of functions of the script environment, attackers may extensively misuse scripts for their purposes. Furthermore, it can be very difficult to contain enabled script languages.

2.3. Dynamic Loading of Jointly Used Libraries

With the command line option LD_PRELOAD, a dynamic library can be loaded before all the other standard libraries that are needed in an application. In this way, individual functions of standard libraries can be specifically overwritten by one's own. An attacker could thus

manipulate an operating system to execute malicious functions when using certain applications (for example).

2.4. Software from Third-Party Sources

In Unix-like IT systems, users may download and compile software source code themselves instead of installing ready-made software packages. Furthermore, when ready-made software packages are used, they are sometimes installed from third-party sources without further checking instead of exclusively from the manufacturer's existing package sources. Each of these alternative means of software installation entails additional risks because incorrect or incompatible software and malware may be installed.

3. Requirements

The specific requirements of module SYS.1.3 *Linux and Unix Servers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module SYS.1.3 *Linux and Unix Servers*, the following requirements MUST be met as a matter of priority:

SYS.1.3.A1 ELIMINATED (B)

This requirement has been eliminated.

SYS.1.3.A2 Careful Allocation of IDs (B)

Each login name, each user ID (UID), and each group ID (GID) MUST ONLY be used once. Every user MUST be a member of at least one group. Every GID mentioned in the */etc/passwd* file MUST be defined in the */etc/group* file. Every group SHOULD only contain the users that are absolutely necessary. In networked systems, care MUST also be taken to ensure that user and group names (UIDs and GIDs) are assigned consistently in the system network if there is a possibility that the same UIDs or GIDs could be assigned to different user or group names on the systems during cross-system access.

SYS.1.3.A3 No Automatic Integration of Removable Drives (B)

Removable media such as USB pen drives or CDs/DVDs MUST NOT be integrated automatically.

SYS.1.3.A4 Protection from Exploitation of Vulnerabilities in Applications (B)

ASLR and DEP/NX MUST be activated in the kernel and used by applications to make it harder to exploit vulnerabilities in applications. Security functions of the kernel and of the standard libraries (such as heap and stack protection) MUST NOT be disabled.

SYS.1.3.A5 Secure Installation of Software Packages (B)

If software to be installed is to be compiled from source code, it MUST ONLY be unpacked, configured, and compiled using an unprivileged user account. The software to be installed MUST NOT then be installed in the root file system of the server in question in an uncontrolled manner.

If the software is compiled from the source text, the selected parameters SHOULD be documented appropriately. Based on this documentation, it SHOULD be possible to compile the software in a transparent and reproducible manner at any time. All further installation steps SHOULD also be documented.

3.2. Standard Requirements

For module SYS.1.3 *Linux and Unix Servers*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

SYS.1.3.A6 Managing Users and Groups (S)

The corresponding management tools SHOULD be used for managing users and groups. The configuration files */etc/passwd, /etc/shadow*, */etc/group*, and */etc/sudoers* SHOULD NOT be edited directly.

SYS.1.3.A7 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.3.A8 Encrypted Access via Secure Shell (S)

Only Secure Shell (SSH) SHOULD be used to create an encrypted and authenticated interactive connection between two IT systems. All other protocols whose functions are covered by Secure Shell SHOULD be disabled completely. For authentication, users SHOULD primarily use certificates instead of passwords.

SYS.1.3.A9 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.3.A10 Preventing Further Intrusion When Vulnerabilities Are Exploited (S)

Services and applications SHOULD be protected with individual security architecture (e.g. with AppArmor or SELinux). In addition, chroot environments and LXC or Docker containers SHOULD be taken into account here. It SHOULD be ensured that the standard profiles and rules provided are activated.

SYS.1.3.A11 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.3.A12 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.1.3 *Linux and Unix Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.1.3.A13 ELIMINATED (H)

This requirement has been eliminated.

SYS.1.3.A14 Preventing Unauthorised Collection of System and User Information (H)

Information output for users regarding the operating system and access to protocol and configuration files SHOULD be limited to the required minimum. Moreover, confidential information SHOULD NOT be provided as parameters when commands are issued.

SYS.1.3.A15 ELIMINATED (H)

This requirement has been eliminated.

SYS.1.3.A16 Additional Prevention of Further Intrusion When Vulnerabilities Are Exploited (H)

The use of system calls SHOULD be limited to those absolutely necessary, particularly for exposed services and applications. The standard profiles and/or rules (e.g. of SELinux or AppArmor) SHOULD be checked manually and, if necessary, adapted to an organisation's own security policies. If necessary, new rules and profiles SHOULD be drawn up.

SYS.1.3.A17 Additional Kernel Protection (H)

Specially hardened kernels (e.g. grsecurity, PaX) and appropriate protective safeguards such as memory protection or file system protection SHOULD be implemented to prevent exploitation of vulnerabilities and propagation in operating systems.

4. Additional Information

4.1. Useful Resources

NIST Special Publication 800-123, "Guide to General Server Security" (July 2008), is offered by the National Institute of Standards and Technology (NIST).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.1.3 *Linux and Unix Servers*.

G 0.14 Interception of Information / Espionage

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Federal Office
for Information Security

SYS.1.5 Virtualisation

1. Description

1.1. Introduction

When IT systems are virtualised, one or several virtual IT systems are run on a physical IT system. A physical IT system of this kind is referred to as a virtualisation server. Several virtualisation servers may be consolidated to form a virtual infrastructure. Here, the virtualisation servers themselves and the virtual IT systems operated on them may be jointly administered.

The virtualisation of IT systems provides many advantages for IT operations in an information domain. For example, cost savings are possible in the fields of hardware procurement, electricity, and air conditioning if the resources of physical IT systems are used more efficiently. However, virtualisation also poses a challenge in operating an information domain. Since the virtualisation technology used affects different areas and fields of work in an information domain, knowledge and experience is required in these areas. In addition, problems on a virtualisation server can also affect all the other virtual IT systems operated on the same server. Virtual IT systems can also interfere with each other's operations.

1.2. Objective

The objective of this module is to show how virtualisation servers in an information domain can be securely implemented and operated.

1.3. Scoping and Modelling

SYS.1.5 *Virtualisation* must be applied to every virtualisation server.

In addition to this module, the relevant server or client modules of the SYS *IT Systems* layer must also be applied to each virtualisation server. Along with the operating-system-specific modules, modules SYS.1.1 *General Server* and SYS.2.1 *General Client* must be applied, as they summarise the platform-independent security aspects for servers and clients.

This module only deals with the virtualisation of complete IT systems. Other techniques, some of which are also associated with the term “virtualisation” (e.g. application virtualisation using terminal servers, storage virtualisation and containers), are not the subject of this module.

In the field of software development, the terms "virtual machine" and "virtual machine monitor" are also used for runtime environments (e.g. when Java or Microsoft .NET are used). Runtime environments like these are not addressed in this module either.

Virtual infrastructures are normally administered using specific management systems. Since these IT systems can be used to gain comprehensive access to a virtualisation infrastructure, it is important that they be sufficiently secured. This is applicable to both the physical or virtual server used to execute the management software and the product itself.

Virtualisation environments are mostly used together with storage networks (NAS or SAN). The connection and protection of these systems are also not addressed in this module (for this, see module SYS.1.8 *Storage Solutions*).

When using virtualisation, an organisation must structure its networks differently. This subject is not addressed comprehensively in this module. To this end, the requirements of module NET.1.1 *Network Architecture and Design* must be implemented. Finally, network virtualisation is also not examined in depth in this module.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module SYS.1.5 *Virtualisation*, the following specific threats and vulnerabilities are of particular importance.

2.1. Poor Planning of Virtualisation

A virtualisation server makes it possible to operate virtual IT systems, integrates these systems into a data centre, and, in so doing, controls their connection to further infrastructure elements such as networks (including storage networks). In the absence of any planning as to how virtualisation servers are to be integrated into existing infrastructure from a technical and organisational point of view, the responsibilities for different areas might not be clearly defined (e.g. for applications, operating systems, and network components). Moreover, the responsibilities for different areas may overlap, or there may be no appropriate rights structure for separating administrative access for the different areas.

2.2. Poor Configuration of Virtualisation

Virtualisation changes the way servers are provisioned. Resources such as CPUs, RAM, network connections, and storage are normally configured centrally using a management system and thus no longer depend on hardware and cabling. This can quickly lead to configuration errors. For example, if a virtual IT system is highly sensitive and is incorrectly located in an external demilitarised zone (DMZ), the system may be accessed from the Internet and is thereby exposed to increased risk.

2.3. Insufficient Resources for Virtual IT Systems

To operate virtual IT systems, virtualisation servers require disk space that is provided either locally in the servers themselves or in a storage network. If the storage capacities this requires are planned insufficiently, there will be extensive risks regarding the availability of virtual IT systems and the integrity of the information they process. This is particularly applicable if special virtualisation functions such as snapshots or the overbooking of disk space are used.

Bottlenecks can arise that involve not only the space available on hard disks or in storage networks, but processing power, RAM, or network connections, as well. Furthermore, insufficient resources on a virtualisation server may result in virtual machines disrupting one another's operations, which in turn can ultimately cause them to malfunction (or fail entirely).

2.4. Information Leaks or Resource Bottlenecks due to Snapshots

A snapshot may be used to capture and store the condition of a virtual machine. If a snapshot of this kind is restored at a later point in time, all the changes made since it was taken will be lost. As a consequence, any patched vulnerabilities may be reopened. Furthermore, open files, file transfers, or database transactions captured at the time of the snapshot may result in inconsistent data.

Attackers might also misuse snapshots to access the data of a virtual IT system in an unauthorised manner. For example, if a snapshot was made during live operations, the content of the main memory was also saved to the hard disk and may be restored and analysed in a virtual environment outside of the original IT infrastructure. Snapshots can also be large enough to cause a shortage of available storage space.

2.5. Failure of the Administration Server for Virtualisation Systems

Since an administration server controls and administers all the functions of a virtual infrastructure, a failure of this administration system will make it impossible to perform any configuration changes to the virtual infrastructure. During this period, the administrators cannot react to problems such as resource bottlenecks or the failure of individual virtualisation servers, nor can they integrate a new virtualisation server into the infrastructure and/or create new virtual IT systems. Live migration (and by extension, the dynamic assignment of resources for individual guest systems) is also not possible without an administration server.

2.6. Misuse of Guest Tools

Guest tools are often executed with very high authorisations on virtual machines. As a consequence, they may be misused for denial-of-service attacks or as a means of taking over the entire virtualisation server (for example).

2.7. Compromised Virtualisation Software

Virtualisation software (also known as a "hypervisor") is the central component of a virtualisation server. It controls all the virtual machines run on a server and assigns processor

and memory resources to them. If this component is attacked successfully, this will also compromise all the virtual IT systems that are run on the corresponding virtualisation server.

3. Requirements

The specific requirements of module SYS.1.5 *Virtualisation* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Planner

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

SYS.1.5.A1 ELIMINATED (B)

This requirement has been eliminated.

SYS.1.5.A2 Secure Use of Virtual IT Systems (B)

Every administrator of virtual IT systems MUST know how virtualisation affects the IT systems and applications in operation. The access rights of administrators regarding virtual IT systems MUST be reduced to those actually required.

It MUST be ensured that the network connections necessary for virtual IT systems are available in the respective virtual infrastructure. It MUST also be checked whether the isolation and encapsulation requirements of virtual IT systems and the applications operated on them are being met. Furthermore, the virtual IT systems used MUST meet the requirements at hand regarding availability and data throughput. During live operations, the performance of virtual IT systems MUST be monitored.

SYS.1.5.A3 Secure Configuration of Virtual IT Systems (B)

Guest systems MUST NOT access the devices and interfaces of a virtualisation server. However, if such a connection is necessary, it MUST be allocated exclusively. It MUST ONLY be established for the necessary duration by the administrator of the host system. Binding rules MUST be specified in this regard.

Virtual IT systems SHOULD be configured and protected according to the respective organisation's security policy.

SYS.1.5.A4 Secure Configuration of a Network for Virtual Infrastructures (B)

It MUST be ensured that existing security mechanisms (e.g. firewalls) and monitoring systems cannot be bypassed by virtual networks. It MUST also be ensured that virtual IT systems connected to several networks cannot be used to establish undesired network connections.

Network connections between virtual IT systems and physical IT systems and for virtual firewalls SHOULD be configured in accordance with the security policies of the organisation in question.

SYS.1.5.A5 Protection of Administration Interfaces (B)

All administration and management access to management systems and host systems MUST be restricted. It MUST be ensured that it is not possible to access administration interfaces from untrustworthy networks.

In order to administer and monitor virtualisation servers or management systems, protocols that are considered secure SHOULD be used. If insecure protocols are nevertheless used, a separate administration network MUST be used.

SYS.1.5.A6 Logging in the Virtual Infrastructure (B)

The operating condition, usage, and network connections of virtual infrastructures MUST be logged continuously. If capacity limits are reached, virtual machines SHOULD be moved. In addition, the corresponding hardware SHOULD be expanded, if applicable. Monitoring MUST also be conducted to ensure that virtual networks have been assigned properly to the respective virtual IT systems.

SYS.1.5.A7 Time Synchronisation in Virtual IT Systems (B)

The system time of all virtual IT systems in production use MUST always be synchronous.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

SYS.1.5.A8 Planning a Virtual Infrastructure [Planner] (S)

The structure of a virtual infrastructure SHOULD be planned in detail. In this process, the applicable rules and policies for operating IT systems, applications, and networks (including storage networks) SHOULD be taken into consideration. If several virtual IT systems are operated on a virtualisation server, conflicts regarding the protection requirements of the IT systems SHOULD be ruled out. Moreover, the tasks of the individual administrator groups SHOULD be defined and clearly separated. The employees responsible for operating specific components SHOULD also be defined.

SYS.1.5.A9 Network Planning for Virtual Infrastructure [Planner] (S)

The network structure for virtual infrastructures SHOULD be planned in detail. It SHOULD also be checked whether a separate network must be established and used for certain virtualisation functions (such as live migration). The network segments that need to be set up (e.g. management networks, storage networks) SHOULD be planned. It SHOULD be

determined how the network segments can be safely separated and protected from each other. Here, it SHOULD be ensured that the production network is separated from the management network (see SYS.1.5.A11 *Administration of the Virtualisation Infrastructure Using a Separate Management Network*). The availability requirements for the network in question SHOULD also be met.

SYS.1.5.A10 Introduction of Management Processes for Virtual IT Systems (S)

For virtualisation servers and virtual IT systems, processes for commissioning, inventory, operation, and decommissioning SHOULD be defined and established. The processes SHOULD be documented and updated at regular intervals.

If the use of such virtual IT systems is planned, the virtualisation functions that may be used by the virtual IT systems SHOULD be defined. Test and development environments SHOULD NOT be operated on the same virtualisation server as virtual IT systems in production use.

SYS.1.5.A11 Administration of the Virtualisation Infrastructure Using a Separate Management Network (S)

A virtualisation infrastructure SHOULD only be administered using a separate management network (see NET.1.1 *Network Architecture and Design*). The available security mechanisms of the management protocols used for authentication, integrity assurance, and encryption SHOULD be activated. All insecure management protocols SHOULD be disabled (see NET.1.2 *Network Management*).

SYS.1.5.A12 Rights and Role Concept for Virtual Infrastructure Administration (S)

Based on the tasks and roles defined in the planning phase (see SYS.1.5.A8 *Planning a Virtual Infrastructure*), a rights and role concept SHOULD be drawn up and implemented for administrating virtual IT systems and networks on virtualisation servers and in the management environment. All components of the virtual infrastructure SHOULD be integrated into a central identity and access management system. Administrators of virtual machines SHOULD be differentiated from administrators of the virtualisation environment at hand. They SHOULD be assigned different access rights.

Furthermore, the management environment SHOULD be able to group virtual machines for appropriate structuring. The roles of the administrators SHOULD be assigned accordingly.

SYS.1.5.A13 Selection of Suitable Hardware for Virtualisation Environments (S)

The hardware used SHOULD be compatible with the virtualisation solution used. Here, it SHOULD be ensured that the manufacturer of the virtualisation solution will also offer support for the hardware operated for the scheduled period of deployment.

SYS.1.5.A14 Uniform Configuration Standards for Virtual IT Systems (S)

Uniform configuration standards SHOULD be defined for the virtual IT systems used. The virtual IT systems SHOULD be configured in accordance with these standards. The configuration standards SHOULD be regularly reviewed and amended if required.

SYS.1.5.A15 Operation of Guest Operating Systems with Different Protection Needs (S)

If virtual IT systems with different protection needs are operated jointly on the same virtualisation server, it SHOULD be ensured that the virtual IT systems are encapsulated and isolated sufficiently. The network separation of the virtualisation solution used SHOULD be sufficiently secure, as well. If this is not the case, further security safeguards SHOULD be identified and implemented.

SYS.1.5.A16 Encapsulation of Virtual Machines (S)

The functions for copying and pasting information between virtual machines SHOULD be disabled.

SYS.1.5.A17 Monitoring the Operating Condition and Configuration of the Virtual Infrastructure (S)

The operating condition of the virtual infrastructure in question SHOULD be monitored. Among other things, it SHOULD be checked whether sufficient resources are still available. The shared resources of a virtualisation server SHOULD also be checked for conflicts.

Furthermore, it SHOULD be ensured that the configuration files of the virtual IT systems are regularly checked for unauthorised modifications.

If changes are to be made to the configuration of the virtualisation infrastructure, they SHOULD be checked and tested prior to being implemented.

SYS.1.5.A18 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.5.A19 Regular Audits of Virtualisation Infrastructure (S)

Regular audits SHOULD be carried out to check whether the actual state of the virtual infrastructure in question corresponds to the state defined in the respective planning. There SHOULD also be regular audits to check whether the configuration of the virtual components complies with the specified standard configuration. The audit results SHOULD be documented in a transparent manner. Deviations SHOULD be eliminated.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

SYS.1.5.A20 Using Highly Available Architectures [Planner] (H)

Virtual infrastructures SHOULD be designed for high availability. All virtualisation servers SHOULD be consolidated in clusters.

SYS.1.5.A21 Secure Configuration of Virtual IT Systems for Increased Protection Needs (H)

For virtual IT systems, features for overbooking resources SHOULD be disabled.

SYS.1.5.A22 Hardening of the Virtualisation Server (H)

The virtualisation server in question SHOULD be hardened. In order to further isolate and encapsulate virtual IT systems from each other and from the virtualisation server, mandatory access controls (MACs) SHOULD be used. The IT system on which the management software is installed SHOULD also be hardened.

SYS.1.5.A23 Restriction of Rights of Virtual Machines (H)

All interfaces and communication channels that make it possible for a virtual IT system to request and obtain information about the host system SHOULD be disabled or suppressed. Furthermore, only the virtualisation server SHOULD be able to access its resources. Virtual IT systems SHOULD NOT share pages of the main memory.

SYS.1.5.A24 Disabling Snapshots of Virtual IT Systems (H)

The snapshot feature SHOULD be disabled for all virtual IT systems.

SYS.1.5.A25 Minimal Use of Console Access to Virtual IT Systems (H)

Direct access to the emulated consoles of virtual IT systems SHOULD be reduced to a minimum. The virtual IT systems SHOULD be controlled via the network whenever possible.

SYS.1.5.A26 Use of a PKI [Planner] (H)

A public key infrastructure (PKI) SHOULD be used for certificate-protected communication between the components of a given IT infrastructure.

SYS.1.5.A27 Use of Certified Virtualisation Software (H)

Virtualisation software certified as EAL4 or higher SHOULD be used.

SYS.1.5.A28 Encryption of Virtual IT Systems (H)

All virtual IT systems SHOULD be encrypted.

4. Additional Information

4.1. Useful Resources

In the cyber security publication BSI-CS 113, “Server-Virtualisierung” [Server Virtualisation], the BSI provides recommendations on the use of virtualisation.

The Information Security Forum (ISF) provides specifications for the operation of virtual servers in “The Standard of Good Practice for Information Security” (section SYS.1.3, "Virtual Servers").

The National Institute of Standards and Technology (NIST) provides recommendations for the use of virtualisation in NIST Special Publication 800-125, “Guide to Security for Full Virtualization Technology”.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module SYS.1.5 *Virtualisation*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violations of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.37 Repudiation of Actions

G 0.43 Attack with Specially Crafted Messages

G 0.46 Loss of Integrity of Sensitive Information

SYS.1.6 Containerisation

1. Description

1.1. Introduction

The term *containerisation* describes a concept in which resources of an operating system are partitioned to create execution environments for processes. Depending on the operating system used, techniques that differ in terms of their functional scope and security features can be employed. This is often referred to as “operating system virtualisation”. However, an operating system is not virtualised in its entirety; certain resources are made available through a shared kernel. Generally, the term *container* is used to describe the resulting construct.

Before building and using complex container environments without due consideration, a thorough evaluation should be made in terms of whether the effort required to create and operate a container environment is suitably proportional to the actual benefits. The proper operation of container environments is very complex and there are many requirements to consider. Containers can be used as an additional separation mechanism to harden an environment, provided that the type of container technology and the configuration undertaken are appropriate and suitable for this purpose.

Here, a distinction is made between application containers (e.g. in line with the specification of the Open Container Initiative, OCI) and system containers. System containers such as FreeBSD jails, Solaris zones, OpenVZ, LXC, and LXD are the oldest type of containers. They provide an environment that behaves similarly to a standalone operating system that can provide appropriate services and run multiple applications. Application containers, on the other hand, are specifically designed to run a single application. They follow the lifecycle of the application, but do not offer operating-system-specific services within the container. From a technical point of view, however, these two types rely on the same mechanism for separation (i.e. process isolation by the kernel).

In the example of the Linux container (LXC), the mechanisms of *namespaces* and *cgroups* are mainly used to supplement process isolation.

- Namespaces are used to control which resources a process can see. There are seven different namespaces: mount (mnt), process ID (pid), network (net), inter-process communication (ipc), UTS (uts), user ID (user), and control group (cgroup).

- cgroups are used to control which resources or which part of a resource a process can use. In particular, resources include memory, CPU, BLKIO, or PIDS.

There are many details to consider when using namespaces and cgroups. Among other things, the order in which namespaces are shared plays a decisive role. Container runtimes have been developed for this purpose, such as *runc, crun, railcar*, or even *katacontainers*. The main task of container runtimes is to create a special execution environment for processes. They communicate with the kernel and issue syscalls with the appropriate parameters or in the correct order to obtain the desired execution environment.

As with an operating system, containers usually require a file system in which the programs to be executed are stored. In the container environment, certain file formats have become established to describe these file systems. These are also called *images*. However, they are sometimes also referred to incorrectly as containers. Depending on the type of container used, the content of these images can range from a single statically compiled application to the complete content of an operating system, including various execution environments and other dependencies. These images are transportable, self-contained units that can be deployed in a container environment and contain all the components required for functionality.

In addition to runtimes, there are container engines such as *Docker*, *Rocket*, or *CRI-O*, which take on many administrative tasks. Primarily, they form the interface to the user and process transferred commands. They ensure that the required images are available and that corresponding metadata are prepared. Finally, the container engine calls the container runtime with corresponding parameters. The container engine is thus not part of the containerisation mechanism, but takes on an administrative function here.

Furthermore, there are different types of containers. These differ according to the deployment scenario and the lifecycle of the container in question. A “persistent container” is a container that is intended to be used for a longer period of time. There may well be valid reasons to store data permanently in containers. Especially in the cloud environment, however, “volatile containers” are frequently encountered. There, containers usually have a much shorter lifespan, which is also often determined by orchestration tools.

Within the OCI, efforts are being made to provide standards and reference implementations. For example, *runc* is the standard reference implementation of a container runtime. Other container runtimes that are compatible with the OCI standard can thus be widely exchanged and used.

1.2. Objective

The objective of this module is to protect information which is processed, provided, or transmitted from or with containers. The module deals with how containers can be secured in principle. A distinction is made between the services for operating containers (i.e. the software that is responsible for configuring and managing them) and the applications and services that are executed within containers.

1.3. Scoping and Modelling

SYS.1.6 *Containerisation* must always be used whenever services or applications are run in containers.

This module considers containers without regard for specific products. The requirements are based on the capabilities of implementations currently available on the market. When selecting a product, module APP.6 *General Software* must be taken into account.

The module supplements the aspects dealt with in the modules SYS.1.1 *General Server* and SYS.1.3 *Linux and Unix Servers* with specifics related to containerisation. The requirements of these modules should be met by the host system regardless of whether it is running on physical servers or is virtualised. Furthermore, the requirements of these modules also apply to each of the user space environments created in the context of containerisation. Other modules, such as CON.8 *Software Development* or the modules of the sub-layer OPS.1.1 *Core IT Operation*, must be considered on a regular basis. This is especially true for the creation of images.

Typically, containers communicate with each other through virtual networks on the host system. The modules of the sub-layers NET.1 *Networks* and NET.3 *Network Components* must be considered accordingly.

Security requirements of possible services, such as web servers (APP.3.2 *Web Servers*) or web applications (APP.3.1 *Web Applications and Web Services*) are the subject of separate modules that must be applied additionally. If the host system is virtualised, module SYS.1.5 *Virtualisation* must be followed.

If containers and their underlying infrastructure are not completely operated and used on their own, but parts of them are provided or used by third parties, additional requirements of the modules OPS.2.1 *Outsourcing for Customers*, OPS.2.2 *Cloud Usage*, and OPS.3.1 *Outsourcing for Service Providers* must be considered.

The present module contains basic specifications for setting up and operating containers. The other common services in the containerisation environment, such as orchestration of containers, storage systems, virtual networks, automation for CI/CD pipelines, or the operation of image registries, are not considered here. This module also does not make any statements about requirements that apply to the construction of images. For requirements regarding the orchestration of containers with Kubernetes, module APP.4.4 *Kubernetes* should be considered.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module SYS.1.6 *Containerisation*, the following specific threats and vulnerabilities are of particular importance.

2.1. Vulnerabilities or Malware in Images

Containers are primarily created on the basis of ready-made images that are created by the user, but are also often obtained from the Internet. Furthermore, software is increasingly being delivered by manufacturers in the form of images. An IT department can also use these images to create their own images by adding, changing, or even removing software or configurations.

The software contained in the images could be vulnerable and the containers launched from the image could be vulnerable as a result. Such vulnerabilities may also often not be known to the IT department responsible, as the software contained in the images is often not recorded in their own software administration. As a rule, an IT department must rely on updates being made available through the image creation process. From the outside, it is often difficult to determine which software packages are contained in these images.

In addition, images may contain intentionally integrated malware, such as ransomware or crypto miners. Since a single image is often deployed in a large number of containers, the resulting damage can be immense.

2.2. Administrative Access Without Security

Administrative access is needed to manage container services on a host. Such access is often realised as services that can be accessed either locally or via a network. Mechanisms for authentication and encryption of the administrative accesses are often present, but not activated by default in all products.

If unauthorised persons can access the network sockets or the host system, they can execute commands via unprotected administrative access points, which can lead to a loss of confidentiality, integrity, and availability in all the containers running on the host.

2.3. Resource Conflicts on the Host

Individual containers can overload the host, jeopardising the availability of all other containers on the host or even the operation of the host system itself.

2.4. Unauthorised Communication

All containers on a host are basically able to communicate with each other, with the host, and with any other host. If this communication is not restricted, malware or an attacker can exploit this to attack other containers or hosts (for example).

Furthermore, there is the danger that containers will be accessible from the outside, even if this is not desired. This could allow an external attack against services that should only be accessible internally. This threat is increased by the fact that less attention is often paid to internal services. If a vulnerability is tolerated in a service that is only used internally but is also accessible from the outside, this can put the entire corresponding operation at considerable risk.

2.5. Breaking Out of the Container into the Host System

If an attacker is able to execute their own code in a container, they may be able to overcome the container's isolation from other containers or the host and thus access other containers, the host system, or adjacent infrastructure. This is also referred to as a “container outbreak”. Such an attack can occur, for example, via vulnerabilities in processors, in the operating system kernel, or in locally offered infrastructure services such as DNS or SSH.

An attacker could thereby take control of the host system or other systems from the infrastructure. This presents the threat of a loss of confidentiality, integrity, and availability in all the containers running on the host, as well as on the host itself if the attacker can also gain elevated privileges there.

2.6. Data Loss Through Container Management

As part of the management of containers, they can be switched off without giving software currently running in them the opportunity to complete current write processes, for example (improper shutdown). If data is being processed by a container at these times, all this data is lost. Data that is persistently stored in the container can also be permanently lost in this way.

2.7. Loss of Confidentiality of Access Data

The principles of building and creating images for containers presuppose that access data (e.g. for databases) is available in the container. Such access data can fall into unauthorised hands via the images themselves, the scripts for creating the images, or the version control of the scripts.

In many cases, access data is also made available as an environment variable at the time a container is created. This presents another threat to the confidentiality of this data.

2.8. Disorderly Provision and Distribution of Images

In contrast to conventional installations in which IT departments have full control over the applications, components, and services deployed, this control is lost in container environments, (e.g. in the case of automation through CI/CD). Here, the IT department only provides a platform into which developers can directly introduce their applications—including all their dependencies—and change them at any time.

3. Requirements

The specific requirements of module SYS.1.6 *Containerisation* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	None

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

SYS.1.6.A1 Planning Container Use (B)

Before containers are deployed, the goal of such a deployment (e.g. scaling, availability, disposable containers for safety or CI/CD) SHOULD be determined so that all the security-related aspects of installation, operation, and decommissioning can be planned. The planning SHOULD also take into account the operational overhead resulting from container deployment or mixed operation. The planning MUST be adequately documented.

SYS.1.6.A2 Container Management Planning (B)

The management of containers MUST ONLY be carried out in line with appropriate planning. This planning MUST cover the entire lifecycle from commissioning to decommissioning, including operation and updates. When planning container management, it MUST be taken into account that the creator of a container is to be considered like an administrator due to the effects they have on parts of the operation.

Containers MUST be started, stopped, and monitored via the management software used.

SYS.1.6.A3 Secure Use of Containerised IT Systems (B)

In the case of containerised IT systems, consideration MUST be given to how containerisation affects the IT systems and applications operated, in particular the management and suitability of the applications.

Based on the protection needs of the applications, it MUST be checked whether the requirements for isolation and encapsulation of the containerised IT systems, virtual networks, and operated applications are sufficiently fulfilled. The mechanisms of the operating system in question SHOULD be included in this check. Since the host performs the function of a network component for virtual networks, the modules of the sub-layers NET.1 *Networks* and NET.3 *Network Components* MUST be considered accordingly. Logical and overlay networks MUST also be considered and modelled. Furthermore, the containerised IT systems used MUST meet the requirements at hand regarding availability and data throughput.

During operation, the performance and the state of the containerised IT systems SHOULD be monitored (health checks).

SYS.1.6.A4 Planning the Provision and Distribution of Images (B)

The process for the provision and distribution of images MUST be planned and appropriately documented.

SYS.1.6.A5 Separation of Administration and Access Networks for Containers (B)

Networks for the administration of the host, the administration of the containers, and their access networks MUST be separated according to the protection needs at hand. In principle, at least the administration of the host SHOULD only be possible from the administration network.

Only the communication relationships necessary for operation SHOULD be allowed.

SYS.1.6.A6 Use of Secure Images (B)

It MUST be ensured that all images used originate from trusted sources. The creator of each image MUST be clearly identifiable.

Sources MUST be selected on the basis of whether the creator of a given image regularly checks the included software for security problems, fixes and documents them, and provides corresponding guarantees to customers.

The utilised version of base images MUST NOT be deprecated. Unique version numbers MUST be provided. If an image with a newer version number is available, a patch and change management process MUST check whether and how it can be rolled out.

SYS.1.6.A7 Persistence of Container Logging Data (B)

Container logging data MUST be stored outside of the respective container (on the container host at minimum).

SYS.1.6.A8 Secure Storage of Container Access Data (B)

Access data MUST be stored and managed in such a way that only authorised persons and containers can access it. In particular, it MUST be ensured that access data is only stored in specially protected locations and not in images. The access data management mechanisms provided by container service management software SHOULD be used.

At minimum, the following credentials MUST be stored securely:

- Passwords of any accounts
- API keys for services used by the application
- Keys for symmetric encryption
- Private keys for public key authentication

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

SYS.1.6.A9 Suitability for Container Operation (S)

An application or service to be operated in a container SHOULD be suitable for such operation. It SHOULD be considered that containers can often be terminated unexpectedly, with corresponding consequences for the application run therein. The results of the checking described under SYS.1.6.A3 *Secure Use of Containerised IT Systems* SHOULD be documented in a comprehensible manner.

SYS.1.6.A10 Policy for Images and Container Operation (S)

A policy SHOULD be established and applied that specifies the requirements for container operation and permitted images. The policy SHOULD also include requirements for the operation and deployment of images.

SYS.1.6.A11 Only One Service per Container (S)

Each container SHOULD only provide one service at a time.

SYS.1.6.A12 Distribution of Secure Images (S)

The sources of images that have been classified as trusted and SHOULD be adequately documented along with the corresponding reasons. In addition, the process of how images or the software components contained in an image are obtained from trusted sources and eventually deployed to a productive environment SHOULD be adequately documented.

Images used SHOULD have metadata that makes their function and history traceable. Digital signatures SHOULD secure each image against modification.

SYS.1.6.A13 Release of Images (S)

All images for productive operation SHOULD undergo a test and release process in the same way as software products in accordance with module OPS.1.1.6 *Software Tests and Approvals*.

SYS.1.6.A14 Updating Images (S)

When establishing a concept for patch and change management according to OPS.1.1.3 *Patch and Change Management*, it SHOULD be decided when and how the updates of images or the software or service operated are to be rolled out. For persistent containers, checks SHOULD be made as to whether an update of a container is more appropriate than completely re-provisioning the container in exceptional cases.

SYS.1.6.A15 Limitation of Resources per Container (S)

Resources on the host system such as CPU, volatile and persistent memory, and network bandwidth SHOULD be appropriately reserved and limited for each container. How the system should react if these limits are exceeded SHOULD be defined and documented.

SYS.1.6.A16 Administrative Remote Access to Containers (S)

In principle, administrative access from a container to the container host and vice versa SHOULD be considered as administrative remote access. Remote administrative access SHOULD NOT be established from a container to the container host. Application containers SHOULD NOT contain remote maintenance access points. Administrative access to application containers SHOULD always be carried out via the container runtime.

SYS.1.6.A17 Running Containers Without Privileges (S)

A container runtime and any instantiated containers SHOULD only be executed by a non-privileged system account that does not have (and cannot gain) elevated rights to the container service or host operating system. The container runtime SHOULD be encapsulated by additional measures, such as using the virtualisation extensions of CPUs.

If containers are to take over tasks of the host system in exceptional cases, privileges on the host system SHOULD be limited to the minimum necessary. Exceptions SHOULD be adequately documented.

SYS.1.6.A18 Application Services Accounts (S)

System accounts within a container SHOULD have no permissions on the host system. If such authorisation is required for operational reasons, it SHOULD only apply to the data and system access that is absolutely necessary. The account in the container that is necessary to exchange data SHOULD be known in the host system.

SYS.1.6.A19 Including Data Stores in Containers (S)

Containers SHOULD ONLY be able to access the mass storage and directories necessary for operation. Permissions SHOULD only be explicitly assigned where needed. If the container runtime for a container includes local storage, the access rights in the file system SHOULD be restricted to the service account of the container. If network storage is used, the permissions SHOULD be set on the network storage itself.

SYS.1.6.A20 Protection of Configuration Data (S)

Descriptions of container configuration data SHOULD be versioned. Changes SHOULD be documented in a comprehensible manner.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

SYS.1.6.A21 Extended Security Policies (H)

Extended policies SHOULD restrict the permissions of containers. Mandatory Access Control (MAC) or a comparable technology SHOULD enforce these policies. At minimum, policies SHOULD restrict the following types of access:

- Incoming and outgoing network connections
- File system access attempts
- Kernel requests (syscalls)

A runtime SHOULD start containers in such a way that the kernel of the host system prevents all activities of the containers that are not allowed by the relevant policy (e.g. by setting up local packet filters or revoking permissions), or at least reports violations appropriately.

SYS.1.6.A22 Provision for Investigations (H)

In order to have containers available for later investigation in case they are needed, an image of each container's state SHOULD be created according to specified rules.

SYS.1.6.A23 Container Immutability (H)

Containers SHOULD not be able to change their file system during runtime. File systems SHOULD not be integrated with write permissions.

SYS.1.6.A24 Host-Based Attack Detection (H)

The behaviour of containers and the applications or services running in them SHOULD be monitored. Deviations from normal behaviour SHOULD be noticed and reported. The reports SHOULD be handled appropriately in a centralised process for security incident handling.

At minimum, the behaviour to be monitored SHOULD cover:

- Network connections
- Created processes
- File system access attempts
- Kernel requests (syscalls)

SYS.1.6.A25 High Availability of Containerised Applications (H)

In cases involving containerised applications with high availability requirements, the necessary level of availability SHOULD be defined (e.g. redundant at the host level).

SYS.1.6.A26 Advanced Isolation and Encapsulation of Containers (H)

If further isolation and encapsulation of containers is required, the following measures SHOULD be considered for increased effectiveness:

- Fixed assignment of containers to container hosts
- Execution of the individual containers and/or the container host by means of hypervisors
- Fixed assignment of a single container to a single container host

4. Additional Information

4.1. Useful Resources

For more information about threats and security safeguards with regard to containers, see the following publications, among others:

- NIST 800-190
  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf
- CIS Benchmark Docker
  https://www.cisecurity.org/benchmark/docker/
- OCI – Open Container Initiative
  https://www.opencontainers.org/
- CNCF – Cloud Native Computing Foundation
  https://www.cncf.io/
- SANS Checklist
  https://www.sans.org/reading-room/whitepapers/auditing/checklist-audit-docker-containers-37437

- Docker Security Guide
  https://docs.docker.com/engine/security/

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module SYS.1.6 *Containerisation*:

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.40 Denial of Service

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

SYS.1.7 IBM Z

1. Description

1.1. Introduction

IBM Z type systems belong to the server systems generally referred to as mainframes. Mainframes have evolved from classic stand-alone systems with batch processing into state-of-the-art client/server systems. The Z architecture – the successor to the S/360 architecture introduced in 1964 – is often used in current mainframe installations.

1.2. Objective

The objective of this module is to protect information which is processed, provided, or transmitted via Z systems.

1.3. Scoping and Modelling

Module SYS.1.7 *IBM Z* must be applied to every server based on IBM's Z architecture.

Module SYS.1.1 *General Server* forms a generic basis for the protection of servers. For Z systems, both the general requirements listed there and the specific requirements in this module must be met.

Different operating systems are available for the Z hardware (e.g. z/OS, z/VM, KVM, or Linux on Z). These are normally selected based on the size and purpose of the computer at hand. The recommendations of this module are essentially limited to the operating system z/OS. Select security aspects of z/VM are also addressed. For the Linux on Z operating system, please refer to module SYS.1.3 *Linux and Unix Servers*.

Modules ORP.4 *Identity and Access Management* and OPS.1.2.5 *Remote Maintenance* contain additional requirements that are particularly relevant for IBM Z.

An important component of the security concept of Z systems at the technical level is the security system used—for example, TopSecret, ACF2 (Access Control Facility), or RACF (Resource Access Control Facility). To simplify the information presented, only RACF is

discussed below. The recommendations should be adapted accordingly if a different security system is used.

The respective specific services offered by the Z system are not part of this module. For these services, additional modules will need to be implemented based on the results of the IT-Grundschutz modelling process.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module SYS.1.7 *IBM Z*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inadequate or Incorrect Configuration of Hardware or the z/OS Operating System

The configuration of a z/OS operating system is very complex and requires action from a system administrator in many areas. Incorrect or inadequate configuration can quickly lead to vulnerabilities and related security problems. Supervisor calls (SVCs), for example, are calls to special z/OS utilities that run with a high level of authorisation in kernel mode. Under certain circumstances, insecure SVC programs can be used to circumvent z/OS security mechanisms.

2.2. Incorrect Configuration of the z/OS Security System RACF

In a z/OS operating system, a special security system is responsible for authenticating users and authorising them to access resources. RACF is often used for this. As a rule, the default configuration of RACF does not match the security requirements in the operational scenario at hand. The resources and z/OS system commands are protected using special classes in RACF, for example. If these classes are inadequately defined, it is possible for users to issue system commands that could degrade stable system operation in certain circumstances.

2.3. Incorrect Use of z/OS System Functions

Due to the complexity of a z/OS operating system and its components, operating errors cannot be ruled out completely. Depending on the nature of an incorrect action, individual components or the entire system may fail. For example, if different resources lock one another (contention), functions may not be available until the lock is removed. A series of system prompts (displays) and considerable experience are often necessary to remove mutual locks like this with the aid of the right z/OS commands.

2.4. Manipulation of the z/OS System Configuration

z/OS systems can be influenced via various interfaces, such as the hardware management console, local/remote MCS consoles, automation procedures, and remote maintenance access. For example, if physical or logical access to remote MCS consoles is inadequately protected, z/OS systems may be tampered with from these locations.

2.5. Attacks on z/OS Systems Using TCP/IP

To attack a z/OS system via a network connection, it is often not necessary to have any special knowledge of z/OS or the network architecture at hand. Due to their TCP/IP connections to (in some circumstances public) networks and Unix System Services, many z/OS systems can be reached by external attackers using standard protocols and services such as HTTP or FTP. External attackers can, in certain circumstances, carry out denial-of-service attacks against the services provided over a TCP/IP connection to public networks, or read or tamper with transmitted data without authorisation. Internal attackers can try to increase their authorisations using a TCP/IP connection to internal networks by obtaining the ID and password of a user with SPECIAL rights (for instance).

2.6. Incorrect Character Conversion When Using z/OS

EBCDIC, ASCII, and Unicode are character sets that determine how letters, numbers, and other characters are represented by bits. z/OS systems work with EBCDIC code. Only HFS and zFS file systems used with Unix System Services (USS) make it possible to save data in both ASCII and EBCDIC. When exchanging data between z/OS systems and systems using ASCII or Unicode (including from USS to z/OS, for example), there is a risk that information could be corrupted if incorrect translation tables (code page translation) are used. Here, the translation of special characters is a particularly frequent problem.

3. Requirements

The specific requirements of module SYS.1.7 *IBM* Z are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Supervisor

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

SYS.1.7.A1 Use of Restrictive z/OS IDs (B)

High-level authorisations MUST ONLY be assigned to users who need these rights for their activities. In particular, the RACF attributes SPECIAL, OPERATIONS, AUDITOR, and the corresponding GROUP attributes, as well as the user ID 0, MUST be handled restrictively under Unix System Services (USS). The assignment and use of these authorisations MUST be

documented transparently. The special ID IBMUSER MUST ONLY be used during reinstallation to create IDs with SPECIAL attributes. Once this is complete, this ID MUST be permanently disabled. To prevent administrators from permanently locking themselves out, an emergency user procedure MUST be set up.

SYS.1.7.A2 Protection of Security-Critical z/OS Utilities (B)

Security-critical (service) programs and commands and their alias names MUST be protected with rights to corresponding RACF profiles in such a way that they can only be used by the designated and authorised employees. It MUST be ensured that (third-party) programs cannot be installed without authorisation. In addition, programs MUST ONLY be installed from secured sources using transparent methods (e.g. SMP/E).

SYS.1.7.A3 Maintenance of Z Systems (B)

Z hardware and firmware, the operating system in question, and the various programs used MUST be maintained regularly and on the basis of need. The maintenance activities required for this MUST be planned and integrated into change management (see OPS.1.1.3 *Patch and Change Management*). In particular, updates MUST ONLY be performed by the manufacturer under the supervision of the operator and either locally via SE (Support Elements) or HMC (Hardware Management Console) or remotely via the RSF (Remote Support Facility).

SYS.1.7.A4 Training z/OS Operators [Supervisor] (B)

Administrators, operators, and auditors with tasks related to z/OS MUST be trained accordingly. In particular, RACF administrators MUST be familiar with the security system itself and any other functions relevant to it.

SYS.1.7.A5 Use and Protection of System-Related z/OS Terminals (B)

System-adjacent z/OS terminals MUST be physically and logically protected against unauthorised access. The Support Elements in particular MUST be considered, along with the HMC, MCS, SMCS, Extended MCS, and monitor consoles. Default passwords MUST be changed. Access via web servers and other remote access MUST be protected by encryption. Web servers and other forms of remote access MUST be disabled when not in use.

SYS.1.7.A6 Use and Protection of the Remote Support Facility (B)

The head of the IT Operation Department MUST decide whether and how RSF is to be used. Such use MUST be governed by a corresponding maintenance contract and coordinated with hardware support staff. It MUST be ensured that the RSF configuration can only be changed by authorised persons. Maintenance access for firmware modifications by the manufacturer MUST be explicitly approved by the operator and disabled again after these modifications are completed. RSF communication MUST take place via a proxy server and also using secure connections (such as TLS).

SYS.1.7.A7 Restrictive Authorisation in z/OS (B)

In the basic configuration of z/OS, the authorisation mechanisms MUST be configured so that all persons (defined user IDs in groups according to the respective roles) only have the access options they need for their respective activities. For this purpose, APF (authorised program facility) authorisations, supervisor calls (SVCs), resources of the z/OS operating system, IPL parameters, Parmlib definitions, started tasks, and JES2/3 definitions MUST be considered.

SYS.1.7.A8 Use of the z/OS Security System RACF (B)

The use of the RACF for z/OS MUST be planned carefully. This includes the selection of a character set, the definition of rules for user IDs and passwords, and the activation of KDFAES encryption. If RACF PassTickets are used, the Enhanced PassTicket algorithm MUST be enabled. Default passwords for the RVARY command and for newly created user IDs MUST be changed. If RACF exits are to be used, their use MUST be justified, documented, and regularly monitored.

Suitable procedures MUST be defined for creating, locking, releasing, and deleting RACF IDs. After a specified number of failed login attempts, an RACF ID MUST be locked (exception: emergency user procedures). User IDs MUST also be blocked after a prolonged period of inactivity, but process IDs must not.

Files, started tasks, and security-critical programs MUST be protected with RACF profiles. Users MUST ONLY receive the data access they need in accordance with their roles. It MUST also be ensured that users are not able to extend their access options without permission.

SYS.1.7.A9 Multi-Client Capability in z/OS (B)

If a z/OS system is to be used by clients, an RACF concept for client separation MUST be created. The data and applications of the clients MUST be segregated by means of RACF profiles. High-level authorisations in RACF (SPECIAL, OPERATIONS, AUDITOR) and change access to files of the z/OS operating system MUST ONLY be granted to employees of the operator. The maintenance time slots in which the z/OS system will not be available MUST be coordinated with all the clients working on the system concerned.

SYS.1.7.A10 ELIMINATED (B)

This requirement has been eliminated.

SYS.1.7.A11 Protection of Session Data (B)

Session data for the connections of RACF administrators and other employees MUST be transferred in encrypted form.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

SYS.1.7.A12 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.7.A13 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.7.A14 Reporting on the Secure Operation of z/OS (S)

A process SHOULD be set up to monitor all security-relevant operations in z/OS. This SHOULD specify the security reports to be produced regularly, the tools and data sources to be

used (e.g. the system management facility), and how deviations from specifications are to be dealt with. The security reports SHOULD be used as information during checks.

SYS.1.7.A15 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.7.A16 Monitoring of z/OS Systems (S)

During operation, the z/OS system SHOULD be monitored for important messages, events, and compliance with thresholds. In particular, error messages on the HMC console, WTOR and important WTO messages (write to operator/with reply), system tasks, security breaches, capacity limits, and system utilisation SHOULD be considered. At minimum, the MCS console, the system management facility, the SYSLOG, and the relevant log data of applications SHOULD also be used for monitoring. It SHOULD be ensured that all important messages are recognised promptly and responded to in an appropriate manner when required. System messages SHOULD be filtered in such a way that only those messages that are actually important are displayed.

SYS.1.7.A17 Synchronisation of z/OS Passwords and RACF Commands (S)

If z/OS passwords or RACF commands are to be automatically synchronised across several z/OS systems, the respective systems SHOULD be standardised to the greatest extent possible. The blocking of user IDs due to incorrect password entries SHOULD NOT be synchronised. The risk of synchronising security-critical RACF commands SHOULD be taken into account. The management function of the synchronisation program used SHOULD only be available to authorised employees within the scope of their activities.

SYS.1.7.A18 Role Concept for z/OS Systems (S)

For z/OS systems, a role concept SHOULD be introduced for system administration at minimum. Arrangements for deputies SHOULD also be in place for all important system administration roles. The RACF attributes SPECIAL, OPERATIONS, and AUDITOR SHOULD be assigned to different people (role separation).

SYS.1.7.A19 Protection of z/OS Transaction Monitors (S)

If transaction monitors or databases such as IMS, CICS, or Db2 are used in z/OS, they SHOULD be backed up using RACF. This also applies to the associated system commands and files. Internal security mechanisms for transaction monitors and databases, on the other hand, SHOULD only be used where there are no corresponding RACF functions. Users and administrators SHOULD only receive the access rights they need for their respective tasks.

SYS.1.7.A20 Decommissioning z/OS Systems (S)

When decommissioning a z/OS system, other z/OS systems, groupings, and management systems SHOULD be adapted so that they no longer refer to the decommissioned system. The impact on software licences SHOULD also be considered.

Hard disks containing confidential data SHOULD be deleted in such a way that their content cannot be reproduced. In the event that defective hard disks are replaced by the manufacturer, it SHOULD be contractually agreed that these hard disks will be securely destroyed or deleted in such a way that their contents can no longer be reproduced.

SYS.1.7.A21 Protection of the Startup Process of z/OS Systems (S)

The parameters necessary for the startup procedure of a z/OS system SHOULD be documented and known to the operating personnel. The required hardware configurations, such as the IOCDS file (Input/Output Configuration Data Set) and the LPARs (logical partitions), SHOULD also be available. A z/OS master console and a backup console SHOULD be defined to control messages. After the startup procedure, a checklist SHOULD be used to monitor whether the system status corresponds to the target specifications. In addition, a fallback configuration with which the system was successfully started before the last change SHOULD be maintained.

SYS.1.7.A22 Protection of the Operating Functions of z/OS (S)

All maintenance work affecting production, as well as dynamic changes and other modifications, SHOULD only be carried out within the framework of change management (see OPS.1.1.3 *Patch and Change Management*). SDSF (System Display and Search Facility) and similar functions, as well as priority control for jobs, SHOULD be protected against unauthorised access using RACF. z/OS system commands—in particular, security-relevant commands for dynamic changes—SHOULD be protected via RACF. When defining hardware dynamically, it SHOULD be ensured that a resource is not assigned to several individual systems outside a Parallel Sysplex during actual operations.

SYS.1.7.A23 Protection of z/VM (S)

If z/VM is used, it SHOULD be integrated into patch management. All default passwords SHOULD be changed. The role of z/VM system administrator SHOULD only be assigned to persons who require the corresponding authorisations. RACF for z/VM SHOULD be used for z/VM security administration. Passwords for real users and guest users SHOULD be encrypted using RACF for z/VM. z/VM system commands that are critical to security SHOULD be protected using RACF. The virtual machines defined in z/VM SHOULD only be provided with the resources necessary to perform their particular tasks and strictly separated from each other. Only the services needed SHOULD be started in z/VM. When checks are performed, the journalling function of z/VM and the audit functions of RACF SHOULD be used.

SYS.1.7.A24 Administration of Storage Media in z/OS Systems (S)

Files, programs, and functions for the administration of storage media—as well as storage media themselves (hard disks and tapes), including the master catalogue—SHOULD be protected using RACF profiles. Backup copies of all important files SHOULD be available that can be installed in case of an emergency. The assignment of storage media to Z systems SHOULD be documented transparently. It SHOULD be ensured that sufficient tape stations are available for the volume and time frame at hand. The hard disks that are to be backed up and the backup procedure itself SHOULD be specified when using the HSM (Hierarchical Storage Manager). Tapes that are managed by the HSM SHOULD NOT be modified elsewhere.

SYS.1.7.A25 Stipulation of z/OS System Capacity (S)

The limits for maximum resource load (number of CPUs, storage, bandwidth, etc) SHOULD be set according to the hardware requirements at hand and made known to the administrators and application owners in charge. The number of magnetic tape stations available, the times during which applications access these stations, and the required disk capacities SHOULD be

agreed with the application owners. Hard disk capacities SHOULD also be monitored by a space management solution.

SYS.1.7.A26 Workload Management for z/OS Systems (S)

The programs, files, and commands of the Workload Manager (WLM), as well as the necessary couple data sets, SHOULD be protected by RACF. It SHOULD be ensured that the authorisations required to change the WLM via z/OS commands and via the SDSF interface are the same.

SYS.1.7.A27 Character Set Conversion in z/OS Systems (S)

When text files are transferred between z/OS systems and other systems, it SHOULD be taken into account that character set conversion may be required. The correct conversion table SHOULD be used for this. When transferring program source code, the correct translation of characters SHOULD be checked. When transmitting binary data, on the other hand, it SHOULD be ensured that no character set conversion takes place.

SYS.1.7.A28 Licence Key Management for z/OS Software (S)

For licence keys with limited validity, a timely renewal procedure SHOULD be put in place. The contract periods of the licence keys SHOULD be documented. The documentation SHOULD be made available to all the administrators concerned.

SYS.1.7.A29 Protection of Unix System Services on z/OS Systems (S)

The parameters of Unix System Services (USS) SHOULD be set according to the functional and security specifications at hand while taking the available resources into account. HFS and zFS files containing USS file systems SHOULD be backed up via RACF profiles and included in a backup concept. The root file system SHOULD also be mounted with the read-only option. In the USS file system, APF (authorised program facility) authorisations SHOULD NOT be granted using a file security packet (FSP). The modules of APF files of the z/OS operating system SHOULD be loaded instead. The assignment between USS user IDs and z/OS user IDs SHOULD be clear. Authorisations under USS SHOULD be assigned using the RACF class UNIXPRIV and NOT by assigning UID 0. The USS SHOULD be checked and monitored using the same mechanisms used for z/OS.

SYS.1.7.A30 Protection of the z/OS Trace Functions (S)

The trace functions of z/OS, such as GTF (generalised trace facility), NetView, or ACF/TAP (Advanced Communication Function/Trace Analysis Program) and the corresponding files, SHOULD be protected in such a way that only the responsible and authorised employees have access to them. The trace function of NetView SHOULD be disabled and only activated if required.

SYS.1.7.A31 Contingency Planning for z/OS Systems (S)

A procedure SHOULD be established for recovering a functioning RACF database. Furthermore, a copy of the z/OS operating system SHOULD be kept as a z/OS backup system and a z/OS business continuity system maintained separately from the production system.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

SYS.1.7.A32 Determining Standards for z/OS System Definitions (H)

Standards and naming conventions for z/OS system definitions SHOULD be defined and documented. The documentation SHOULD be made available to all administrators. Regular checks SHOULD be performed to ensure that the standards are being followed. Standards SHOULD be defined for file, database, job, and volume names in particular, as well as for application, system, and user IDs.

SYS.1.7.A33 Separation of Test and Production Systems in z/OS (H)

Technical measures SHOULD be taken to separate development and test systems from production systems in z/OS. Possible access options via shared hard disks and the Parallel Sysplex SHOULD be taken into account.

SYS.1.7.A34 Batch Job Planning for z/OS Systems (H)

If a z/OS system processes a large number of batch jobs, a job scheduler SHOULD be used for batch job flow control. The job scheduler and the associated files and tools SHOULD be suitably protected by RACF.

SYS.1.7.A35 Use of RACF Exits (H)

If RACF exits are used, the ramifications for technical security and operations SHOULD be analysed. RACF exits SHOULD also be installed and monitored via the SMP/E (System Modification Program/Enhanced) as USERMOD.

SYS.1.7.A36 Internal Communication Between Operating Systems (H)

Communication between operating systems—e.g. between z/OS and Linux, which are either installed in LPAR mode or under z/VM on the same Z hardware—SHOULD take place over internal channels (i.e. HiperSockets or virtual channel-to-channel (CTC) connections).

SYS.1.7.A37 Parallel Sysplex in z/OS (H)

Based on the availability and scalability requirements at hand, a decision SHOULD be taken as to whether a Parallel Sysplex (a cluster of z/OS systems) is to be used and, if so, what redundancies are planned. The requirements of applications SHOULD be taken into account when planning the capacity of the necessary resources. The software and the definitions of the LPARs of the Sysplex, including RACF, SHOULD be synchronised or provided as shared files.

It SHOULD be ensured that all the LPARs of the Sysplex can access the couple data sets. The couple data sets, as well as all security-critical programs and commands for managing the Sysplex, SHOULD be protected by RACF. A GRS (global resource serialisation) network SHOULD also be set up. The hard disks of the Sysplex SHOULD be strictly separated from the hard disks of other systems. The system logger SHOULD be used with staging data sets.

SYS.1.7.A38 Use of the VTAM Session Management Exit in z/OS (H)

If a VTAM session management exit is to be used, it SHOULD be ensured that it will not impair secure and efficient operations. At minimum, the exit SHOULD allow a subsequent check of a rejected login attempt. In addition, the exit SHOULD be configured dynamically and the set of rules loaded from an external file. Functions, commands, and files related to the exit SHOULD be protected by RACF.

4. Additional Information

4.1. Useful Resources

A number of abbreviations that are not explained elsewhere in IT-Grundschutz are commonly used in the Z system environment. These include:

- HMC (Hardware Management Console), MCS (Multiple Console Support), SMCS, Extended MCS: consoles for monitoring and controlling a Z system or z/OS operating system
- HFS: Hierarchical File System
- IPL: Initial Program Load, the startup procedure of an operating system
- RSF: Remote Support Facility
- SE: Support Elements, for system configuration and control
- SMP/E: System Modification Program/Extended, a software installation procedure
- zFS: zSeries File System, a file system used in z/OS and Unix System Services (USS)

IBM provides further information on the IBM Z in “ABC of z/OS System Programming Volume 1-13” (IBM Redbooks, https://www.redbooks.ibm.com).

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module SYS.1.7 *IBM Z*:

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

SYS.1.8 Storage Solutions

1. Description

1.1. Introduction

The constant growth of digital information and the increasing amount of unstructured information are prompting organisations to implement central storage solutions. The requirements for such storage solutions are subject to constant change; this can be seen, for example, in the following aspects:

- The data of an organisation should be available at any time and place for various application scenarios. This is why state-of-the-art storage solutions are often subject to more stringent availability requirements.
- The increasing digitalisation of all information within an organisation also makes it necessary to consider and comply with wide-ranging legal requirements (compliance).
- Storage solutions should be dynamically adaptable to the continuously changing requirements and able to provide storage space in a centralised manner.

In the past, storage solutions were often implemented by connecting storage media directly to a server. However, these direct-attached storage (DAS) systems often are no longer able to meet current and future requirements. This has led to the necessity for the central storage solutions commonly used today (and their components). They are differentiated as follows:

- Storage solution: This consists of one or several storage networks and at least one storage system.
- Storage network: This enables access to storage systems and the replication of data between storage systems.
- Storage system: a central instance that provides the other IT systems with storage space. A storage system also allows multiple IT systems to access the available storage space simultaneously.

1.2. Objective

The objective of this module is to show how central storage solutions can be planned, implemented, operated, and decommissioned in a secure manner.

1.3. Scoping and Modelling

Module SYS.1.8 *Storage Solutions* must be applied whenever central storage solutions are used. It can thus be applied to network-attached storage (NAS) systems, storage area networks (SAN) systems, hybrid storage, object storage, and cloud storage. However, the following must be taken into account:

- **Network-attached storage (NAS)** provides access to the storage systems using the protocols NFS (Network File System), AFP (Apple Filing Protocol), or CIFS (Common Internet File System), for example. The main application case is the provision of file server services. For NAS systems, the modules SYS.1.1 *General Server* and APP.3.3 *File Servers* must therefore be applied in addition to this module.
- **Storage area networks (SAN)** are generally created using a dedicated storage network between storage systems and connected IT systems. For SAN systems, it is therefore appropriate to consider module NET.1.1 *Network Architecture and Design*. Storage systems that can provide data via both NAS and SAN are often referred to as **hybrid storage** or combined storage systems (unified storage). For hybrid systems, the modules SYS.1.1 *General Server* and APP.3.3 *File Servers* must therefore be applied, as well. Module NET.1.1 *Network Architecture and Design* must also be appropriately considered.
- **Object storage** (often also referred to as **object-based storage**) allows for object-based access, in contrast to the traditional block-based and file-based access methods. A leading application is used to access object-based storage. Here, the application uses a specific interface (an application programming interface, or API) and its possible commands to access the object storage or access the storage directly via IP. For object-based storage solutions, module SYS.1.1 *General Server* must also be applied. In addition, security requirements must be taken into account that result from the use of web services. Web services are not considered in this module.
- In the context of further developments in the field of storage, the term **"cloud storage"** is becoming more and more established. This term refers to storage solutions as a basis for cloud services. In principle, the storage solution remains largely unchanged, but it accessed in a different way than with classic SAN or NAS architectures. Usually, this is implemented by means of a web service interface (via Representational State Transfer (REST) and Simple Object Access Protocol (SOAP)).

Backup devices connected to a storage system or a storage network are not addressed here; they are addressed in module OPS.1.2.2 *Archiving*. Design aspects of data backups are explained in module CON.3 *Backup Concept*.

A large number of user accounts can often access storage solutions. Therefore, storage solutions should be appropriately considered in roles and rights concepts. Requirements for this can be found in module ORP.4 *Identity and Access Management*.

If external service providers are used to operate a storage solution, the requirements of module OPS.2.1 *Outsourcing for Customers* must be taken into consideration separately.

2. Threat Landscape

For module SYS.1.8 *Storage Solutions*, the following specific threats and vulnerabilities are of particular importance.

2.1. Insecure Default Settings of Storage Components

Storage components are frequently delivered with a default configuration that makes it possible to commission the devices quickly and with as many functions as possible. Unnecessary protocols (such as HTTP, Telnet, and insecure SNMP versions) are thus enabled in many devices. If storage components with insecure factory settings are used in production environments, it is easier to access them without authorisation. This may result in services, for example, being no longer available or confidential information of the organisation being accessed without authorisation.

2.2. Manipulation of Data via the Storage System

Unwanted network connections can be established via a poorly configured storage area network (SAN). For example, if a server with an SAN connection can be accessed from the Internet and thus compromised from the outside, the server may be used as an entrance point for attackers in order to access sensitive information stored in the SAN without authorisation. Since all security and monitoring safeguards in the IT networks of an organisation (such as firewalls or intrusion detection systems (IDS)) may be bypassed this way, the potential for damage is high.

2.3. Loss of Confidentiality due to Storage-Based Replication Methods

The purpose of storage-based replication methods is to duplicate stored or archived data in real time via a storage network in order to achieve additional redundancy. This helps to avoid data losses. The automated replication of unencrypted data, however, entails risks both in an organisation's own network and when using public network providers. This way, unauthorised access to replication traffic is possible—for example, by means of FC analysers (FC replication) or sniffers (IP replication).

2.4. Access to Information of Other Clients Using WWN Spoofing

Devices in an FC-SAN are managed and assigned internally using world wide names (WWNs). They are similar in some ways to the MAC addresses of Ethernet network adapters. Using programs made available by the manufacturers of host bus adapters (HBA), the WWN of an HBA may be changed. An attacker may thus access data without corresponding authorisation. The manipulation of WWNs, also referred to as WWN spoofing, poses a considerable damage risk to an organisation. Particularly in connection with multi-client-capable storage systems, unauthorised persons may access the information of other clients.

2.5. Bypassing Logical Network Separation

If the network structures of different clients are separated by virtual storage area networks (VSANs) rather than by physically separate networks, the information security of the organisation in question may be endangered as a consequence. If an attacker manages to penetrate the network of another client, they may access the virtual SAN of this client and the payloads transferred.

2.6. Failure of Storage Solution Components

Complex network-based storage solutions often consist of many components (e.g. FC switches, storage controllers, and virtualisation appliances). If individual components of a storage solution fail, this may result in important applications no longer working properly and data being lost.

2.7. Obtaining Physical Access to SAN Switches

If the site and system access controls for the components of a storage system are insufficient or simply not in place in an organisation, it is possible for an attacker to gain physical access to existing switches or to connect additional FC-SAN switches to the network. The attacker may be seeking to access the distributed zoning database in order to change it and gain access to storage systems.

3. Requirements

The specific requirements of module SYS.1.8 *Storage Solutions* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Building Services

3.1. Basic Requirements

For module SYS.1.8 *Storage Solutions*, the following requirements MUST be met as a matter of priority:

SYS.1.8.A1 Appropriate Installation of Storage Systems [Building Services] (B)

The IT components of storage solutions MUST be installed in closed rooms. Access to these rooms MUST be restricted to authorised persons. In addition, a secure power supply MUST be

ensured. Manufacturer recommendations on ambient temperature and humidity MUST be observed.

SYS.1.8.A2 Secure Basic Configuration of Storage Solutions (B)

Prior to production use of a storage solution, it MUST be ensured that all the software components and firmware in use are up to date. Afterwards, a secure basic configuration MUST be established.

Unused interfaces of the storage system MUST be disabled. The files for the default configuration, the basic configuration performed, and the current configuration SHOULD be stored in a secure and redundant manner.

SYS.1.8.A3 ELIMINATED (B)

This requirement has been eliminated.

SYS.1.8.A4 Protection of Administration Interfaces (B)

All administration and management access to storage systems MUST be restricted. It MUST be ensured that it is not possible to access administration interfaces from untrustworthy networks.

Protocols that are considered secure SHOULD be used. If insecure protocols are nonetheless utilised, a separate administration network MUST be used (see NET.1.1 *Network Architecture and Design*).

SYS.1.8.A5 ELIMINATED (B)

This requirement has been eliminated.

3.2. Standard Requirements

For module SYS.1.8 *Storage Solutions*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

SYS.1.8.A6 Creation of a Security Policy for Storage Solutions (S)

Based on an organisation's general security policy, a specific policy SHOULD be drawn up for storage solutions. This policy SHOULD transparently describe specifications as to how storage solutions may be planned, administered, installed, configured, and operated securely.

The policy SHOULD be known to all administrators in charge of storage solutions and be integral to their work. If the policy is changed or deviations from its specifications are allowed, this SHOULD be coordinated with the CISO and documented. It SHOULD be checked regularly whether the policy is still being properly implemented. It SHOULD be updated as required. The results SHOULD be appropriately documented.

SYS.1.8.A7 Planning of Storage Solutions (S)

Before storage solutions are implemented in an organisation, a requirements analysis SHOULD be carried out. The requirements analysis SHOULD consider, among other things, the topics of performance and capacity. Based on the requirements identified, a detailed plan

for storage solutions SHOULD then be drawn up. The following items SHOULD be taken into account:

- selection of manufacturers and suppliers
- decision for or against central administration systems (management systems)
- planning of the network connection
- planning of the infrastructure
- integration into existing processes

SYS.1.8.A8 Selecting an Appropriate Storage Solution (S)

The technical fundamentals of different storage solutions SHOULD be examined in detail. The impact of these technical principles on an organisation's potential use of the solutions SHOULD be examined. The options and limits of the different storage system types SHOULD be illustrated in a transparent manner for the persons in charge in the organisation. The criteria for choosing a storage solution SHOULD be documented in a transparent manner. The decision regarding the selection of a storage solution SHOULD also be documented in a transparent manner.

SYS.1.8.A9 Selection of Suppliers for a Storage Solution (S)

Based on the specified requirements an organisation's storage solution needs to meet, an appropriate supplier SHOULD be selected. The selection criteria and the decision in favour of a supplier SHOULD be documented in a transparent manner. Furthermore, maintenance and repair aspects SHOULD be documented in writing in service level agreements (SLAs). The SLAs SHOULD be unambiguous and quantifiable. The exact scheduled end of the contract with the supplier SHOULD be established in writing.

SYS.1.8.A10 Drawing Up and Maintaining an Operating Manual (S)

An operating manual SHOULD be drawn up. It SHOULD document all the rules, requirements, and settings for operating storage solutions. The operating manual SHOULD be updated at regular intervals.

SYS.1.8.A11 Secure Operation of a Storage Solution (S)

Storage systems SHOULD be monitored in terms of the availability of internal applications, system load, and critical events. Furthermore, fixed maintenance windows in which changes may be implemented SHOULD be defined for storage solutions. In particular, firmware or operating system updates to storage systems or the network components of a storage solution SHOULD only be performed within a maintenance window.

SYS.1.8.A12 ELIMINATED (S)

This requirement has been eliminated.

SYS.1.8.A13 Monitoring and Administration of Storage Solutions (S)

Storage solutions SHOULD be monitored. All collected data (messages) SHOULD be checked, in particular to see if the specifications of the respective operating manual are being followed.

Essential messages SHOULD be highlighted using message filters. Individual components of storage solutions and the respective overall systems SHOULD be managed in a centralised manner.

SYS.1.8.A14 Protection of an SAN Through Segmentation (S)

An SAN SHOULD be segmented. A concept SHOULD be drawn up that assigns SAN resources to the respective servers. To this end, a decision SHOULD be taken as to which segmentation should be used in each implementation (e.g. FC SANs or iSCSI storage networks) based on the security requirements at hand and the administration effort required. The current resource allocation SHOULD be easily and clearly identifiable with the help of the administration tools. Furthermore, the current zoning configuration SHOULD be documented. The documentation SHOULD also be available in case of emergency.

SYS.1.8.A15 Secure Separation of Clients in Storage Solutions (S)

An organisation's requirements regarding the multi-client capability of a storage solution SHOULD be defined and documented in a transparent manner. The storage solutions used SHOULD meet these documented requirements.

In block storage environments, LUN masking SHOULD be used in order to separate clients. In file service environments, it SHOULD be possible to use virtual file servers. Here, every client SHOULD be assigned its own file service.

When using IP or iSCSI, clients SHOULD be separated via segmentation within the network. If fibre channel is being used, VSANs and soft zoning SHOULD be used for segmentation purposes.

SYS.1.8.A16 Secure Deletion in SAN Environments (S)

In multi-client-capable storage systems, it SHOULD be ensured that the logical unit numbers (LUNs) assigned to a certain client are deleted.

SYS.1.8.A17 Documenting Storage System Settings (S)

All storage system settings SHOULD be documented. The documentation SHOULD include the technical and organisational specifications in question, as well as any specific configurations of an organisation's storage systems.

If the documentation of system settings includes confidential information, this information SHOULD be protected against unauthorised access. The documentation SHOULD be regularly reviewed. It SHOULD always be up to date.

SYS.1.8.A18 Security Audits and Reporting Storage Systems (S)

All storage systems used SHOULD be audited at regular intervals. A corresponding process SHOULD be established. It SHOULD be specified what security reports are to be drawn up at regular intervals and what they are to contain. Furthermore, it SHOULD also be specified how deviations from specifications must be handled and how often and to what extent audits are to be performed.

SYS.1.8.A19 Decommissioning Storage Solutions (S)

If entire storage solutions or individual components thereof are no longer required, any data they contain SHOULD be transferred to other storage solutions. A transitional phase SHOULD be scheduled for this. Afterwards, all payload and configuration data SHOULD be securely deleted. Any references to the decommissioned storage solution SHOULD be removed from any relevant documents.

SYS.1.8.A20 Contingency Planning and Emergency Response for Storage Solutions (S)

A business continuity plan for the storage solution deployed SHOULD be drawn up. The business continuity plan SHOULD include an accurate description of the steps to take in certain emergency situations. Instructions in the form of safeguards and commands that support error analysis and error correction SHOULD be included, as well. In order to remedy errors, appropriate tools SHOULD be used.

Regular drills and tests SHOULD be conducted using the business continuity plan. The data generated during the drills and tests and after an actual emergency SHOULD be deleted securely afterwards.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.1.8 *Storage Solutions* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.1.8.A21 Use of Storage Pools in Client Separation (H)

Clients SHOULD be assigned storage resources from different storage pools. In this process, a storage medium SHOULD only be assigned to one pool at a time. The logical hard disks (LUNs) generated from such a pool SHOULD only be assigned to a single client.

SYS.1.8.A22 Use of a High Availability SAN Solution (H)

A highly available SAN solution SHOULD be used. The replication mechanisms used SHOULD meet the availability requirements of the organisation in question regarding its storage solution. The configuration of the storage solution SHOULD also meet the availability requirements. Furthermore, there SHOULD be a test and consolidation system.

SYS.1.8.A23 Use of Encryption for Storage Solutions (H)

All data stored in storage solutions SHOULD be encrypted. The levels at which encryption is to be performed SHOULD be defined (regarding data in motion and data at rest). In this process, it SHOULD be ensured that the encryption along the transport channel is also relevant for replications and backup traffic.

SYS.1.8.A24 Ensuring the Integrity of the SAN Fabric (H)

In order to ensure the integrity of the SAN fabric, protocols with additional security features SHOULD be used. The security features of the following protocols SHOULD be taken into consideration and corresponding configurations SHOULD be used:

- Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP)
- Fibre Channel Authentication Protocol (FCAP)
- Fibre Channel Password Authentication Protocol (FCPAP)

SYS.1.8.A25 Multiple Overwrites of LUN Data (H)

In SAN environments, data SHOULD be deleted by overwriting the related storage segments of a LUN several times.

SYS.1.8.A26 Securing a SAN with Hard Zoning (H)

In order to segment SANs, hard zoning SHOULD be used.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for securing storage solutions in the standard ISO/IEC 27040:2015, “Information Technology – Security Techniques – Storage Security”.

The Information Security Forum (ISF) provides guidelines for securing storage solutions in section SY1.4 ("Network Storage Systems") of “The Standard of Good Practice for Information Security”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.1.8 *Storage Solutions*.

G 0.2 Unfavourable Climatic Conditions

G 0.8 Failure or Disruption of the Power Supply

G 0.11 Failure or Disruption of Service Providers

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

SYS.2.1 General Client

1. Description

1.1. Introduction

The term “general client” refers to an IT system running any operating system that allows the separation of users and is not used to provide server services. On a client, it should be possible to configure at least an administrator environment and a user environment. The underlying IT system generally has drives and connection options for external and removable storage media, additional interfaces for data exchange, and other peripheral devices. An IT system of this kind is typically integrated into a client-server network. The IT system can, for example, be a PC with or without a hard drive, a mobile or stationary device, a Linux workstation, or an Apple Mac.

1.2. Objective

The objective of this module is to protect information that is created, read, processed, stored, or sent on any type of client, regardless of the operating system used.

1.3. Scoping and Modelling

SYS.2.1 *General Client* must be applied to all clients regardless of the specific operating system at hand.

As a rule, clients run in an operating system that requires its own security safeguards. For common client operating systems, specific modules are available in the SYS.2 *Desktop Systems* layer that are based on this module and also need to be applied. If there is no specific module for the clients used in a particular case, the requirements of this module must be adapted and extended appropriately. Security recommendations for mobile devices with fixed operating systems (such as smartphones or tablets) can be found in the SYS.3 *Mobile Devices* layer.

If a client has further interfaces for exchanging data (e.g. USB, Bluetooth, LAN, or WLAN), they need to be protected in line with the respective organisation’s security policies as described in the corresponding modules. Requirements for this can be found in SYS.4.5 *Removable Media* or NET.2.2 *WLAN Usage*, for example.

The requirements of module CON.3 *Backup Concept* must also be taken into account for clients. Since clients are often threatened by malware, the requirements of OPS.1.1.4 *Protection Against Malware* for clients must be taken into account.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module SYS.2.1 *General Client*, the following specific threats and vulnerabilities are of particular importance.

2.1. Malware

Malware is developed with the goal of executing unwanted and malicious functions on IT systems. In most cases, it becomes active without the awareness or consent of users. Depending on its form, malware may provide an attacker with extensive communication and control options with an array of different functions. Among other things, it can be specifically used to read passwords, remotely control IT systems, disable protective software, and steal or encrypt data.

Clients are particularly vulnerable to malware. They are operated directly by users and are thus often a gateway for malicious content of any kind. If users visit malicious websites, open e-mails with malicious content from private accounts, or copy malware via local storage media to their clients, malware can spread via the clients into the respective organisation's network. Central protection mechanisms, such as virus protection on a file or e-mail server, can often be bypassed in this way.

2.2. Data Loss Due to Local Data Storage

Despite regular recommendations to the contrary, many users only save important data locally. For example, data is often stored in local user directories instead of on a central file server. E-mails are often only archived locally, as well. Data can then be easily lost in the event of hardware defects, for example. If data important to an organisation is destroyed or falsified, business processes can be delayed or even thwarted altogether. Overall, the loss of stored data can lead to unproductive time and additional costs of recovery, and especially to long-term consequences such as a loss of trust among customers and partners or a negative public image. In extreme cases, the direct and indirect damage caused by a loss of data can threaten the existence of an organisation.

Moreover, if important data is only kept locally, other users cannot access it—for example, if someone is standing in for a colleague who is ill or on holiday.

Even when basic specifications for central storage are observed, however, additional local copies of centrally stored data are often made. In addition to inconsistent versions of data, this often leads to data being deleted hastily or not being deleted as required.

2.3. Hardware Defects in Client Systems

Unlike in the case of central IT systems such as servers, client users work directly on their end devices. As a result, they might damage their clients intentionally or unintentionally. For example, they could kick IT systems standing on the floor, trip over cables and damage interfaces, or spill liquids onto devices. If no quick replacement is available, the user in question will not be able to work with the IT system affected until repairs are completed. If a mobile device such as a laptop fails while the user is on the move, they are often only able to continue working after returning to their organisation.

2.4. Unauthorised Use of IT

The identification and authentication of users is intended to prevent a client from being used in an unauthorised manner. However, IT systems in which users are required to identify and authenticate themselves via user IDs and passwords can also be used in an authorised manner if an attacker succeeds in obtaining or guessing access data. If no screen lock is activated, it is also possible for a client to be used in an unauthorised manner, even during a short absence.

2.5. Installation of Unnecessary Operating System Components and Applications

When installing an operating system, there is generally the option to remove optional software. Software is also regularly installed and tested during live operations. Each additional application increases the computing and memory load of a client, along with the probability of vulnerabilities arising. Software that is not required is often not subject to regular patch management, which means that even known vulnerabilities are not rectified promptly. Attackers can exploit such vulnerabilities.

2.6. Eavesdropping on Rooms Using Microphones and Cameras

Many clients are equipped with a microphone and camera. In principle, these devices can be activated and used by anyone who has corresponding access rights—including external parties in the case of networked systems. If these rights are not carefully assigned, unauthorised persons can manipulate a microphone or camera to eavesdrop on rooms or record meetings unnoticed via the Internet. This also includes intelligent personal assistants (IPAs) or voice assistants, which constantly listen to their environment and carry out functions such as playing music, calling contacts, controlling lighting, or changing the room temperature when they hear device-dependent code words. If conversations are transmitted to third parties (e.g. by IPAs), they could be intercepted by unauthorised persons. Recorded conversations could also be stored and processed further by the operators of an IPA for a longer period of time.

2.7. Incorrect Administration or Use of Devices and Systems

Modern client operating systems are very complex. Therefore, the misconfiguration of components in particular can compromise security so that IT systems function incorrectly or may be compromised. In general, each interface on an IT system not only provides the opportunity to use certain services of the IT system in an authorised manner, but also carries

the risk of the IT system being accessed without authorisation. For example, if incorrectly configured authentication mechanisms make it possible to obtain user IDs and the corresponding passwords, the applications or IT systems in question may be used in an unauthorised manner.

Incorrect or improper use of devices, systems, and applications may also jeopardise security, especially if existing security safeguards are ignored or bypassed. Security incidents can occur, for instance, when access rights are granted too liberally, passwords are easy to guess, storage media containing backup copies are inadequately protected, or workstations are not locked during temporary periods of absence. Another possible consequence of the incorrect operation of IT systems or applications involves the accidental deletion or modification of data. It is also possible for confidential information to fall into the hands of third parties if access rights are set incorrectly (for example).

3. Requirements

The specific requirements of module SYS.2.1 *General Client* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	User, Building Services

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

The following requirements MUST be met for this module as a matter of priority.

SYS.2.1.A1 Secure User Authorisation (B)

In order to use a client, users MUST be authenticated by the corresponding IT system. Users MUST use a screen lock when leaving their clients running without supervision. The screen lock SHOULD be activated automatically if no action has been taken by the user for a set period of time. Successful user authentication MUST be the only way to disable a screen lock. Users SHOULD be required to log out of IT systems and applications after completing their tasks.

SYS.2.1.A2 ELIMINATED (B)

This requirement has been eliminated.

SYS.2.1.A3 Activation of Automatic Update Mechanisms (B)

Automatic update mechanisms MUST be activated unless other mechanisms (such as regular manual maintenance or a central software distribution system) are used for updates. If a time interval can be specified for auto-update mechanisms, there SHOULD be an automatic search for updates at least daily and they SHOULD be installed when found.

SYS.2.1.A4 ELIMINATED (B)

This requirement has been eliminated.

SYS.2.1.A5 ELIMINATED (B)

This requirement has been eliminated.

SYS.2.1.A6 Using Malware Protection Programs (B)

Depending on the operating system installed and other protection mechanisms of a given client, it MUST be checked whether malware protection programs should be used. Where available, concrete statements from the operating system modules of the IT-Grundschutz Compendium on whether such virus protection is necessary MUST be considered.

Protection programs on clients MUST be configured so that users cannot disable such programs or make any security-relevant changes to their settings.

Protection programs MUST search for malware when files are exchanged or transmitted. All the data on clients MUST be checked regularly for malware. If a client is infected, it MUST be examined in offline mode to determine whether the detected malware has already collected confidential data, disabled any protective functions, or downloaded any code from the Internet, for example.

SYS.2.1.A7 ELIMINATED (B)

This requirement has been eliminated.

SYS.2.1.A8 Protecting the Boot Process (B)

The start-up procedure (boot process) of IT systems MUST be protected against manipulation. The media that can be used to boot a given system MUST be defined. A decision SHOULD be taken as to whether and how the boot process is to be protected cryptographically. It MUST be ensured that only administrators can boot clients from anything other than the default drive, or from an external storage medium. The ability to boot IT systems from removable or external storage media MUST be restricted to administrators. The ability to change the configuration settings of boot processes MUST also be restricted to administrators. All unused functions in firmware MUST be disabled.

SYS.2.1.A42 Use of Cloud and Online Functions [User] (B)

The use of the cloud and online functions of client operating systems MUST be restricted to those absolutely required. Necessary cloud and online functions SHOULD be documented. The corresponding settings of the operating system at hand MUST be checked for conformity with organisational data protection and security specifications and be configured restrictively; otherwise, such functions MUST be disabled.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

SYS.2.1.A9 Defining a Security Policy for Clients (S)

On the basis of an organisation's general security policy, requirements for general clients SHOULD be specified. The policy SHOULD be known to all users and all persons involved in the procurement and operation of clients and be integral to their work. The implementation of the policy's requirements SHOULD be checked at regular intervals. The results SHOULD be documented in a transparent manner.

SYS.2.1.A10 Planning the Use of Clients (S)

Where and how clients are to be used SHOULD be planned in advance. This planning SHOULD not only address aspects typically associated directly with information security, but also operational aspects that entail requirements in the area of security. All decisions taken in the planning phase SHOULD be documented in such a way that they can be understood at any future point in time.

SYS.2.1.A11 Procurement of Clients (S)

Before clients are procured, a requirements list SHOULD be drawn up that can be used to evaluate the products available on the market. The manufacturers of IT and operating systems SHOULD be expected to provide patches for vulnerabilities promptly throughout the planned duration of use. The systems to be procured SHOULD have a firmware configuration interface for UEFI SecureBoot and for TPM (if available), which allows for control by the owner (organisation) and thereby facilitates the self-managed operation of SecureBoot and TPM.

SYS.2.1.A12 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.1.A13 Access to Runtime Environments with Unmonitored Code Execution (S)

Access to runtime environments with unmonitored code execution (storage areas specifically secured by the operating system, firmware areas, etc) SHOULD only be granted to users with administrative rights. The corresponding settings in the BIOS or the UEFI firmware SHOULD be protected against unauthorised changes by a password. If control of the functions in question is delegated to the operating system, the ability to access the functions there SHOULD be restricted to users with administrative authorisations.

SYS.2.1.A14 Updates and Patches for Firmware, Operating Systems, and Applications (S)

Operating systems that are updated via a rolling release model SHOULD be avoided. Only application programs for which support is offered SHOULD be selected and installed. Operating systems, application programs, and firmware for which regular security updates are not offered MUST NOT be used.

SYS.2.1.A15 Secure Installation and Configuration of Clients (S)

Operating system components, specialised applications, and other tools to be installed SHOULD be specified. The installation and configuration of IT systems SHOULD only be performed by authorised persons (administrators or service providers bound by contract) according to a defined installation process in a specific installation environment. After installation and configuration have been completed, the basic settings SHOULD be checked. Provided that the installation and configuration meet the requirements of the security policy at hand, the clients SHOULD then be put into operation in the respective production environment. All installation and configuration steps SHOULD be documented in such a way that they can be understood and repeated by a competent third party.

SYS.2.1.A16 Disabling and Removing Unnecessary Components and IDs (S)

Firmware and operating system components, applications, and other tools that are installed and activated on clients SHOULD be checked after installation. Unnecessary modules, programs, services, tasks, and firmware functions (like remote maintenance) SHOULD be disabled or removed. Unnecessary runtime environments, interpreter languages, and compilers should also be removed. Unnecessary user IDs SHOULD be disabled or deleted. Unnecessary interfaces and IT system hardware (like webcams) SHOULD be disabled. The reactivation of these components SHOULD be prevented. The decisions taken in this regard SHOULD be documented in a comprehensible manner.

SYS.2.1.A17 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.1.A18 Using Encrypted Communication (S)

Communication SHOULD be protected by encryption whenever possible.

Clients SHOULD use cryptographic algorithms and key lengths that conform to the current state of the art and meet the security requirements of the organisation in question.

New certificates from certificate issuers SHOULD only be used after their fingerprints are checked.

SYS.2.1.A19 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.1.A20 Protecting the Administration Process for Clients (S)

Adequate security precautions SHOULD be taken based on whether clients are administrated locally or via a network. The procedures used for administration SHOULD conform to the specifications of the applicable security policy.

SYS.2.1.A21 Preventing Unauthorised Use of Computer Microphones and Cameras (S)

Access to a client's microphone and camera SHOULD only be available to the users themselves while they are working locally on the corresponding IT system. If a microphone or camera is not used and its misuse is to be prevented, it SHOULD be switched off, covered (camera only), disabled, or physically disconnected from the respective device whenever possible. Rules

SHOULD be specified on how cameras and microphones in clients are to be used and how the related rights are to be assigned.

SYS.2.1.A22 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.1.A23 Preferences for Client-Server Services (S)

If possible, dedicated server services for exchanging information SHOULD be used and direct connections between clients avoided. If this is not possible, it SHOULD be specified which client-to-client services (often also referred to as peer-to-peer services) may be used and which information may be exchanged through them. If necessary, users SHOULD be trained in the use of such services. Direct connections between clients SHOULD be restricted to the respective LAN. Auto-discovery protocols SHOULD be restricted to those required.

SYS.2.1.A24 Dealing with External and Removable Media (S)

Interfaces to external networks SHOULD ONLY be accessible in a restricted manner. Connecting unauthorised devices or removable media to clients SHOULD be prohibited. Clients SHOULD generally be prevented from accessing removable media from untrusted sources. The unauthorised execution of programs on or from external storage media SHOULD be technically prevented. Copying unauthorised data from clients via removable drives or external interfaces SHOULD be prevented.

SYS.2.1.A25 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.1.A26 Protection Against Exploitation of Vulnerabilities in Applications (S)

To make it more difficult to exploit vulnerabilities, ASLR and DEP/NX SHOULD be activated in operating systems and used by applications. Security functions of kernels and standard libraries, such as heap and stack protection, SHOULD be activated.

SYS.2.1.A27 Orderly Decommissioning of Clients (S)

When decommissioning a client, it SHOULD be ensured that no data is lost and no sensitive data remains. There SHOULD be an overview of the data stored on IT systems, along with the respective locations. A checklist which can be completed when decommissioning an IT system SHOULD be created. This checklist SHOULD, at minimum, include aspects of backing up data that is still needed and the subsequent secure deletion of all data.

SYS.2.1.A34 Encapsulation of Security-Critical Applications and Operating System Components (H)

In order to prevent an attacker from accessing the operating system or other applications and prevent access from the operating system to files that are particularly sensitive, applications and operating system components (such as authentication or certificate verification) SHOULD be specially encapsulated according to their protection needs or isolated from other applications and operating system components. Particular attention SHOULD be paid to

security-critical applications that work with data from insecure sources (e.g. web browsers and office communication applications).

SYS.2.1.A43 Local Security Policy for Clients (S)

All security-relevant settings SHOULD be configured, tested, and regularly checked as needed. To this end, security policies SHOULD be configured that take into account the recommendations of the respective operating system manufacturer and the client's default behaviour, provided that this behaviour does not contradict other requirements of IT-Grundschutz or the organisation in question. The decisions taken in this regard SHOULD be documented and justified. Security policies SHOULD be defined in any case, even if the client's default behaviour is not changed.

SYS.2.1.A44 Client Security Policy Management (S)

All client settings SHOULD be administered using a management system and configured according to the identified protection needs and the internal policies at hand. Configuration changes SHOULD be documented, justified, and coordinated with the relevant security management personnel so that they can be carried out quickly and distributed in a centralised manner. It SHOULD also be possible to trace the status of security configurations at any time.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

SYS.2.1.A28 Encryption of Clients (H)

If confidential information is stored on clients, at least the sensitive files and select areas of the file system—or better yet, all storage media—SHOULD be encrypted. A separate concept SHOULD be developed for this and special care should be taken when documenting the details of the configuration. In this context, authentication (by means of passwords, PINs, tokens, etc), the storage of recovery information, the drives to be encrypted, and the write permissions to unencrypted media SHOULD be regulated. Access to the key material used MUST be adequately protected.

Users SHOULD be informed of the steps they should take if they lose authentication resources.

SYS.2.1.A29 System and Client Monitoring (S)

Clients SHOULD be integrated into a suitable system monitoring concept that continuously monitors their system status and functionality while also reporting error conditions and any threshold violations to the respective operating personnel.

SYS.2.1.A30 Setting Up a Reference Environment for Clients (H)

A reference installation SHOULD be set up for clients in which basic configurations and all configuration changes, updates, and patches can be tested before they are installed on clients. Checklists SHOULD be created for various typical and frequently recurring test cases which should be processed as automatically as possible during test runs. The test cases SHOULD take

into account both the user and the operational perspective. In addition, all tests SHOULD be documented in such a way that they can be reconstructed at a later point in time.

SYS.2.1.A31 Configuring Local Packet Filters (H)

In addition to the central security gateways used, local packet filters SHOULD be used on all clients. A packet filter implementation strategy SHOULD be selected that explicitly only allows network communication that is necessary.

SYS.2.1.A32 Use of Additional Safeguards to Protect Against Exploits (H)

Additional safeguards SHOULD be implemented on clients as explicit protection against exploits of system vulnerabilities. If necessary security safeguards cannot be implemented via operating system functions, additional suitable security safeguards SHOULD be implemented. If it is not possible to implement sustainable safeguards, other suitable (generally organisational) security safeguards SHOULD be implemented.

SYS.2.1.A33 Using Execution Control (H)

Execution control SHOULD be used to ensure that only explicitly authorised programs and scripts can be executed. The rules SHOULD be set as restrictively as possible. If explicit specification of paths and hashes is not possible, certificate-based or path rules SHOULD be used as an alternative.

SYS.2.1.A35 Active Administration of Root Certificates (H)

As part of the procurement and installation of clients, the root certificates required for their operation SHOULD be documented. Only the previously documented root certificates required for operation SHOULD be present on clients. Regular checks SHOULD be performed as to whether existing root certificates still comply with the respective organisation's requirements. All certificate stores available on an IT system (e.g. UEFI certificate stores, certificate stores of web browsers) SHOULD be included in these checks.

SYS.2.1.A36 Self-Managed Use of SecureBoot and TPM (H)

On UEFI-compatible systems, the bootloader, kernel, and all required firmware components SHOULD be signed by self-controlling key material, and any key material that is not required SHOULD be removed. If Trusted Platform Module (TPM) is not required, it SHOULD be disabled.

SYS.2.1.A37 Use of Multi-Factor Authentication (H)

Secure authentication involving multiple different factors (knowledge, possession, property) SHOULD be established for logging into clients locally (e.g. using a password with a chip card or token).

SYS.2.1.A38 Integration into Contingency Planning (H)

Clients SHOULD be taken into account in business continuity management processes. Clients SHOULD be prioritised for restoration of service in terms of the business processes or specialised tasks for which they are needed. At minimum, suitable business continuity safeguards SHOULD be implemented by drawing up recovery plans, generating boot media for system recovery, and securely storing passwords and cryptographic keys.

SYS.2.1.A39 Stable and Uninterruptible Power Supply [Building Services] (H)

Clients SHOULD be connected to an uninterruptible power supply (UPS). The UPS SHOULD have sufficient capacity in terms of its output power and backup time. Clients SHOULD be protected against overvoltage.

SYS.2.1.A40 Operational Documentation (H)

The performance of operational tasks on clients or groups of clients SHOULD be documented in a transparent manner with regard to who has done what and when. In particular, the documentation SHOULD make configuration changes transparent. Security-relevant responsibilities (e.g. who is authorised to install new hard disks) SHOULD also be documented. Everything that can be documented automatically SHOULD be documented automatically. The documentation SHOULD be protected from unauthorised access and loss. Security-relevant aspects SHOULD be explained and highlighted in a transparent way.

SYS.2.1.A41 Use of Quotas for Local Media (H)

Consideration SHOULD be given to setting up quotas that limit the space used on local disks. As an alternative, mechanisms of the file or operating system in question should be used that warn users if the hard drive capacity reaches a specific level or only grant write privileges to the system administrator.

SYS.2.1.A45 Extended Logging (H)

Client behaviour that is not directly related to security SHOULD also be logged and immediately evaluated (in an automated way) to detect covert attacker activity.

4. Additional Information

4.1. Useful Resources

No further information is available for module SYS.2.1 *General Client*.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module SYS.2.1 *General Client*:

G 0.8 Failure or Disruption of the Power Supply

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.40 Denial of Service

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

SYS.2.2.2 Windows 8.1 Clients

1. Description

1.1. Introduction

In Windows 8, Microsoft presented a further development of its client operating system and the features and components introduced with it. One new feature of Windows 8 (or 8.1) is a user interface that is geared towards the use of mobile devices with touch screens. This brings with it a new operating concept for applications: In addition to classic desktop applications, Microsoft has provided for a class of mobile applications, or simply "apps". These apps are primarily designed to be controlled by touch. In addition, they can perform display functions as “tiles” on screen. Some applications—above all Internet Explorer, which comes with Windows 8.1—are available in two versions: the familiar desktop version and a new app version. Windows 10 is a successor to Windows 8.1. Microsoft's extended support for Windows 8.1 is scheduled to end on 10 January 2023.

1.2. Objective

The objective of this module is to protect information that is processed in Windows 8.1, including by corresponding clients.

1.3. Scoping and Modelling

Module SYS.2.2.2 *Windows 8.1 Clients* must be applied to all client systems on which the Microsoft Windows 8.1 operating system is used.

This module describes requirements specific to Windows 8.1. The requirements of module SYS.2.1 *General Client* must also be met. For application programs used on Windows clients, the requirements of the corresponding modules must be fulfilled—for example, from APP.1.1 *Office Products* or APP.1.2 *Web Browsers*. When being used in a Windows domain, the requirements of corresponding modules such as APP.2.2 *Active Directory* must be met.

2. Threat Landscape

For module SYS.2.2.2 *Windows 8.1 Clients*, the following specific threats and vulnerabilities are of particular importance:

2.1. Malware Designed for Windows

Since Microsoft Windows is a popular target for a wide variety of attacks due to its widespread use, malware presents a high level of danger. Malware can have many different functions and thus offer an attacker extensive communication and control options. Among other purposes, malware may be used to obtain specific passwords, control systems remotely, disable protective software, and collect data without authorisation. The damage caused by the loss or corruption of information or applications is particularly serious for an organisation. However, the reputational and financial damage that can result from malware are often also severe.

2.2. Integrated Cloud Functions

Windows 8.1 includes numerous features that are used to store and synchronise data in the cloud services of Microsoft. Here, there is the risk that this will result in the unwitting (or at least careless) use of cloud services in connection with data that is personal or critical for a given organisation. Users who store data with third parties (especially those located abroad) may also find themselves in violation of data protection laws. If a user logs into a new device using an already activated Microsoft account, the Microsoft cloud services utilised by the user will be set up automatically on the device. An organisation's data may thus be synchronised accidentally to the private devices of employees. As another example, Windows 8.1 offers the default option to back up BitLocker recovery keys directly to the cloud via one's Microsoft account. This puts sensitive encrypted information into the hands of third parties.

2.3. Impairment of Software Features due to Compatibility Issues

Software that has been successfully operated on previous versions of Windows will not necessarily work automatically with the current version of the operating system. Possible reasons for this may include new security features or operating system properties, as well as the discontinuation of functions or services. As a result, the use of certain software may be limited or impossible. In new Windows versions, activating new security features (for example) may result in compatibility issues. Examples of this include User Account Control (UAC), or Kernel Patch Guard in 64-bit versions of the operating system. In addition, signed drivers may be necessary, but not available for older devices. Functions are also regularly omitted from newer versions of Windows. One example involves the discontinuation of the GINA login component, which was used by several fingerprint readers.

3. Requirements

The specific requirements of module SYS.2.2.2 *Windows 8.1 Clients* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The

Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	User

3.1. Basic Requirements

For module SYS.2.2.2 *Windows 8.1 Clients*, the following requirements MUST be implemented as a matter of priority:

SYS.2.2.2.A1 Selecting a Suitable Windows 8.1 Version (B)

Before proceeding with procurement, a suitable version of Windows 8.1 MUST be selected that has all the necessary features for future use. Priority SHOULD be given to 64-bit versions that include advanced security features.

SYS.2.2.2.A2 Defining a Login Procedure for Windows 8.1 (B)

Depending on the security requirements at hand, it MUST be decided whether other mechanisms such as PINs are to be allowed in addition to the conventional login process using a password.

SYS.2.2.2.A3 Use of Virus Protection Programs with Windows 8.1 (B)

Unless equivalent or higher-order safeguards have been implemented to protect an IT system from malware, an anti-virus program must be used on Windows 8.1 clients.

3.2. Standard Requirements

For module SYS.2.2.2 *Windows 8.1 Clients*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

SYS.2.2.2.A4 Procurement of Windows 8.1 (S)

When procuring Windows 8.1 or corresponding hardware for a Windows 8.1 system, the applicable Windows Hardware Certification requirements SHOULD be taken into account. Furthermore, the systems to be procured SHOULD have a firmware configuration interface for UEFI SecureBoot and, if available, for the TPM, which enables control by the owner. In addition, an appropriate licensing model SHOULD be selected.

SYS.2.2.2.A5 Local Security Policy for Windows 8.1 (S)

All security-relevant settings SHOULD be configured, tested, and checked regularly as needed using appropriate security policies. The distribution of security settings to several Windows 8.1 clients SHOULD be performed in accordance with the specific circumstances of the organisation in question.

SYS.2.2.2.A6 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.2.2.A7 Use of Windows User Account Control (S)

In order to support restrictive rights assignment, User Account Control (UAC) SHOULD be enabled. For standard users, it SHOULD be defined that password prompts will be rejected automatically for higher rights. For administrator accounts, a balance between user-friendliness and security SHOULD be achieved when configuring UAC. This decision SHOULD be documented and the corresponding settings SHOULD be configured. It SHOULD be checked regularly whether the corresponding rights are still required and whether they should be adapted or withdrawn accordingly.

SYS.2.2.2.A8 No Use of the Homegroup Feature [User] (S)

Clients SHOULD NOT offer services such as file or printer sharing. A security policy or Group Policy Object (GPO) with the setting "Prevent the computer from joining a homegroup" SHOULD apply to all clients. If the feature is being used for internal reasons, the users SHOULD be trained in handling the approvals the homegroup.

SYS.2.2.2.A9 Data Protection and Data Economy in Windows 8.1 Clients [User] (S)

If Microsoft accounts are created for users, only the personal information absolutely required SHOULD be entered. The SmartScreen feature, which checks files and web content downloaded from the Internet and transmits personal data to Microsoft in the process under certain circumstances, SHOULD be disabled. Before an application or app is approved for use within an organisation, the data it automatically sends to the Microsoft cloud SHOULD be checked carefully. Applications SHOULD be configured in such a way that no sensitive data is transmitted. Apps that transmit data to third parties in an unwanted or unnecessarily extensive way SHOULD NOT be used.

SYS.2.2.2.A10 Integration of Online Accounts into the Operating System [User] (S)

Logging into an IT system and domain SHOULD only be possible using an account of a self-operated directory service (e.g. Active Directory). The ability to log in locally SHOULD be reserved for administrators. If online accounts such as a Microsoft account or accounts from other identity management service providers are used to log in, care SHOULD be taken to ensure that the respective provider is trustworthy and that data protection is respected.

SYS.2.2.2.A11 Configuration of Synchronisation Mechanisms in Windows 8.1 (S)

The synchronisation of user data with Microsoft cloud services SHOULD be disabled completely.

SYS.2.2.2.A12 Secure Central Authentication of Windows Networks (S)

In Windows-only networks, only Kerberos SHOULD be used for central authentication for Single Sign On (SSO). A group policy SHOULD prevent the use of older protocols. The protection of the Local Credential Store (LSA) SHOULD be activated (PPL, Protected Mode

Light). The storage of LAN Manager hash values when changing passwords SHOULD be disabled based on a group policy. The monitoring settings SHOULD be aligned carefully with the requirements of the information domain in question together with the server components of DirectAccess. Client-side logging SHOULD be ensured.

SYS.2.2.2.A13 Connection of Windows 8.1 to the Microsoft Store (S)

The ability to install apps from the Microsoft Store SHOULD be disabled if it is not needed.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.2.2.2 *Windows 8.1 Clients* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.2.2.2.A14 Application Control Using Software Restriction Policies and AppLocker (H)

Applications in paths for which users have write privileges SHOULD be prevented from being executed by software restriction policies (SRP) or AppLocker. In a domain-based network, AppLocker and SRP GPO SHOULD ONLY be managed centrally by means of Group Policy Objects for each user and user group.

AppLocker SHOULD be used in a whitelist approach, meaning that all applications that are not explicitly allowed SHOULD be prohibited. Preference SHOULD be given to rules based on the application signatures of defined publishers. Attempted violations of the rules SHOULD be logged and evaluated appropriately.

For clients with particularly high security requirements, AppLocker SHOULD prevent the execution of any unapproved applications (instead of merely logging them).

The SRP and AppLocker rules SHOULD be tested on a test system or by means of operation in monitoring mode before being used on a production system.

SYS.2.2.2.A15 File System Encryption Using EFS (H)

In case of increased protection needs, file systems SHOULD be encrypted. If the Encrypting File System (EFS) is used in this regard, a complex password SHOULD be used to protect the data encrypted using EFS. Files encrypted with EFS SHOULD also be protected by restrictive access rights. The recovery agent SHOULD be a dedicated account and not the administrator account. The private key of this account SHOULD be outsourced to an external storage medium, stored securely, and removed from the corresponding system. In this context, backups of all private keys SHOULD be created. When using EFS with local user accounts, the registry SHOULD be encrypted using syskey. Users SHOULD be trained in the correct use of EFS.

SYS.2.2.2.A16 Use of Windows PowerShell (H)

If Windows PowerShell (WPS) is not required, it SHOULD be uninstalled. It SHOULD be considered that in Windows 8.1, the PowerShell script environment may only be removed by uninstalling the .NET framework along with it. Alternatively, only administrators (local and

domain) SHOULD be permitted to execute WPS files. The process of logging write-only and read-only access to the Windows PowerShell profile SHOULD be activated and the logs checked regularly. The execution of Windows PowerShell scripts SHOULD be restricted with the command "Set-Execution Policy AllSigned" in order to at least prevent any accidental execution of scripts without a signature.

SYS.2.2.2.A17 Secure Use of the Maintenance Centre (H)

A security policy SHOULD define how the users utilise the Maintenance Centre. The settings for "Call up latest troubleshooting from the Windows Online Service for troubleshooting", "Send error reports", "Send data on computer configuration at regular intervals to Microsoft", "Windows backup", "Program for user-friendliness" and "Troubleshooting – other settings" SHOULD be disabled in Windows 8.1.

SYS.2.2.2.A18 Activation of the Last Access Time Stamp (H)

If a security concept is created for an IT system using Windows 8.1, it SHOULD be checked whether the last access time stamp can be activated in the file system to facilitate analysis of system misuse. The analysis SHOULD take into account possible effects of this setting, such as performance aspects or resulting limitations in incremental backups.

SYS.2.2.2.A19 Use of Login Information Management (H)

A policy SHOULD define whether or not storing access data in the vault is permitted. If it is not, doing so SHOULD be technically impossible.

SYS.2.2.2.A20 Security During Remote Access Using RDP (H)

The effects on the configuration of the local firewall SHOULD be taken into account when planning remote assistance procedures. The group of users authorised for remote desktop access SHOULD be specified in a corresponding policy and be assigned the corresponding user rights. Remote assistance SHOULD only be provided after explicit invitation via EasyConnect or on the basis of an invitation file. If an invitation is stored in a file, the file SHOULD be protected by a password. In every case, the user currently logged in SHOULD have to agree explicitly to starting a session. The maximum validity of an invitation SHOULD be of an appropriate duration. Strong encryption SHOULD also be used (128-bit, "highest level" setting). Furthermore, automatic password logins SHOULD be disabled. It SHOULD be checked whether diversions of the cache, printers, file repository, and smartcard connections are necessary. If they are not, they SHOULD be disabled. Unless remote control mechanisms are used, they SHOULD be completely disabled.

SYS.2.2.2.A21 Use of File and Registry Virtualisation (H)

It SHOULD be checked whether the operation of legacy applications that require write privileges for critical system folders or registry keys or have to be executed with administrator rights is still required. If this is the case, a strategy SHOULD be developed to replace the legacy applications that are still needed with secure alternatives. Until the legacy applications are replaced, it SHOULD be examined whether the Windows techniques "File Virtualisation" and "Registry Virtualisation" can be used to secure these applications. Registry virtualisation SHOULD only be able to access the necessary registry keys.

4. Additional Information

4.1. Useful Resources

Microsoft provides the following additional information about Windows 8.1:

- Secure Windows (for Windows 8/8.1, but largely also applicable to Windows Server 2012 / 2012 R2): https://technet.microsoft.com/en-us/library/hh832031.aspx
- Security and Protection: https://technet.microsoft.com/en-us/library/hh831778.aspx
- Security Auditing Overview: https://technet.microsoft.com/en-us/library/dn319078.aspx
- List of security events on Windows 8.1 and Windows Server 2012: https://www.microsoft.com/en-us/download/confirmation.aspx?id=50034
- Configuring Additional LSA Protection: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.2.2.2 *Windows 8.1 Clients*.

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

SYS.2.2.3 Windows 10 Clients

1. Description

1.1. Introduction

In Windows 10, Microsoft has adapted its Windows client operating system to a new corporate strategy. In particular, the basic philosophy has also changed, moving away from the previous principle of the “local operating system” to “Windows as a Service”. This means that in addition to its previous functions, the operating system contains further (in particular, cloud-based) applications and is therefore dependent on close integration with Microsoft's server infrastructure. Important new aspects compared to previous Windows versions above all include the integral and partly uncontrollable exchange of data between clients and Microsoft's infrastructure, as well as the increasing outsourcing of security-critical core components of Windows infrastructures (e.g. authentication) to the cloud. These new features should definitely be taken into account before using Windows 10.

1.2. Objective

The objective of this module to protect information processed in Windows 10, including on corresponding clients.

1.3. Scoping and Modelling

SYS.2.2.3 *Windows 10 Clients* must be applied to all clients on which the Microsoft Windows 10 operating system is used.

This module includes specific requirements to be considered and met in order to securely operate clients under Windows 10 in addition to the requirements contained in module SYS.2.1 *General Client*. For application programs used on Windows clients, the requirements of the corresponding modules must be fulfilled—for example, from APP.1.1 *Office Products* or APP.1.2 *Web Browsers*. In use cases located in a Windows domain, the requirements of corresponding modules such as APP.2.2 *Active Directory* must be met.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module SYS.2.2.3 *Windows 10 Clients*, the following specific threats and vulnerabilities are of particular importance.

2.1. Malware in Windows 10

Due to the prevalence of Windows operating systems and the backwards compatibility that often exists between system generations, the threat of malware and unauthorised penetrations of corresponding IT systems is relatively high. Malware may have numerous functions and provide an attacker with extensive control options. Among other purposes, it can be used to obtain specific passwords, control systems remotely, disable protective software, and collect data without authorisation. The damage caused by the loss or corruption of information or applications is particularly serious for an organisation. The reputational and financial damage that can result from malware is often also severe.

2.2. Integrated Cloud Functions

Windows 10 includes numerous features that are used to store and synchronise data using cloud services from Microsoft. This results in the risk of these services being used, whether unwittingly or carelessly, for data that could be personal or critical to an organisation. At the same time, storing data with third parties (which are usually located abroad) can result in infringements of data protection law. If a user logs into a new device using an already activated Microsoft account, the Microsoft cloud services utilised by the user will be set up automatically on the device. An organisation's data may thus be synchronised accidentally to the private devices of employees. As another example, a default setting of Windows 10 is to back up BitLocker recovery keys directly in the cloud via the user's Microsoft account, which constitutes providing sensitive cryptographic secrets to third parties.

2.3. Impairment of Software Features Due to Compatibility Issues

Software that ran successfully in previous versions of an operating system will not necessarily work with the current version of Windows 10. Possible reasons for this may include new security features or operating system properties, as well as the discontinuation of functions or services. As a result, the use of certain software may be limited or impossible. Examples of enabled security features that may be the cause of compatibility problems with new versions of Windows include User Account Control (UAC) or, with 64-bit versions of the operating system, Kernel Patch Guard. In addition, signed drivers could be necessary, but unavailable for older devices.

2.4. Telemetry Functions of Windows 10

Windows 10 sends diagnostic data to Microsoft by default. In addition, Microsoft can specifically request information from a client via the telemetry service integrated into Windows 10. At the telemetry level "Full", which is the default level in Windows 10 Home and

Pro, this includes, for example, access to the registry and the execution of certain diagnostic tools on the client. There is a risk that the diagnostic or telemetry data may contain sensitive information that could be passed on to third parties.

2.5. Restricted Forensics When Using the Virtual Secure Mode (VSM)

The use of Virtual Secure Mode (VSM) limits or complicates forensic investigations, including for security incident handling. Processes that are protected by Secure Kernel or Isolated User Mode (IUM) are no longer accessible. For example, memory images of these processes cannot be evaluated due to cryptographic measures.

3. Requirements

The specific requirements of module SYS.2.2.3 *Windows 10 Clients* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	User

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

The following requirements MUST be met for this module as a matter of priority.

SYS.2.2.3.A1 Planning the Use of Cloud Services for Windows 10 (B)

Since Windows 10-based devices are closely intertwined with the cloud services of Microsoft, the extent to which these cloud services should or may be used MUST be strategically determined before this occurs.

SYS.2.2.3.A2 Selecting and Procuring a Suitable Windows 10 Version (B)

The functional scope and functional changes included in a given Windows 10 version MUST be selected based on the identified protection needs and the purpose of use at hand. The feasibility of the required safeguards MUST be considered in the selection process. Based on the results of this review, the established procurement process at hand MUST be extended to include the selection of a corresponding licence model and service branches (CB, CBB, or LTSC).

SYS.2.2.3.A3 ELIMINATED (B)

This requirement has been eliminated.

SYS.2.2.3.A4 Telemetry and Privacy Settings in Windows 10 (B)

Telemetry services transmit diagnostic and usage data that the manufacturer links to unique characteristics for the purposes of troubleshooting, the improvement of services and products, and identification. This data can only be greatly reduced in Windows 10 Enterprise by setting the telemetry level to 0 (Security). If this setting cannot be effectively implemented, appropriate safeguards (e.g. at the network level) MUST be taken to ensure that this data is not transmitted to the manufacturer.

SYS.2.2.3.A5 Protection Against Malware in Windows 10 (B)

Unless equivalent or higher safeguards (such as execution control) have been implemented to protect an IT system from malware infection, a specialised malware protection component MUST be deployed on Windows 10 clients.

SYS.2.2.3.A6 Integration of Online Accounts into the Operating System [User] (B)

Logging into the system and domain MUST ONLY be possible using an account of a self-operated directory service. The ability to log in using local accounts SHOULD be reserved for administrators. Online login accounts (e.g. Microsoft accounts or accounts from other providers of identity management systems) MUST NOT be used because doing so transmits personal data to the systems of the respective manufacturer.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

SYS.2.2.3.A7 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.2.3.A8 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.2.3.A9 Secure Central Authentication of Windows Networks (S)

Only Kerberos SHOULD be used for central authentication. A group policy SHOULD prevent the use of older protocols. If this is not possible, NTLMv2 MUST be implemented as an alternative. Authentication by means of LAN Manager and NTLMv1 MUST NOT be allowed within an organisation or production operating environments. The cryptographic mechanisms used SHOULD be configured and documented according to the identified protection needs and based on the applicable internal guidelines. Deviating settings SHOULD be justified and coordinated with the respective security management personnel.

SYS.2.2.3.A10 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.2.3.A11 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.2.3.A12 File and Share Authorisation in Windows 10 (S)

Access to files and folders on a local system and to network shares SHOULD be configured in accordance with an authorisation and access concept. The standard administrative approvals on the system SHOULD also be taken into account. Users' write privileges SHOULD be restricted to a defined area in the file system. In particular, users SHOULD NOT be granted write privileges to folders of the operating system or of installed applications.

SYS.2.2.3.A13 Using the SmartScreen Function (S)

The SmartScreen feature, which checks files and web content downloaded from the Internet and transmits personal data to Microsoft in the process under certain circumstances, SHOULD be disabled.

SYS.2.2.3.A14 Use of the Voice Assistant Cortana [User] (S)

Cortana SHOULD be disabled.

SYS.2.2.3.A15 Use of Synchronisation Mechanisms in Windows 10 (S)

The synchronisation of user data with Microsoft cloud services and the process of sharing WLAN passwords SHOULD be disabled completely.

SYS.2.2.3.A16 Connection of Windows 10 to the Microsoft Store (S)

The use of the Microsoft Store SHOULD be checked and evaluated with respect to its compatibility with the data protection and security regulations of the organisation at hand. The general installation of apps in Windows 10 is not dependent on a connection to the Microsoft Store, so it SHOULD be disabled if it is not needed.

SYS.2.2.3.A17 No Storage of Automatic Login Data (S)

Storing passwords, certificates, and other information for automatic logins to websites and IT systems SHOULD NOT be allowed.

SYS.2.2.3.A18 Use of Windows Remote Support (S)

The effects on the configuration of the local firewall SHOULD be taken into account when planning Windows remote support procedures (this does not refer to RDP). Remote support SHOULD only be performed following an explicit invitation. When storing an invitation in a file, the file SHOULD be protected by a password. The user currently logged in SHOULD always have to agree explicitly to starting a session. A remote support invitation SHOULD have an appropriate maximum duration. If this service is not used, it SHOULD be disabled completely.

SYS.2.2.3.A19 Security During Remote Access Using RDP [User] (S)

The effects on the configuration of the local firewall SHOULD be taken into account when planning remote access. The group of users authorised for remote desktop access (RDP) SHOULD be specified by assigning corresponding user rights. In complex infrastructures, it SHOULD only be possible to reach an RDP target system via an intermediate RDP gateway. In order to use RDP, a check SHOULD be performed to ensure that the following convenience functions are in accordance with the protection needs of the target system:

- Use of the cache

- Integration of printers
- Integration of removable media and network drives
- Use of file repositories and smartcard connections

If the use of remote desktop access is not planned, it SHOULD be disabled completely. The cryptographic protocols and algorithms deployed SHOULD comply with the respective organisation's internal specifications.

SYS.2.2.3.A20 Use of User Account Control (UAC) for Privileged Accounts (S)

For privileged accounts, the configuration parameters of User Account Control (UAC) SHOULD be set with an appropriate balance between user-friendliness and security. The decisions regarding the configuration parameters to be used SHOULD be documented. In addition, the related documentation SHOULD include all accounts with administrator rights. Regular checks SHOULD be carried out to determine whether the ability to extend rights is necessary.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

SYS.2.2.3.A21 Use of the Encrypting File System (H)

Since the Encrypting File System (EFS) protects the keys used with the passwords of user accounts, secure passwords SHOULD be used. In addition, restrictive access rights SHOULD protect files that are encrypted using EFS. The recovery agent SHOULD be a dedicated account and not the administrator. In this context, the private key of this account SHOULD be secured and removed from the system. Backups of all private keys SHOULD be created. When using EFS with local user accounts, the local password memories SHOULD be encrypted by means of syskey. Windows Defender Credential Guard can also be used as an alternative. Users SHOULD be trained in the correct use of EFS.

SYS.2.2.3.A22 Use of Windows PowerShell (H)

PowerShell and WPS files SHOULD ONLY be executed by administrators. The execution of PowerShell SHOULD be logged centrally and the logs SHOULD be monitored. The execution of PowerShell scripts SHOULD be restricted using the command *Set-Execution Policy AllSigned* to prevent any accidental execution of unsigned scripts.

SYS.2.2.3.A23 Advanced Protection of Login Information in Windows 10 (H)

SecureBoot SHOULD be used on UEFI-based systems, and the status of the protected mode for the LSA credential store SHOULD be monitored during system startup (see also SYS.2.2.3.A11 *Protection of Login Information in Windows 10*). If remote maintenance of clients is intended using RDP, the “restrictedAdmin” option for RDP SHOULD be used for deployments of Windows 10 in domains with the functional level 2012 R2 or higher.

SYS.2.2.3.A24 Activation of the Last Access Time Stamp (H)

If a security concept is created for an IT system using Windows 10, it SHOULD be checked whether the last access time stamp can be activated in the file system to facilitate analysis of system misuse. Such checks SHOULD take into account possible effects of this setting, such as performance aspects or resulting limitations in incremental backups.

SYS.2.2.3.A25 Handling Remote Access Features of Connected User Experience and Telemetry (H)

It SHOULD be taken into account that the Connected User Experience and Telemetry (CUET) component in Windows 10 is an integral part of the operating system that, in addition to the telemetry feature, provides Microsoft with a way to access local systems remotely. This type of remote access to Windows 10 clients SHOULD be logged on the network side and blocked if required.

4. Additional Information

4.1. Useful Resources

As part of the project "SiSyPHuS Win10 (Study on System Integrity, Logging, Hardening, and Security-Relevant Functionality in Windows 10)", the BSI provides an analysis of the security functions of Windows 10 and appropriate hardening recommendations: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html

Microsoft provides the following additional information about Windows 10:

- Configuring Additional LSA Protection: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
- How Windows Defender Credential Guard Works: https://docs.microsoft.com/de-de/windows/access-protection/credential-guard/credential-guard-requirements
- Windows Defender Application Control and Virtualization-Based Protection of Code Integrity:https://technet.microsoft.com/de-de/library/dn986865.aspx

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module SYS.2.2.3 *Windows 10 Clients*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.39 Malware

SYS.2.3 Linux and Unix Clients

1. Description

1.1. Introduction

In addition to Windows, Linux- and (less frequently) Unix-based operating systems are being installed on more and more clients. Examples of classic Unix systems include the BSD series (FreeBSD, OpenBSD, and NetBSD), Solaris, and AIX. Linux, on the other hand, constitutes a functional rather than a classic Unix system because the Linux kernel is not based on the original source code from which the various Unix derivatives have evolved. Since the configuration and operation of Linux and Unix clients are similar, Linux and Unix are jointly referred to in this module as "Unix clients" and "Unix-like".

Linux is free software that is developed by the open-source community. This means anyone can use, copy, distribute, or modify it. In addition, there are providers that consolidate and maintain distributions comprising the Linux kernel and various software components while offering additional services. Derivatives of the distributions Debian, Red Hat Enterprise Linux, or SUSE Linux Enterprise are often used. In addition, there are Linux distributions that are tailored to special purposes and devices. These include, for example, Qubes OS, which attempts to achieve a high level of security through virtualisation; LibreElec, for the use of home theatre PCs; or Kali Linux, a distribution specialised in security, computer forensics, and penetration testing. Clients can also boot live distributions without changing the operating systems installed on the clients. The market share of the Linux operating system on clients has increased in recent years. In special operational environments, various derivatives of "classic" Unix systems continue to be used. Typically, an IT system of this type is networked and operated as a client in a client-server network.

As the number of pre-selected software packages in standard installations of common Linux distributions or Unix derivatives increases, so does the number of potential targets for attacks. At the same time, however, Unix-like operating systems also offer extensive protection mechanisms.

1.2. Objective

The objective of this module is to protect information created, processed, stored, or sent on Linux and Unix clients. The requirements of the module mainly address Linux clients, but can be adapted generally to Unix clients.

1.3. Scoping and Modelling

Module SYS.2.3 *Linux and Unix Clients* must be applied to all clients on which Linux or Unix-based operating systems are used.

This module includes fundamental requirements for operating Unix-like clients. It substantiates the aspects addressed in module SYS.2.1 *General Client* and adds specific features of Unix systems. Although Apple's macOS is a Unix-like operating system, it is not addressed in this module. Related recommendations can be found in module SYS.2.4 *macOS Clients*.

This module only includes the actual operating system that is usually involved in a basic installation of a distribution. Software based on this, such as e-mail clients or office software, is not considered in this module. Corresponding requirements can be found, for example, in the modules of layer APP.1 *Client Applications* of the IT-Grundschutz Compendium.

This client module requires that, in addition to the administrator, only one unchanged person with an interactive user account be permanently active. Clients used by several persons consecutively or simultaneously require additional safeguards that are not addressed within the framework of this module.

2. Threat Landscape

For module SYS.2.3 *Linux and Unix Clients*, the following specific threats and vulnerabilities are of particular importance:

2.1. Software from Third-Party Sources

In Unix-like IT systems, users may download and compile software themselves instead of installing ready-made software packages. Furthermore, when ready-made software packages are used, they are sometimes installed from third-party sources without further checking instead of exclusively from the manufacturer's existing package sources. Each of these alternative means of software installation entails additional risks because incorrect or incompatible software and malware may be installed.

2.2. Exploitability of the Script Environment

Script languages are often used in Unix-like operating systems. Scripts are lists of individual commands that are stored in text files and opened via the command line (for example). Due to the large scope of functions of script environments, attackers may make extensive use of scripts for their purposes. Furthermore, it can be very difficult to contain enabled script languages.

2.3. Dynamic Loading of Jointly Used Libraries

With the command line option LD_PRELOAD, a dynamic library can be loaded before all the other standard libraries that are needed in an application. In this way, individual functions of standard libraries can be specifically overwritten by one's own. An attacker could thus manipulate an operating system to execute malicious functions when using certain applications (for example).

2.4. Incorrect Configuration

When using Unix-like operating systems, numerous applications requiring separate configurations are already installed within the framework of a default installation. Subsequently installed applications must also be configured separately, which eventually leads to countless configuration files in the operating system in use.

Since many applications are configured independently of each other, the configuration options may be contradictory without this being apparent from the individual settings. For example, a remote administration service might be listening on a port that is blocked by packet filtering rules. In this way, applications may provide additional functions that are not desired by the user or be blocked from providing important functions. This can make it more difficult (or impossible) to perform certain tasks on a client.

3. Requirements

The specific requirements of module SYS.2.3 *Linux and Unix Clients* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	User

3.1. Basic Requirements

For module SYS.2.3 *Linux and Unix Clients*, the following requirements MUST be implemented as a matter of priority:

SYS.2.3.A1 Authentication of Administrators and Users [User] (B)

Administrators MUST NOT log in as “root” during normal operations. For system administration tasks, “sudo” or an appropriate alternative with appropriate logging SHOULD be used. Multiple users SHOULD be prevented from logging into a client simultaneously.

SYS.2.3.A2 Selection of an Appropriate Distribution (B)

An appropriate Unix derivative or Linux distribution MUST be selected based on the security requirements and intended purpose at hand. Support MUST be available for the operating system for the planned period of use. All the required application programs SHOULD be directly available as part of the distribution chosen. They SHOULD ONLY be obtained from third-party sources in exceptional cases. Distributions in which the operating system is compiled independently SHOULD NOT be used in production environments.

SYS.2.3.A3 ELIMINATED (B)

This requirement has been eliminated.

SYS.2.3.A4 Kernel Updates on Unix-Like Systems (B)

Clients MUST be rebooted promptly after the kernel of their operating system has been updated. If this is not possible, live kernel patching MUST be enabled as an alternative.

SYS.2.3.A5 Secure Installation of Software Packages (B)

If software requiring installation is to be compiled from source code, the software MUST ONLY be unpacked, configured, and compiled using an unprivileged user account. The software to be installed MUST NOT then be installed in the root file system of the operating system in question in an uncontrolled manner.

If the software is compiled from source text, the selected parameters SHOULD be documented appropriately. Based on this documentation, it SHOULD be possible to compile the software in a transparent and reproducible manner at any time. All further installation steps SHOULD also be documented so that the configuration can be reproduced quickly in emergencies.

3.2. Standard Requirements

For module SYS.2.3 *Linux and Unix Clients*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

SYS.2.3.A6 No Automatic Integration of Removable Drives [User] (S)

Removable drives SHOULD NOT be integrated automatically. The integration of removable drives SHOULD be configured in such a way that all files are marked as non-executable (mount option “noexec”).

SYS.2.3.A7 Restrictive Granting of Access Rights for Files and Directories (S)

It SHOULD be ensured that services and applications are only allowed to create, change, or delete the files assigned to them. In directories in which all users have write privileges (e.g. /tmp), the sticky bit SHOULD be set.

SYS.2.3.A8 Use of Techniques to Restrict the Rights of Applications (S)

In order to restrict the access rights of applications to files, devices, and networks, AppArmor or SELinux SHOULD be used. The solutions with the best protection provided by the respective Unix derivative or Linux distribution SHOULD be selected. The necessary applications SHOULD be regulated through whitelisting instead of blacklisting. Extensions

regarding the restriction of rights SHOULD be used in enforcing mode or by means of appropriate alternatives.

SYS.2.3.A9 Secure Use of Passwords in the Command Line [User] (S)

Passwords SHOULD NOT be transferred to programs as parameters.

SYS.2.3.A10 ELIMINATED (S)

This requirement has been eliminated.

SYS.2.3.A11 Preventing the Local Hard Drive From Becoming Overloaded (S)

Quotas for users or services SHOULD be set that leave enough capacity for the operating system. In general, different partitions SHOULD be used for the operating system and data. Alternatively, mechanisms of the file system in use SHOULD also be used that only grant write privileges to the “root” user once an appropriate level of capacity has been reached.

SYS.2.3.A12 Secure Use of Appliances (S)

It SHOULD be ensured that appliances are characterised by a level of security similar to that of clients on standard IT systems. It SHOULD be documented how the corresponding security requirements are met when using an appliance. If it is not possible to unequivocally comply with the requirements, a declaration of conformity SHOULD be requested from the respective manufacturer.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.2.3 *Linux and Unix Clients* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.2.3.A13 ELIMINATED (H)

This requirement has been eliminated.

SYS.2.3.A14 Protection Against the Use of Unauthorised Peripheral Devices (H)

It SHOULD only be possible to use peripheral devices if they are included in a centrally managed whitelist. Kernel modules for peripheral devices SHOULD only be loaded and enabled if the devices can be found on the applicable whitelist.

SYS.2.3.A15 Additional Protection Prior to Executing Undesired Files (H)

Partitions and directories for which users have write privileges SHOULD be mounted in such a way that no files can be executed (mount option “noexec”).

SYS.2.3.A16 ELIMINATED (H)

This requirement has been eliminated.

SYS.2.3.A17 Additional Prevention of Further Intrusion When Vulnerabilities Are Exploited (H)

The use of system calls SHOULD be restricted to the necessary minimum (e.g. by means of "seccomp"), particularly for exposed services and applications. The existing standard profiles and rules of SELinux and AppArmor, as well as of alternative extensions, SHOULD be checked manually and adapted as required to the security policy at hand. If necessary, new rules and profiles SHOULD be drawn up.

SYS.2.3.A18 Additional Kernel Protection (H)

Appropriate protective safeguards such as memory protection, file system protection, and role-based access control SHOULD be implemented with specially hardened kernels (e.g. grsecurity, PaX) to prevent exploitation of vulnerabilities and propagation in operating systems.

SYS.2.3.A19 Hard Disk or File Encryption (H)

Hard disks or the files stored on them SHOULD be encrypted. The related keys SHOULD NOT be stored on the same IT system. AEAD (Authenticated Encryption with Associated Data) procedures SHOULD be used for hard disk and file encryption. Alternatively, "dm-crypt" SHOULD be used in combination with "dm-verity".

SYS.2.3.A20 Disabling Critical SysRq Features (H)

The SysRq functions that users may execute SHOULD be specified. In general, it SHOULD NOT be possible for users to trigger any critical SysRq functions.

4. Additional Information

4.1. Useful Resources

No further information is available for module SYS.2.3 *Linux and Unix Clients*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.2.3 *Linux and Unix Clients*.

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Federal Office
for Information Security

SYS.2.4 macOS Clients

1. Description

1.1. Introduction

macOS is a client operating system from Apple. It is based on Darwin, the free Unix operating system from Apple, which in turn is based on the open-source operating system FreeBSD. macOS consists mainly of Darwin and the proprietary graphical user interface Aqua, as well as other applications and services. According to Apple's licensing conditions, macOS may only be installed on Apple IT systems ("Macs"). For this reason, features of these systems are also part of this module.

1.2. Objective

The objective of this module is to protect information which is processed on or transmitted by IT systems running macOS. To achieve this, macOS IT systems must appropriately secured.

1.3. Scoping and Modelling

Module SYS.2.4 *macOS Clients* must be applied to all client systems on which the Apple macOS operating system is used.

This module focuses on protecting a Mac running macOS that is operated as a stand-alone system or a client in a client/server network. It therefore supplements the general aspects of module SYS.2.1 *General Client*, which also applies here. The possible use of macOS as a server operating system is not considered in this module. For professional settings, the Profile Manager tool and mobile device management service offer the option to manage Macs remotely. These solutions offer extended configuration and administration functions which are not covered in this module. The relevant security aspects are covered in module SYS.3.2.2 *Mobile Device Management (MDM)*. It should also be noted that the Apple operating systems macOS (for Macs), iOS (for iPhones), and iPadOS (for iPads) are closely interlinked. Module SYS.3.2.3 *iOS (for Enterprise)* should also be considered if iOS or iPadOS devices are used in addition to macOS.

2. Threat Landscape

For module SYS.2.4 *macOS Clients*, the following specific threats and vulnerabilities are of particular importance:

2.1. Uncontrolled Access to Outsourced Data

macOS offers a number of functions that are executed on centralised servers run by Apple. For example, Apple's iCloud can be used to store and synchronise data among different macOS and iOS devices. Since data is temporarily stored on third-party servers and is therefore no longer under the user's own control, unauthorised persons could, in principle, also access these servers and view and misuse the data stored or transmitted there for their own purposes.

2.2. Misuse of Apple IDs as Central Access Information for Apple Services

To use some macOS functions, a unique Apple ID is required as access information. An Apple ID provides central access to various Apple services such as iCloud, iMessage, and the App Store. If unauthorised persons attain Apple ID access information, they may be able to use these services under a false identity and access information in iCloud.

2.3. Attacks on Wireless Interfaces

A Mac usually has wireless interfaces such as WLAN or Bluetooth, which are also used by many services and activated accordingly. WLAN, for example, can be used to exchange files directly between Apple devices (AirDrop). Furthermore, the WLAN and Bluetooth functions can be used to synchronise macOS and iOS devices (Continuity). AirPlay, meanwhile, makes it possible to send video and audio data to a compatible playback device. Attackers could attempt to misuse these wireless interfaces for attacks in order to intercept confidential information between Macs, iPhones, iPads, and other devices, or to compromise them in other ways.

2.4. Attacks on Applications with a Preview Function

Some of the applications integrated into macOS support a preview function for certain file formats (e.g. image files). These include the Finder, the Safari browser, and the e-mail program integrated into macOS. The preview function automatically displays part of the attachment of an e-mail (for example) if the file format is known. An attacker could thus attempt to hide malicious code in an e-mail attachment. The preview function would display the e-mail attachment and possibly execute the malicious code, which in turn could compromise the Mac in question.

2.5. Insecure Protocols in macOS or macOS Applications

macOS and its applications support various protocols, some of which are Apple's own (e.g. AFP) for communication with central servers or other end devices. If these communication

protocols do not have sufficient security mechanisms or are configured insecurely, the data transmitted could be read, falsified, or otherwise misused without permission.

3. Requirements

The specific requirements of module SYS.2.4 *macOS Clients* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	User

3.1. Basic Requirements

For module SYS.2.4 *macOS Clients*, the following requirements MUST be implemented as a matter of priority:

SYS.2.4.A1 Planning the Secure Use of macOS (B)

The introduction of macOS MUST be planned carefully. A decision MUST be taken as to where and how data will be stored. Organisations MUST make plans regarding how backups can be integrated into their overarching backup concepts. The systematic installation of updates related to security and other aspects of macOS and applications MUST be planned. When switching to macOS, the applications required MUST be determined. If a Mac is operated on a data network, the network protocols to be used MUST also be taken into account.

SYS.2.4.A2 Using the Security Functions Integrated into macOS (B)

The integrated macOS protection mechanisms System Integrity Protection (SIP), Xprotect, and Gatekeeper MUST be activated. Unless unsigned programs are absolutely necessary, Gatekeeper MUST ONLY allow signed programs to run.

SYS.2.4.A3 Use of Suitable User Accounts [User] (B)

The administrator account created during the initial configuration of macOS MUST ONLY be used for administrative purposes. A standard user account MUST be created for normal Mac use. If a Mac is used by several users, a separate user account MUST be created for every user. The guest user account MUST be disabled.

3.2. Standard Requirements

For module SYS.2.4 *macOS Clients*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

SYS.2.4.A4 Use of Hard Drive Encryption (S)

Hard drives SHOULD be encrypted, particularly for portable Macs (e.g. MacBooks). If the FileVault function integrated into macOS is used for this, the key material MUST NOT be stored online at Apple. The recovery keys produced by FileVault MUST be stored in a secure place. Whether an organisational recovery key should be used for FileVault SHOULD be checked.

SYS.2.4.A5 Disabling Security-Critical Functions in macOS (S)

The location services integrated into macOS SHOULD be disabled. Downloaded data SHOULD NOT be opened automatically. Content from optical and other media SHOULD NOT run automatically.

SYS.2.4.A6 Using Up-To-Date Mac Hardware (S)

If new Macs are to be purchased, current models SHOULD be selected. Macs already in use SHOULD be regularly checked to determine whether the installed operating systems still receive security updates from Apple. If Macs are no longer supported by Apple, they SHOULD NOT be used.

SYS.2.4.A7 Two-Factor Authentication for Apple IDs [User] (S)

Two-factor authentication SHOULD be activated for Apple ID accounts.

SYS.2.4.A8 No iCloud Use for Confidential Data [User] (S)

The synchronisation of confidential data among multiple devices via iCloud services SHOULD be prevented. Data SHOULD only be synchronised using self-operated services. Sensitive data SHOULD NOT be stored in iCloud. Draft copies (e.g. of e-mails or documents) SHOULD NOT be stored automatically in iCloud.

SYS.2.4.A9 Using Additional Protection Programs in macOS (S)

If required (such as when operating a Mac in a heterogeneous network), virus protection solutions from third parties SHOULD be used in addition to the integrated protection mechanisms of macOS.

SYS.2.4.A10 Activating the Personal Firewall in macOS (S)

The personal firewall integrated into macOS SHOULD be appropriately activated and configured.

SYS.2.4.A11 Disposing of Macs (S)

When disposing of a Mac, the NVRAM (Non-Volatile Random Access Memory) and SMC (System Management Controller) should be reset.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.2.4 *macOS Clients* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.2.4.A12 Firmware Password and Boot Protection on Macs [User] (H)

On older Macs, the request for a secure firmware password SHOULD be activated in command mode to prevent unauthorised booting from another boot drive. It SHOULD be checked whether a password should be requested for every startup process via full mode.

On Macs with a T2 security chip, a firmware password SHOULD be set via the Startup Security Utility. The option "Secure startup: Full security" SHOULD be activated. The option "Do not allow startup from external media" SHOULD be activated.

4. Additional Information

4.1. Useful resources

The National Institute of Standards and Technology (NIST) has published the document "SP 800-179 Rev. 1 (DRAFT): Guide to Securing Apple macOS 10.12 Systems for IT Professionals: A NIST Security Configuration Checklist" (October 2018).

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.2.4 *macOS Clients*.

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

SYS.3.1 Laptops

1. Description

1.1. Introduction

A laptop (also referred to as a notebook) is a PC designed for mobile use. It has a compact design, peripheral devices such as a keyboard and monitor, batteries that make it temporarily independent from an external power supply and, in many cases, hardware components specially designed for mobile use. Laptops are widely used in most organisations and often replace the traditional desktop PC.

Laptops are usually operated with common desktop operating systems such as Microsoft Windows, Apple macOS, or Linux. Today, the boundaries between laptops and tablets and similar devices have become fluid. Some tablets have desktop operating systems such as Windows 10, and keyboard accessories are also available for mobile devices such as iPads, which make it possible to use them like laptops.

Since laptops are often also used on the move, they are frequently not permanently connected to an organisation's LAN. Instead, they can usually connect to an organisation's network using a virtual private network (VPN), including via the public Internet. The infrastructure in a traditional office environment, which features controllable environmental factors, a stable power supply and restricted areas, cannot be assumed for the mobile use of laptops.

1.2. Objective

The objective of this module is to allow organisations to use laptops securely and to make people aware of the specific threats to this type of device.

1.3. Scoping and Modelling

Module SYS.3.1 *Laptops* must be applied to all laptops subject to mobile or stationary use.

As with all IT systems, the operating systems and software components of laptops must be carefully selected and installed. The requirements to be met here depend on the operating system on a given laptop, which is why they are set out in the client-specific modules—for example, SYS.2.2.3 *Windows 10 Clients*, SYS 2.3 *Linux and Unix Clients,* or SYS.2.4 *macOS Clients*.

By the same token, requirements that apply to all types of clients are not part of this module. These can be found in module SYS.2.1 *General Client*.

Guidelines on setting up specific types of data connections—for example, in WLAN configurations (see NET.2.2 *WLAN Usage*) or via a VPN (see NET.3.3 *VPN*)—are not covered in this module.

Since laptops are often used outside an organisation for longer periods of time, data backups require special consideration. Further requirements for this are included in module CON.3 *Backup Concept*.

2. Threat Landscape

For module SYS.3.1 *Laptops*, the following specific threats and vulnerabilities are of particular importance:

2.1. Degradation due to changing operational environments

Laptops are used in a very wide range of environments and are therefore subject to many threats. These threats include damaging environmental conditions such as excessively high or low temperatures, as well as dust and moisture. Laptops can also be damaged in transit. In addition, laptops communicate with unknown IT systems or networks, particularly while on the move, which always poses a potential risk to a device. Here, malware can be transmitted or sensitive information can be copied (for example).

2.2. Theft and loss of laptops

Employees regularly use their laptops outside their organisations. The devices are transported in cars or on public transportation, left in other peoples' offices during breaks, or left unattended in hotel rooms. Laptops are thus exposed to a higher risk of theft and can also be easily forgotten or lost. If a laptop is lost, replacing it involves costs and effort. Moreover, data that is not backed up is lost, as well. Unauthorised persons could also access sensitive data, which could lead to further damage. In many cases, this is significantly more severe than the mere material loss of the laptop.

2.3. Unregulated Changes of Laptop Users

If employees only need mobile IT systems in exceptional cases (e.g. for occasional business trips), it is often more practical to keep a small number of laptops. These can then be shared. However, if a laptop is simply handed over to the next employee, there is the risk that sensitive data still on the device will be passed on. The laptop could also be infected with malware. Without suitable regulations, it can be difficult to trace who has used the laptop and when, or who is currently using it.

3. Requirements

The specific requirements of module SYS.3.1 *Laptops* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	User, Procurement Department

3.1. Basic Requirements

For module SYS.3.1 *Laptops*, the following requirements MUST be implemented as a matter of priority:

SYS.3.1.A1 Rules for Mobile Laptop Use (B)

The aspects employees must consider when making mobile use of laptops MUST be clearly defined. In particular, the laptops available for mobile use, who is allowed to use them, and what basic security safeguards should be followed MUST be specified. The users MUST be informed of these rules.

SYS.3.1.A2 ELIMINATED (B)

This requirement has been eliminated.

SYS.3.1.A3 Use of Personal Firewalls (B)

A personal firewall MUST be activated on all laptops if they are to be used outside of an organisation's network. The filter rules for personal firewalls MUST be configured as restrictively as possible. They MUST be tested regularly. Personal firewalls MUST be configured to avoid pestering users with warnings they are not able to interpret.

SYS.3.1.A4 ELIMINATED (B)

This requirement has been eliminated.

SYS.3.1.A5 ELIMINATED (B)

This requirement has been eliminated.

SYS.3.1.A9 Secure Remote Access with Laptops (B)

When using publicly available networks, users MUST ONLY access their organisation's internal network through secure communication channels.

3.2. Standard Requirements

For module SYS.3.1 *Laptops*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

SYS.3.1.A66 Security Guidelines for Laptops (S)

Security policies that govern how laptops may be used SHOULD be established. Users SHOULD be made aware of the protection needs for laptops and the data stored on them. They SHOULD also be made aware of the specific threats at hand and the corresponding requirements for use. Furthermore, they SHOULD be informed of the types of information they may process on laptops.

SYS.3.1.A7 Orderly Issue and Return of Laptops [User] (S)

If different people take turns using the same laptops, secure methods of issuing laptops to employees SHOULD be defined. Their safe return SHOULD also be regulated. When a laptop changes users, any sensitive data SHOULD be securely deleted. If a laptop is not reset upon changing users, care SHOULD be taken to ensure that there is no malware on the corresponding IT system or any storage media connected to it. When they are issued a laptop, employees SHOULD also receive an information sheet on secure handling of the device.

SYS.3.1.A8 Secure Connection of Laptops to Data Networks [User] (S)

Secure methods SHOULD be defined for connecting laptops to internal or external data networks and the Internet. Only authorised laptops SHOULD be able to log on to the respective organisation's internal network.

SYS.3.1.A10 Synchronisation of Stored Data on Laptops [User] (S)

The way in which data is transferred from laptops to the corresponding organisation’s information domain SHOULD be regulated. If a synchronisation tool is used, care SHOULD be taken to ensure that synchronisation conflicts can be resolved. The synchronisation process SHOULD be logged. Users SHOULD also be instructed to check the synchronisation logs.

SYS.3.1.A11 Securing the Power Supply for Laptops [User] (S)

All users SHOULD receive information as to how they can best guarantee their laptop's power supply during mobile use. Spare batteries SHOULD be stored and transported in suitable cases.

SYS.3.1.A12 Reporting the Loss of Laptops [User] (S)

If a laptop is lost or stolen, the user SHOULD report this immediately. Organisations SHOULD have clear reporting channels for this purpose. If a lost laptop resurfaces, there SHOULD be an investigation into whether it could have been manipulated. The software used on it, including the operating system, SHOULD be completely reinstalled.

SYS.3.1.A13 Encryption of Laptops (S)

Storage media installed in laptops, such as hard disks or SSDs, SHOULD be encrypted.

SYS.3.1.A14 Suitable Storage of Laptops [User] (S)

All users SHOULD be advised on how to store laptops securely outside their organisation. Depending on the level of protection required for the data stored on them, laptops SHOULD also be secured against theft or kept in a locked location when not in use on the respective organisation's premises.

SYS.3.1.A15 Appropriate Selection of Laptops [Procurement Department] (S)

Before laptops are purchased, the persons in charge SHOULD carry out a requirements analysis. All possible devices SHOULD be assessed on the basis of the results. The decision on which laptops to procure SHOULD be agreed with the IT Operation Department.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.1 *Laptops* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.3.1.A16 Central Administration and Administration of Laptops (H)

A suitable regulation for the central administration of laptops SHOULD be defined. A tool for central laptop management SHOULD support all the operating systems used to the greatest extent possible.

SYS.3.1.A17 Pooled Storage of Laptops (H)

Unused laptops SHOULD be stored in an appropriately secured room. The room used for this SHOULD meet the requirements of INF.5 *Room or Cabinet for Technical Infrastructure*.

SYS.3.1.A18 Use of Anti-Theft Devices (H)

The anti-theft devices to be used for laptops SHOULD be regulated. In the context of mechanical devices, care SHOULD be taken to ensure that they have a good lock.

4. Additional Information

4.1. Useful Resources

No further information is available for module SYS.3.1 *Laptops*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the

second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.3.1 *Laptops*.

G 0.4 Pollution, Dust, Corrosion

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.39 Malware

G 0.45 Data Loss

G 0.31 Incorrect Use or Administration of Devices and Systems

Federal Office
for Information Security

SYS.3.2.1 General Smartphones and Tablets

1. Description

1.1. Introduction

Smartphones are IT systems designed for mobile use that have a customised interface operated via a large, usually touch-sensitive screen. In addition to telephony, smartphones combine features of a media player, personal information manager, and digital camera in one device while also offering users many other applications and functions, such as web browsing, e-mail access, and positioning (e.g. via GPS). They are equipped with interfaces for mobile networks, WLAN, Bluetooth, and NFC. In simple terms, tablets are smartphones with a large form factor that are usually not capable of making phone calls via mobile networks.

1.2. Objective

The objective of this module is to provide the persons in charge of security management and IT operations with information on the typical threats to smartphones and tablets and the requirements that should be met to avoid or eliminate these threats. Furthermore, it seeks to provide the persons in charge with approaches to drawing up configuration profiles in accordance with the protection needs at hand. These configuration profiles may be distributed and managed using a central infrastructure and a mobile device management (MDM) system. However, given the large number of different mobile operating systems, it generally cannot be assumed that mobile devices can be integrated into an MDM system.

1.3. Scoping and Modelling

The SYS.3.2.1 *General Smartphones and Tablets* module must be applied to all smartphones and tablets used for work-related purposes.

This module does not deal with how specific operating systems of smartphones and tablets can be secured; this is explained in detail in the modules for the respective systems, e.g. SYS.3.2.3 *iOS (for Enterprise)* or SYS.3.2.4 *Android*. Security requirements for operating an MDM

system are described in SYS.3.2.2 *Mobile Device Management (MDM)*. Organisations that use smartphones and tablets should apply these modules accordingly in addition to the present module.

Like any other ordinary clients, smartphones are exposed to risks related to malware. They must be taken into account in an organisation's concept for protection against malware. Requirements for protection against malware can be found in module OPS.1.1.4 *Protection Against Malware*.

Smartphones and tablets usually offer the option to install mobile applications (apps). To avoid unnecessary security risks, the requirements of the APP.1.4 *Mobile Applications (Apps)* module must be taken into account. Other modules from the APP *Applications* layer, such as APP.1.2 *Web Browser*, may also be relevant.

Since smartphones usually have mobile phone functions, the relevant requirements of the SYS.3.3 *Mobile Telephones* module must be taken into account, as well.

2. Threat Landscape

For module SYS.3.2.1 *General Smartphones and Tablets*, the following specific threats and vulnerabilities are of particular importance:

2.1. Lack of Operating System Updates

New versions and updates of mobile operating systems are released on a regular basis. For devices with manufacturer-specific extensions of their respective operating systems, the manufacturers must first integrate these extensions into their versions before proceeding with distribution. Updates are usually provided for the latest device generation and for a number of older device generations. However, not all previous operating system versions are supplied with (security) updates to the same extent. In some cases, operating systems are not further developed for economic reasons. Vulnerabilities in an operating system of a device generation that has been discontinued can then no longer be closed by updates, which makes them particularly easy for attackers to exploit.

2.2. Software Vulnerabilities in Pre-Installed Apps

Pre-installed apps may also include vulnerabilities which can be exploited for local attacks or attacks via network connections. Furthermore, many apps from third-party developers are no longer maintained after some time has passed. As a consequence, security deficiencies identified can no longer be remedied by appropriate updates.

2.3. Manipulation of Smartphones and Tablets

An attacker may gain access to smartphones or tablets in order to manipulate files in a targeted manner. For example, they could change configurations, start additional services, or install malware. They may thus be able to tap communication links on a manipulated system (resulting in unwanted data leaks) or change security rules to suit their needs (e.g. to allow access from the Internet to the target end device).

2.4. Malware for Smartphones and Tablets

Like any device connected to the Internet, mobile devices are also threatened by malware. Compared to client operating systems like Microsoft Windows, the risk of infection is lower, but attackers are increasingly concentrating on mobile devices. In particular, if apps are obtained from untrusted sources or updates for known vulnerabilities are not available, there is a risk of infection. If a device is infected, attackers can (for example) extract, modify, or delete data; access an organisation's internal IT resources; or act on behalf of the owner or the organisation.

2.5. Web-based Attacks on Mobile Browsers

Mobile browsers, along with many other apps, can display websites and web content. The devices may thus be affected by phishing attacks, drive-by exploits and other web-based forms of attack.

2.6. Misuse of Health, Fitness, or Location Data

The operating systems of many smartphones and tablets include specific features for managing health, fitness, and location data. This personal data represents an attractive target for attack and is particularly sensitive, especially if it is collected and stored over a longer period of time. For this to occur, such functions must first be activated by the user.

This can make it possible to identify an employee's location (for example) by attacking their device or the cloud services connected to it. In addition to the data protection implications, this can lead to further attacks under certain circumstances. Compromised location data could reveal that an employee is travelling on business, for instance, and expose their home to a break-in.

2.7. Misuse of Sensitive Data on the Lock Screen

Many mobile operating systems are equipped with a function that enables push messages and messages from activated widgets to be displayed on the lock screen. A user's confidential information may thus be disclosed to and exploited by unauthorised third parties. Voice assistants can also be used to access telephone functions and contact data even when a device is locked. This may also allow unauthorised third parties to access sensitive information.

In addition, it is often possible to configure interfaces such as WLAN or Bluetooth even when a device is locked. An attacker with physical access to a device could open up an additional attack vector by activating the device's Bluetooth interface, for example.

2.8. Dangers from Private Use of Work-Related Smartphones and Tablets

When employees use their organisation's smartphones and tablets privately, it immediately creates several problems for the organisation's information security. For example, a user might independently install apps containing malicious functions or visit a website that infects their device with malware. Many apps installed privately by users are also a risk to the

organisational information stored on their devices because they can access address books and send them to unknown servers, for example, or gain direct access to e-mails or documents. This could result in data leaks, or in data entering an organisation in an uncontrolled manner. Typical examples of apps that entail such risks are those used for social media and instant messaging.

2.9. Threats Related to Bring-Your-Own-Device (BYOD) Scenarios

If private end devices are used for work-related purposes, this results in a wide range of potential risks. For example, legal problems can arise in relation to software licences. If, in an emergency, work-related data needs to be deleted from a device through the corresponding MDM system, this may also affect the user's private data.

In addition, the persons in charge of IT cannot check every single private device to see whether it meets their organisation's requirements. This means devices can be used with which users may violate data protection and security requirements. Furthermore, users are often personally responsible for having their devices serviced and repaired. During such repairs, company data could be viewed without authorisation, for example. The same threat exists if an organisation has not regulated what should be done with the data on the devices of employees who are leaving the organisation.

2.10. Extended Rights Through Vulnerabilities

Vulnerabilities are repeatedly discovered in operating systems of smartphones and tablets that make it possible to circumvent the security concept established by the manufacturer and thus access system processes and protected memory areas. This allows programs to obtain unintended authorisations with which they can perform unauthorised actions. For example, the programs could thus access data of the operating system and other apps.

"Jailbreaks" exploit these vulnerabilities as a means of using alternative app stores or other extensions. Jailbreaking techniques can also be used by attackers to install malware or perform other harmful manipulations on a device.

In addition, malware can exploit vulnerabilities to install itself on a device or manipulate it. As a result, the operating system can be used for purposes other than those intended, and important security functions can be bypassed.

Data stored by the mobile operating system in protected areas is particularly affected, as an app with superuser rights may be able to extract it.

Deliberate actions to obtain higher-level rights ("rooting") can create similar threat scenarios if access to privileged rights is not protected.

3. Requirements

The specific requirements of module SYS.3.2.1 *General Smartphones and Tablets* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in

strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	User

3.1. Basic Requirements

For module SYS.3.2.1 *General Smartphones and Tablets*, the following requirements MUST be met as a matter of priority:

SYS.3.2.1.A1 Definition of a Policy for Using Smartphones and Tablets (B)

Before smartphones or tablets are provided, operated, or used by an organisation, a general policy for the use and control of such devices MUST be defined. In so doing, it MUST, amongst other things, be specified who may access which information within the organisation using smartphones.

SYS.3.2.1.A2 Drawing Up a Strategy for Cloud Usage (B)

An organisation MUST define a general policy for cloud use and the protection and control of information in relation to smartphones and tablets. The permitted use of cloud services in connection with the organisation's information MUST be clarified and defined. Whether and to what extent cloud services are allowed for private use of devices MUST be determined. Users MUST be regularly made aware of the issues regarding the use of such cloud services.

SYS.3.2.1.A3 Secure Basic Configuration for Mobile Devices (B)

All mobile devices MUST be configured to meet the required level of protection. To this end, an appropriate basic configuration of security mechanisms and settings MUST be established and documented. Functions that are not required SHOULD be disabled. The activation of communication interfaces MUST be regulated and reduced to the minimum required for work-related purposes. Unused interfaces SHOULD be disabled.

SYS.3.2.1.A4 Use of an Access Control Mechanism [User] (B)

Smartphones and tablets MUST be protected with an appropriately complex device lock code. Screen locking MUST be used. The display of confidential information on lock screens MUST be disabled. All mobile devices MUST automatically activate their screen lock after a reasonably short period of time. This time period MUST be related to the required level of protection.

After each failed attempt to unlock a device, the user SHOULD be required to wait longer before trying again. The number of device lock codes after which a code may be repeated SHOULD be specified. After several failed attempts to unlock a mobile device's screen, the device SHOULD perform a factory reset. The data or encryption keys at hand SHOULD be deleted securely in this process. When changing their passwords, users SHOULD avoid choosing a new password that they have used recently.

SYS.3.2.1.A5 Operating System and App Updates (B)

When selecting mobile devices to be procured, an organisation MUST ensure that the manufacturer specifies the period of time for which it plans to provide security updates for the devices. Older devices that are no longer provided with updates MUST be disposed of and replaced with devices supported by the respective manufacturer. In addition, apps SHOULD NOT be used if they are no longer supported by the manufacturer.

SYS.3.2.1.A6 Privacy Settings and Authorisations (B)

App and operating system access to data and interfaces MUST be restricted appropriately. The related data protection settings MUST be configured as restrictively as possible. In particular, access to camera, microphone, location, and health/fitness data MUST be checked for compliance with an organisation's internal data protection and security requirements. This access MUST be configured restrictively or disabled.

Security-relevant authorisation settings MUST be set so that they cannot be changed by users or apps. If this is not technically possible, the authorisation settings MUST be regularly checked and reset. In particular, this MUST be done after updates are installed.

SYS.3.2.1.A7 Code of Conduct in the Event of Security Incidents [User] (B)

If devices are lost or unauthorised changes to devices and their software are detected, the respective users MUST immediately inform the persons in charge.

SYS.3.2.1.A8 Installation of Apps (B)

An organisation MUST regulate whether, how, and which apps users are allowed to install themselves on their devices. Users SHOULD only be allowed to install approved apps. An organisation MUST define the sources from which apps may be installed. The installation of apps from unapproved sources MUST be prevented.

3.2. Standard Requirements

For module SYS.3.2.1 *General Smartphones and Tablets*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.3.2.1.A9 Restrictive Use of Functional Extensions (S)

Functional extensions SHOULD only be used restrictively. If possible, functional extensions SHOULD not be used at all. Functional extensions SHOULD NOT have any automatic access to sensitive information. They SHOULD NOT be able to circumvent or change the specified basic configurations.

SYS.3.2.1.A10 Policy for Employees Regarding the Use of Mobile Devices [User] (S)

A binding policy for employees SHOULD be established for the use of mobile devices. This policy SHOULD define how mobile devices are to be used and maintained. It SHOULD address the issues of secure storage and loss reporting. It SHOULD also prohibit users from uninstalling management software, rooting their devices, or changing security-related configurations.

SYS.3.2.1.A11 Storage Encryption (S)

The non-volatile storage of mobile devices SHOULD be encrypted. Sensitive data on additional storage media in use (such as SD cards) SHOULD be encrypted.

SYS.3.2.1.A12 Use of Non-Personalised Device Names (S)

Device names SHOULD not include any information regarding the respective users or organisation.

SYS.3.2.1.A13 Rules Regarding Screen Sharing and Casting (S)

A decision SHOULD be taken on whether and how functions should be used to transmit screen content and audio or video content (screen sharing or casting). These functions SHOULD be regulated in organisational or technical terms. To this end, a corresponding agreement SHOULD be established with users.

SYS.3.2.1.A14 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.1.A15 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.1.A16 Disabling Unused Communication Interfaces [User] (S)

Communication interfaces SHOULD only be activated when needed and in suitable environments. If an MDM system is used, the interfaces SHOULD be managed centrally via this system.

SYS.3.2.1.A17 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.1.A18 Use of Biometric Authentication (S)

If a biometric procedure is used for authentication (e.g. based on a fingerprint sensor), it SHOULD be checked whether similarly high or higher protection can be achieved compared to using a device password. If this is unclear or if the level of protection is actually lower, the biometric procedure SHOULD NOT be used. Users SHOULD be made aware that biometric features can be falsified.

SYS.3.2.1.A19 Use of a Voice Assistant (S)

Voice assistants SHOULD only be used when they are necessary. Otherwise, they SHOULD be disabled. In general, it SHOULD not be possible to use a voice assistant when a device is locked.

SYS.3.2.1.A20 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.1.A21 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.1.A22 Integrating Mobile Devices into Internal Infrastructure via VPN (S)

Mobile end devices SHOULD only be integrated into an organisation's infrastructure through a VPN. An appropriate method SHOULD be selected and used for this purpose. Instead of passwords, devices SHOULD authenticate themselves to internal infrastructure via certificates.

SYS.3.2.1.A28 Using the Filter Option for Websites (S)

If an organisation already uses a reputation service or a corresponding proxy server, this SHOULD be stored as a global HTTP proxy for all the installed browsers in use. If such a proxy is only accessible within the internal network in question, end devices SHOULD be integrated (either permanently or based on the apps used) using a VPN connection.

If mobile devices are not integrated into an organisation's existing proxy or reputation infrastructure, filtering options based on whitelists or blacklists or third-party content filters SHOULD be used for web browsers.

SYS.3.2.1.A31 Regulation of Mobile Payments (S)

Whether mobile payments are allowed with work-related smartphones and tablets SHOULD be regulated.

SYS.3.2.1.A32 MDM Usage (S)

Smartphones and tablets SHOULD be managed by an MDM system.

SYS.3.2.1.A33 Selection and Installation of Security Apps (S)

All mobile end devices SHOULD be protected against malware. Appropriate security apps SHOULD be selected for end devices if possible. The security apps SHOULD be installed automatically—for example, via an MDM system.

SYS.3.2.1.A34 Configuration of the DNS Server Used (S)

Default gateway entries, such as the DNS servers of the manufacturer or developer in question, SHOULD be replaced by those of the provider or the organisation at hand.

If the provider offers DNS-over-HTTPS (DoH), this SHOULD be used. If this is not yet offered, it SHOULD be disabled.

3.3. Requirements in case of increased protection needs

Generic suggestions for module SYS.3.2.1 *General Smartphones and Tablets* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.3.2.1.A23 ELIMINATED (H)

This requirement has been eliminated.

SYS.3.2.1.A24 ELIMINATED (H)

This requirement has been eliminated.

SYS.3.2.1.A25 Use of Separate Work Environments (H)

If employees are permitted to use work-related devices privately as well, solutions for isolated working environments SHOULD be used on these end devices. If possible, only certified products (e.g. those in accordance with Common Criteria) SHOULD be purchased for this purpose. The organisation's data SHOULD remain in the organisation's environment.

SYS.3.2.1.A26 Use of PIM Containers (H)

Information on mobile devices SHOULD be encapsulated (e.g. in a PIM container). In addition, this data SHOULD be secured by separate authentication and a form of data and transport encryption that is independent from the operating system in use.

SYS.3.2.1.A27 Use of Specially Secured End Devices (H)

Depending on the protection needs at hand, organisations SHOULD use specially secured mobile devices that are certified for processing information in line with statutory information protection classifications.

SYS.3.2.1.A29 Use of an Organisation-Related APN (H)

It SHOULD be checked whether an organisation-related access point to mobile networks (an access point name, APN) can be used to limit the pool of permitted devices. The mobile service provider in question SHOULD assign an IP address range coordinated with the respective organisation to all the devices that use this APN. For authentication, a complex password with a maximum of 64 characters SHOULD be agreed with the mobile service provider. When using an organisation-related APN, authentication SHOULD take place on the basis of the CHAP protocol.

SYS.3.2.1.A30 Restricted App Installation Using a Whitelist (H)

In case of increased protection needs, the users of mobile end devices SHOULD only be able to install approved and tested apps. If an MDM system is used, it SHOULD prevent other apps from being installed; alternatively, it SHOULD immediately remove apps that are installed without authorisation.

SYS.3.2.1.A35 Using a Firewall (H)

A firewall SHOULD be installed and activated on smartphones and tablets.

4. Additional Information

4.1. Useful resources

The International Organization for Standardization (ISO) provides guidelines for the use of mobile devices in the standard ISO/IEC 27001:2013, especially in annex A, A.6.2 ("Mobile Devices and Teleworking").

The Information Security Forum (ISF) offers guidelines for the use of mobile devices in "The Standard of Good Practice for Information Security", especially in Area PA2 ("Mobile Computing").

The National Institute of Standards and Technology (NIST) has published the following documents in the area of mobile devices:

- Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST Special Publication 800-124, Revision 1, June 2013
- Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4, April 2013
- Securing Electronic Health Records on Mobile Devices: NIST Special Publication 1800-1d, Draft, July 2015

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.3.2.1 *General Smartphones and Tablets*.

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.45 Data Loss

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.46 Loss of Integrity of Sensitive Information

SYS.3.2.2 Mobile Device Management (MDM)

1. Description

1.1. Introduction

For many employees, smartphones, tablets and phablets have become an indispensable part of their work. However, IT departments are having to provide ever greater numbers of such devices in many different designs while also ensuring adequate security. In addition, mobile devices are exposed to particular risks and their administration differs in fundamental respects from other IT systems.

Consequently, a mobile device management (MDM) system is essential for regulated and secure operation of these devices, particularly in organisations with a large number of smartphones, tablets, and phablets. With corresponding MDM software, end devices can be managed centrally, security regulations can be implemented, and emergency actions can be triggered. An MDM system thus ensures a consistent (or at least comparable) security standard on all devices administered.

1.2. Objective

This module shows how organisations can secure the use of mobile devices via an MDM system and provides related operating information.

1.3. Scoping and Modelling

The SYS.3.2.2 *Mobile Device Management (MDM)* module must be applied to any information domain in which mobile devices are administered using a mobile device management (MDM) system.

For the purposes of this module, mobile devices are smartphones, tablets, and phablets on which mobile operating systems such as Android or iOS are installed. The security requirements of smartphones, tablets, laptops, and tablets with desktop operating systems are described in other modules of the SYS *IT Systems* layer. The requirements of SYS.3.2.1 *General*

Smartphones and Tablets must also be taken into account when using an MDM system. Ways to secure specific smartphones, tablets, and phablets from different manufacturers are explained in detail in the modules for the respective operating systems, e.g. SYS.3.2.3 *iOS (for Enterprise)* or SYS.3.2.4 *Android*.

An access control policy SHOULD be drawn up for an MDM system. Requirements for this can be found in module ORP.4 *Identity and Access Management*. One of the most fundamental tasks of an MDM system is the administration of mobile devices. General security requirements for administration are contained in OPS.1.1.2 *Proper IT Administration*.

Finally, this module does not deal with aspects of “bring your own device” (BYOD) scenarios.

2. Threat Landscape

For module SYS.3.2.2 *Mobile Device Management (MDM)*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Synchronisation with the MDM System

In order for an MDM system to be able to implement the regulations defined by the persons in charge on mobile devices, the devices must be regularly synchronised with the MDM system. If a device is not connected to the MDM system for a long period of time, new or updated regulations may not be installed (for example). In addition, if there is no connection to a lost device, the data on it can no longer be remotely deleted.

2.2. Improper MDM Administration

MDM solutions are complex applications that typically have several hundred different rules. Not all of the rules can be combined with one another, while others depend on one another. Due to administrative errors, end devices may be exposed to a wide variety of threats which have a direct or indirect effect on the confidentiality, availability, or integrity of data and applications.

2.3. Inappropriate Rights Management in MDM Systems

An MDM system's rights management component decides which users can configure which settings on mobile devices and who can access which data. If an employee is assigned the wrong role, there is the risk that they will be granted higher-level rights than they should have. For example, they could view data without authorisation or change settings on their device. It would also be possible for them to install and use apps (or cloud storage services, for example) which are not authorised in their organisation. This may result in leaks of the organisation's sensitive data or the violation of statutory data protection regulations.

2.4. Unauthorised Creation of Movement Profiles Through the MDM System

With most MDM products, it is possible to determine where a device is located, and this can be used as a basis for allowing or blocking access to data or apps ("geofencing"). This results in detailed movement profiles for devices, and thus also for their users. If this data is collected without users being appropriately informed, the persons in charge may, under some circumstances, be in violation of data protection regulations. There is also a risk of attackers accessing this data. Geofencing can be misused to unlawfully monitor employees, as well.

3. Requirements

The specific requirements of module SYS.3.2.2 *Mobile Device Management (MDM)* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module SYS.3.2.2 *Mobile Device Management (MDM)*, the following requirements MUST be met as a matter of priority:

SYS.3.2.2.A1 Determining a Strategy for Mobile Device Management (B)

An organisation MUST develop a strategy which determines how its employees may use mobile devices and how the devices are to be integrated into its IT structures. The protection needs of the information to be processed MUST be a fundamental consideration in this regard. The strategy MUST cover at least the following aspects:

- Can the MDM system be operated as a cloud service?
- Should the MDM system be operated by the organisation itself?
- Should the MDM system provide all the necessary apps, or can users install apps themselves? What restrictions does the organisation want to impose on the apps it provides or those that are installed by users?
- Should the MDM system be integrated into a broader infrastructure?
- What support and response requirements does the MDM provider need to fulfil?
- What compliance requirements must be implemented?

- Which mobile devices and which operating systems does the MDM system need to support?
- Does the MDM solution need to be multi-client-capable? Does it guarantee the necessary separation of clients?
- Do cloud services need to be incorporated?
- Do document management systems need to be incorporated?
- Does the MDM system need to incorporate and manage peripheral devices, as well?
- What will the operating model involve: private end devices (bring your own device, BYOD), personalised end devices (owned by the organisation), or non-personalised end devices (owned by the organisation and used jointly)?

The strategy MUST be specified in writing and approved by the CISO.

SYS.3.2.2.A2 Defining Admissible Mobile Devices (B)

The mobile devices and operating systems that are permitted in an organisation MUST be specified. All authorised devices and operating systems MUST satisfy the requirements of the MDM strategy at hand and fully comply with the organisation’s security requirements. The organisation's MDM system MUST be configured such that only approved devices can access the organisation’s information. The procurement of mobile devices MUST be restricted to those approved by the organisation.

SYS.3.2.2.A3 Selecting an MDM Product (B)

When suitable MDM software is to be purchased, care MUST be taken to ensure that it satisfies all of the requirements specified in the MDM strategy at hand. It MUST also be able to implement all the necessary technical and organisational security safeguards and support all the mobile devices permitted.

SYS.3.2.2.A4 Distribution of the Basic Configuration to Mobile Devices (B)

All mobile devices MUST be integrated into the MDM system at hand before they are used. When devices receive their basic configuration, they MUST be set to factory settings. The connection between mobile devices and the MDM system MUST be appropriately secured. For devices which are already in use, all organisation-related data MUST be deleted first. An end device which has not been configured through the MDM system MUST NOT be able to access the corresponding organisation’s information.

SYS.3.2.2.A5 Installing the MDM Client (B)

When mobile devices are handed over to employees, the MDM client in question MUST be installed and configured on them if it is not already provided by the operating system in use.

SYS.3.2.2.A20 Regular Review of the MDM System (B)

Security settings MUST be checked regularly. For new operating system versions of mobile devices, it MUST be checked in advance whether the MDM system in use fully supports them and whether the configuration profiles and security settings are still effective and sufficient. Deviations MUST be corrected. The access rights assigned to users and administrators MUST be checked regularly to ensure that they are still appropriate (minimum principle).

3.2. Standard Requirements

For module SYS.3.2.2 *Mobile Device Management (MDM)*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

SYS.3.2.2.A6 Logging the Device Status (S)

The lifecycle of a mobile device (including its configuration history) SHOULD be sufficiently logged and centrally retrievable. If required, an administrator SHOULD be able to determine the current status of managed devices (device audit).

SYS.3.2.2.A7 Installation of Apps (S)

Apps SHOULD be installed, uninstalled, and updated via the MDM in use system in line with the requirements of the planned deployment scenario. The MDM system SHOULD force the installation, uninstallation, and update process as soon as a connection to a mobile device is established. Users SHOULD not be able to uninstall apps installed via the MDM system. The MDM system SHOULD support a blacklist or whitelist for the installation of apps.

SYS.3.2.2.A8 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.2.A9 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.2.A10 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.2.A11 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.2.A12 Protection of the MDM Operating Environment (S)

The MDM system in use SHOULD itself be secured using technical safeguards in order to satisfy the protection needs of the information it stores or processes. The underlying operating system SHOULD be hardened.

SYS.3.2.2.A21 Administration of Certificates (S)

Certificates for the use of services on mobile devices SHOULD be installed, uninstalled, and updated centrally via the MDM system in use. The installation of untrusted and unverifiable (root) certificates by the user SHOULD be prevented by the MDM system. The MDM system SHOULD support mechanisms that verify the validity of certificates.

SYS.3.2.2.A22 Remote Deletion and Decommissioning of End Devices (S)

The MDM system in use SHOULD ensure that all business data on mobile devices can be deleted remotely (remote wipes for existing data connections). If external storage devices are being used in a mobile device, the system SHOULD check whether these should also be deleted in a remote wipe. This function SHOULD be supported by the MDM system.

The process for decommissioning mobile devices (unenrollment) SHOULD ensure that no sensitive data remains on devices or their integrated storage media. This SHOULD particularly apply if the unenrollment is to be carried out remotely.

3.3. Requirements in case of increased protection needs

Generic suggestions for module SYS.3.2.2 *Mobile Device Management (MDM)* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.3.2.2.A13 ELIMINATED (H)

This requirement has been eliminated.

SYS.3.2.2.A14 Use of External Reputation Services for Apps (H)

If the administrators of an organisation cannot select the admissible apps and users are able to install apps on their devices themselves, a reputation service SHOULD be used. The MDM system in use SHOULD then use information from the reputation service to at least limit the installation of apps.

SYS.3.2.2.A15 ELIMINATED (H)

This requirement has been eliminated.

SYS.3.2.2.A16 ELIMINATED (H)

This requirement has been eliminated.

SYS.3.2.2.A17 Monitoring the Use of Mobile Devices (H)

Appropriate criteria SHOULD be defined and used as a basis for monitoring devices without violating legal or internal provisions. In particular, jailbreaks and attempts at rooting SHOULD be recognised.

SYS.3.2.2.A18 ELIMINATED (H)

This requirement has been eliminated.

SYS.3.2.2.A19 Using Geofencing (H)

A geofencing policy SHOULD ensure that devices with sensitive information cannot be used outside a pre-defined geographical area. If a user leaves this geographical area, the information designated for deletion on their device (or the device itself) SHOULD be wiped completely. Before the device is selectively or completely deleted, the administrators in charge, the security management personnel in question, and the user SHOULD be informed. The device SHOULD only be selectively or completely deleted after an appropriate time delay. The areas in which these additional security safeguards are necessary SHOULD be identified. The security safeguards SHOULD then be implemented in compliance with the relevant legal and internal provisions.

SYS.3.2.2.A23 Enforcing Compliance Requirements (H)

Violations of an organisation's regulations and manipulation of device operating systems SHOULD be detected by a suitable solution. The following actions SHOULD be taken if violations of regulations or OS manipulations are suspected. The solution SHOULD provide corresponding functions, including:

- automated warnings
- autonomous locking of devices
- deletion of the organisation’s confidential information
- deletion of the entire device
- prevention of access to company apps
- prevention of access to the organisation’s systems and information

If a violation or manipulation is suspected, an alert SHOULD be sent to the administrators in charge and the organisation's security management personnel.

4. Additional Information

4.1. Useful resources

In its publications on cyber security, the BSI has published the document BSI-CS 052: “Mobile Device Management”. The BSI has also published the “Überblickspapier Consumerisation und BYOD” [Overview Paper on Consumerisation and BYOD], 2013.

The BSI has published “Mindeststandard des BSI für Mobile Device Management nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 11.05.2017” [BSI Minimum Standard for Mobile Device Management in Accordance with Section 8 (1), Sentence 1 of BSIG – Version 1.0, 11 May 2017].

The National Institute of Standards and Technology (NIST) has published NIST Special Publication 800-124, "Guidelines for Managing the Security of Mobile Devices in the Enterprise", Revision 1, June 2013.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.3.2.2 *Mobile Device Management (MDM)*.

G 0.11 Failure or Disruption of Service Providers

G 0.13 Interception of Compromising Interference Signals

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.45 Data Loss

SYS.3.2.3 iOS (for Enterprise)

1. Description

1.1. Introduction

Due to their modern and simple control concepts and high performance, smartphones and tablets are very common nowadays. This also includes the mobile iPhone and iPad devices produced by Apple, which run on the operating systems iOS and iPadOS. Since iPadOS is based on iOS, both are referred to as “iOS” in this module for simplicity. At present, the two operating systems mainly have functional differences that take into account the different form factor of the devices.

Originally, these devices were designed for private use. Due to the reshaping of infrastructures and the ways in which information is collected and processed, however, they are also being used more and more frequently in professional environments, where they are even replacing laptops in some cases.

Through the integration of business functions, iOS has (from version 4) been gradually extended for use in companies and public authorities, and functions have been integrated for management from an organisation’s point of view. This includes the possibility of centralised device registration (Apple Business Manager) as well as options such as Single Sign-On (SSO).

1.2. Objective

The objective of this module is to show how devices that run on iOS (for Enterprise) can be used securely in organisations. Requirements are presented for the settings of iOS-based end devices, which can be distributed to devices in the form of configuration profiles. iOS configuration profiles include uniformly defined settings (e.g. for security policies or individual system aspects) for managing iOS-based devices in a standardised and centralised manner and configuring them automatically.

1.3. Scoping and Modelling

Module SYS.3.2.3 *iOS (for Enterprise)* must be applied to all smartphones and tablets running the Apple iOS operating system that are used for business purposes.

This module includes basic specifications to be observed and fulfilled when operating iOS-based devices that are integrated into an organisation's processes. Requirements for integrating such devices into an organisation's security or collaboration infrastructure are not the focus of this module. Through mobile device management (MDM), it is possible to manage devices centrally and roll out configuration profiles for specific user groups or intended purposes. Using an MDM system, safeguards can also be implemented in a uniform way. This module assumes that the iOS devices to be managed are integrated into an MDM infrastructure. If a small number of devices are managed, they can be used without MDM in exceptional cases for economic reasons. Requirements for the operation of MDM systems can be found in module SYS.3.2.2 *Mobile Device Management (MDM)*. For smaller environments, Apple Configurator can also be used to roll out the requirements listed in this module to multiple end devices in a uniform way. General and overarching aspects of the operation of smartphones and tablets (regardless of the respective operating systems) can be found in module SYS.3.2.1 *General Smartphones and Tablets* and must also be implemented if iOS-based devices are used.

SYS.3.2.1 *General Smartphones and Tablets* also contains requirements for the use of biometric authentication mechanisms.

2. Threat Landscape

For module SYS.3.2.3 *iOS (for Enterprise)*, the following specific threats and vulnerabilities are of particular importance:

2.1. Concentration of Risk When One User Account (Apple ID) is Used for all Apple services

An Apple ID provides central access to all the services provided by Apple (e.g. iMessage, FaceTime, iCloud, App Store, Apple Music, Book Store, Find My, or synchronisation services). If unauthorised persons obtain access to an inadequately secured Apple ID, they might, under certain circumstances, use these Apple services under a false identity, disrupt the availability of Apple ID-based services, remotely locate iOS-based devices, reset a device to factory settings, or access information from the iCloud service. Especially when iCloud backups have been activated, an attacker may be able to clone the data stored on a user's iOS device.

2.2. Fixed Integration of Pre-Installed Apps and Their Functions

Apple delivers integrated and pre-installed apps (such as Mail and Safari) with iOS. These apps are partially designed with higher authorisations than apps that can be downloaded from the App Store, which increases the range of possible attacks on iOS-based devices.

2.3. Improper Access to Outsourced Data

For a number of iOS-specific functions, the infrastructure operated by Apple must be used. If iCloud Keychain, iMessage, FaceTime, Siri, Continuity, Spotlight Suggestions, or iCloud functions for creating backups or working jointly on documents are used, the corresponding

data is constantly synchronised among different devices and users via Apple's infrastructure. Push messages for iOS-based devices are also transmitted via this infrastructure. There is therefore a general risk that Apple servers will be accessed and the data stored or transmitted there will be misused for other purposes.

3. Requirements

The specific requirements of module SYS.3.2.3 *iOS (for Enterprise)* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module SYS.3.2.3 *iOS (for Enterprise)*, the following requirements MUST be met as a matter of priority:

SYS.3.2.3.A1 Strategy for Using iOS Devices (B)

If an MDM system is used, any iOS-based devices in use MUST be managed and configured via this system. There MUST be a strategy for using iOS devices that defines aspects such as the selection of end devices or backup strategies. Whether additional apps from third-party providers should or may be used MUST be regulated. Furthermore, jailbreaks MUST be prohibited by organisational guidelines and, if possible, technically prevented.

SYS.3.2.3.A2 Planning the Use of Cloud Services (B)

Before iOS-based devices are used, it MUST be determined which cloud services should or may be used and to what extent. It SHOULD be taken into account that iOS-based devices are generally closely intertwined with Apple's own iCloud services. It SHOULD also be considered that this integration can be triggered by merely activating individual devices with an Apple ID. It SHOULD therefore be checked whether Apple Business Manager (formerly the Device Enrollment Program, DEP) can be used for device registration.

SYS.3.2.3.A3 ELIMINATED (B)

This requirement has been eliminated.

SYS.3.2.3.A4 ELIMINATED (B)

This requirement has been eliminated.

SYS.3.2.3.A5 ELIMINATED (B)

This requirement has been eliminated.

SYS.3.2.3.A6 ELIMINATED (B)

This requirement has been eliminated.

SYS.3.2.3.A7 Preventing Unauthorised Deletion of Configuration Profiles (B)

In order to ensure that configuration profiles cannot be deleted without authorisation, suitable technical (e.g. through support mode) or organisational regulations MUST be established and implemented. Users of mobile devices SHOULD be made aware of the intention and purpose of these security safeguards.

SYS.3.2.3.A8 ELIMINATED (B)

This requirement has been eliminated.

3.2. Standard Requirements

For module SYS.3.2.3 *iOS (for Enterprise)*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

SYS.3.2.3.A9 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.3.A10 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.3.A11 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.3.A12 Using Apple IDs (S)

An anonymised Apple ID SHOULD be used instead of a user's personal Apple ID. If possible, Apple Business Manager SHOULD be used for volume licensing (formerly the Volume Purchase Program, VPP) and the centralised installation of apps.

SYS.3.2.3.A13 Using the “iOS Restrictions” Configuration Option (S)

All iOS functions and services that are not needed or allowed SHOULD be disabled. Based on the intended purpose at hand and the underlying protection needs, the use of lock screens, unified communication, Siri, background images, connections to host systems, and diagnostic and usage data SHOULD be checked in particular.

SYS.3.2.3.A14 Using the iCloud Infrastructure (S)

Before extensive or selective usage of the iCloud infrastructure is approved for business use, the compatibility of Apple’s general terms and conditions with an organisation's internal policies SHOULD be assessed in terms of availability, confidentiality, integrity, and data

protection. If the use of the iCloud infrastructure is allowed, identities on the iCloud web service SHOULD be verified by two-factor authentication. Otherwise, iCloud use for purely business purposes SHOULD be reduced to a minimum or completely prohibited.

SYS.3.2.3.A15 Using Continuity Functions (S)

If using the iCloud infrastructure has not been generally prohibited by an organisation's security management department, the compatibility of Continuity functions with the organisation's internal policies SHOULD be assessed, taking account of the aspects of confidentiality and integrity. Based on the results of this assessment, the extent to which these functions are technically and organisationally restricted SHOULD be regulated.

SYS.3.2.3.A16 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.3.A17 Using the Device Code History (S)

In configuration profiles, the number of unique codes that must be used before repetition is allowed SHOULD be set to an appropriate value.

SYS.3.2.3.A18 Using the Configuration Option for the Safari Browser (S)

The browser policies already established in an organisation SHOULD also be implemented accordingly for Safari by means of technical and organisational safeguards. The requirements for browsers on stationary and portable PCs that are already in place SHOULD be used as a basis for securing iOS-based devices and establishing application scenarios. The operational environment of the devices SHOULD be considered.

SYS.3.2.3.A19 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.3.A20 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.3.A21 Installation of Apps and Integration of the Apple App Store (S)

To ensure that the required apps are sufficiently available to authorised users at the necessary time, consideration SHOULD be given to integrating Apple Business Manager into the MDM infrastructure. Payments in the App Store SHOULD NOT be confirmed using biometrics.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.2.3 *iOS (for Enterprise)* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.3.2.3.A22 ELIMINATED (H)

This requirement has been eliminated.

SYS.3.2.3.A23 Using Automatic Deletion of Configuration Profiles (H)

Devices that are continuously offline for a clearly defined period of time SHOULD lose their access to the corresponding organisation's internal infrastructure. At the end of the defined period or on a specific day, their configuration profiles SHOULD be deleted without the need for action on the part of those in charge of IT. If the user of such a device accesses their organisation's internal network before the period expires, this SHOULD reset the period until their configuration profile will be automatically deleted. If it is necessary to ensure that a user is still in possession of a given device, the user SHOULD be actively prompted to establish access within a set period of time. If no access is established before this period expires, the user's configuration profile SHOULD be automatically deleted.

SYS.3.2.3.A24 ELIMINATED (H)

This requirement has been eliminated.

SYS.3.2.3.A25 Using the Configuration Option for AirPrint (H)

Approved AirPrint printers SHOULD be provided to users by means of a configuration profile. In order to prevent users from printing information on untrusted printers, all communication links SHOULD always be routed through an organisation’s infrastructure systems.

SYS.3.2.3.A26 No Connections to Host Systems (H)

To prevent iOS-based devices from being connected to other IT systems in an unauthorised manner, users SHOULD only be able to connect iOS-based devices to a corresponding MDM system.

SYS.3.2.3.A27 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

In its publications on cyber security, the BSI has published the document BSI-CS 074, “iOS-Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit” [iOS Configuration Recommendation Based on the Operating System's Own Resources for Use with Enhanced Security], 2015.

In the context of the topics of this module, Apple provides additional support information, including:

- Apple Configurator: https://support.apple.com/de-de/apple-configurator
- Apple Security Updates: https://support.apple.com/en-us/HT1222
- Obsolete and vintage products: https://support.apple.com/de-de/HT201624
- Apple Business Manager: https://business.apple.com
- Support for companies and education institutions: https://www.apple.com/de/support/business-education/

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.3.2.3 *iOS (for Enterprise)*.

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.35 Coercion, Blackmail or Corruption

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.46 Loss of Integrity of Sensitive Information

SYS.3.2.4 Android

1. Description

1.1. Introduction

Google's Android operating system is commonly used on smartphones and tablets. Since version 4, Android has been gradually implementing protections for business use. For example, functions that enable organisations to administrate Android devices have been integrated. The number of administration policies supported by Android also increases with every new version, and there are manufacturer-specific expansions that enable additional policies.

1.2. Objective

The objective of this module is to provide information on typical threats related to Android and to show how Android-based devices can be used securely in organisations. Moreover, security policies can be created on the basis of the requirements stated in the module.

1.3. Scoping and Modelling

Module SYS.3.2.4 *Android* must be applied to all smartphones and tablets running the Google Android operating system that are used for business purposes.

This module includes basic specifications which must be observed and fulfilled when operating Android-based devices. General and comprehensive requirements for the operation of smartphones and tablets are not part of this module; they are covered in module SYS.3.2.1 *General Smartphones and Tablets* and must also be implemented for the use of Android-based devices. The requirements for the central administration of Android devices using an MDM system are also not part of this module. They are covered in module SYS.3.2.2 *Mobile Device Management (MDM)*.

2. Threat Landscape

For module SYS.3.2.4 *Android*, the following specific threats and vulnerabilities are of particular importance:

2.1. Disabling Security Features

The boot process of Android-based devices is secured with the help of a manufacturer certificate. Each subsequent step is checked before it is executed. This ensures that the Android operating system starts unchanged.

When the boot loader is unlocked, this chain of trust is interrupted so that a modified operating system can start. Such changes to the boot process are partly supported by the manufacturer, and boot loaders are also sometimes unlocked via vulnerabilities.

In such cases, the Android security concept is bypassed or overridden, giving rise to new threats that have to be secured in another way.

2.2. Malware for the Android Operating System

Due to their widespread use and open architecture, devices running the Android operating system are a popular target of malware, which is often installed by users themselves. On Android, it is relatively easy to install apps not only from Google's Play Store, but also from alternative sources or via direct download. In addition to the app stores monitored by Google, device manufacturers, and other providers, apps are also offered for installation from more dubious sources. Since it is not mandatory to install apps from the official Google Play Store on Android, an attacker could, for example, infect a popular app with malware and then make it available for download.

2.3. Lack of Updates for the Android Operating System

Some manufacturers provide smartphones and tablets with outdated Android versions, fail to provide regular updates, or provide no updates at all. Meanwhile, Android vulnerabilities are detected regularly, which poses a particular risk to such devices. As a consequence, known vulnerabilities on these devices are not eliminated and are therefore easy for attackers to exploit.

2.4. Risks Posed by User Accounts (Google Accounts) for Google Services

Users may utilise their Google account for central access to all Google services, including in connection with device management, recorded geographical locations, chat software, cloud storage, Google Play Store, music, books, movies, backups, bookmarks, or stored passwords for websites and synchronisation. Many other online service providers also use Google accounts for authenticating users.

If an attacker can authenticate themselves with a stolen Google account, they can use all the services connected to this identity. The attacker may also access the data stored there, locate devices, or reset them from a remote location (deleting all their data in the process), for example.

2.5. Pre-Installed apps and Integrated Functions on Android-Based Devices

In the Android operating system, manufacturers of corresponding devices often deliver integrated and pre-installed apps, as well as connections to third-party services (Twitter, Facebook, etc). Users often cannot remove these apps on their own. This increases the range of possible attacks on the Android operating system. In many cases, direct connections to third-party services are also undesirable in organisations.

Overall, the deep integration of third-party apps and interfaces increases the risk that a device will be infected with malware or that an attacker may gain unauthorised access to confidential information.

3. Requirements

The specific requirements of module SYS.3.2.4 *Android* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module SYS.3.2.4 *Android*, the following requirements MUST be implemented as a matter of priority:

SYS.3.2.4.A1 ELIMINATED (B)

This requirement has been eliminated.

3.2. Standard Requirements

For module SYS.3.2.4 *Android*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

SYS.3.2.4.A2 Disabling Developer Options (S)

The developer options SHOULD be disabled on all Android-based devices.

SYS.3.2.4.A3 Using Multi-User and Guest Mode (S)

Whether a device may be shared with other persons SHOULD be regulated. Whether multi-user or guest mode must be used for this purpose SHOULD be specified. Users on Android-based devices SHOULD be natural persons.

SYS.3.2.4.A4 ELIMINATED (S)

This requirement has been eliminated.

SYS.3.2.4.A5 Advanced Security Settings (S)

Only the approved security apps SHOULD be entered as device administrators or "Trust Agents". This SHOULD be checked regularly.

Furthermore, only authorised apps SHOULD be able to access usage data and notifications.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.2.4 *Android* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.3.2.4.A6 ELIMINATED (H)

This requirement has been eliminated.

SYS.3.2.4.A7 ELIMINATED (H)

This requirement has been eliminated.

4. Additional Information

4.1. Useful Resources

No further information is available for module SYS.3.2.4 Android.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security

objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.3.2.4 *Android*.

G 0.14 Interception of Information / Espionage

G 0.21 Manipulation of Hardware or Software

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.38 Misuse of Personal Information

G 0.41 Sabotage

G 0.46 Loss of Integrity of Sensitive Information

SYS.3.3 Mobile Telephones

1. Description

1.1. Introduction

The mobile phones considered in this module, which are also known as “feature phones” or "dumbphones", have fewer features than a smartphone, but offer more than just telephony functions. These mobile phones can also have a camera for videos and photos, an appointment calendar, e-mail programs, games, an MP3 player, or a radio receiver. "Classic" mobile phones do not usually have a touch screen or an operating system on which additional apps can be installed. The lack of these functions distinguishes a conventional mobile phone from a smartphone.

A mobile telephone is characterised by its internationally unambiguous serial number (International Mobile Equipment Identity, or IMEI). Mobile phone users are identified by their SIM cards, which are issued by mobile phone providers upon entry into a contract.

1.2. Objective

The aim of this module is to identify typical hazards that can occur when using mobile phones and to secure information stored on or transmitted by mobile phones.

1.3. Scoping and Modelling

Module SYS.3.3 *Mobile Telephones* must be applied to all mobile phones used for business purposes.

This module deals with general aspects of typical mobile phones, security aspects of telephony and messaging over mobile networks, and security aspects of using such devices. The module thus covers a wide range of different devices that can be connected to mobile telephone networks. Supplementary aspects that go beyond communication via a mobile network and handling related devices can be found in other modules of the IT-Grundschutz Compendium. Security requirements for smartphones and the operating systems used on them can be found in the SYS.3.2 *Tablets and Smartphones* module layer. Aspects of IT-based telephony are covered in module NET.4.2 *VoIP*. If the mobile phones under consideration use VPNs, module

NET.3.3 *VPN* should also be considered. For smartphones or tablets, module SYS.3.2.1 *General Smartphones and Tablets* must be applied.

2. Threat Landscape

For module SYS.3.3 *Mobile Telephones*, the following specific threats and vulnerabilities are of particular importance:

2.1. Inadequate Planning for the Purchase of Mobile Phones

If information on the relevant features of mobile phones to be purchased is not gathered during the planning phase, urgently required functions may not be available. If specific mobile phone standards are not supported, the devices will not be usable in certain countries. In the worst case, their range of functions will not correspond to the intended purposes and render the devices entirely unusable. There are often additional general conditions that must be fulfilled to enable the use of such devices. These include, for example, security features that are often not obvious at first glance, but can lead to availability and confidentiality issues when deployed.

2.2. Loss of a Mobile Phone

Since mobile phones are usually small and constantly carried around, they can easily be forgotten, lost, or stolen. In addition to the resulting economic damage, the loss of the confidentiality and integrity of the data on the devices is particularly serious. An attacker may use a stolen mobile phone to access an organisation's critical information. Enabling the corresponding user to work again also entails costs and effort.

2.3. Carelessness in Handling Mobile Telephony Information

Employee inattentiveness and carelessness with mobile phones may allow third parties to access sensitive information. Information can be overheard or recorded during telephone conversations, for example, or messages can be read as they are being written.

2.4. Unauthorised Private Use of a Mobile Business Phone

Mobile business phones can be used without permission for private purposes. Negligence and carelessness can cause problems for an organisation's information security—for example, when private and business content are mixed. In this way, unauthorised persons could gain knowledge of an organisation’s internal affairs. If mobile business phones are used privately, additional costs may also arise for the respective organisation.

2.5. Mobile Telephone Failure

There can be several reasons for mobile telephone failure. A user may fail to charge their device's battery, or the battery may have lost its ability to hold a charge. A user may also have forgotten their access password or PIN and may no longer be able to use their device. Devices can also become locked if several incorrect access codes are entered by a user. If a phone is not

handled with care, it may become damaged when dropped, for example. In all of these instances, the corresponding user will be unreachable and unable to contact others using their mobile phone.

2.6. Analysis of Call Data Relating to the Use of Mobile Phones

The inherent features of mobile communication mean it is impossible to prevent transmitted signals being listened to and recorded without permission by those willing to invest the effort. Due to technical reasons, connecting with mobile communication partners requires knowledge of their location when using most radio communication services. Location information can thus be used by network operators or service providers to create movement profiles.

2.7. Eavesdropping on Indoor Conversations over Mobile Phones

Mobile phones can be used to record or listen in on conversations unnoticed. If mobile phones are brought to meetings, they may be used to establish connections to unauthorised listeners. Many mobile phones are equipped with a speaker function that allows them to record conversations in an entire room with ease. Since it is not always clear whether many devices are switched on or not, it is also not immediately apparent whether they are recording or eavesdropping on conversations.

2.8. Use of Obsolete Mobile Phones

Since smartphones are more versatile than conventional mobile phones, many manufacturers now exclusively offer smartphones. This means that the range of smartphones available clearly exceeds that of conventional mobile telephones; in fact, very few "dumbphones" are still produced. The low supply means that many mobile phones are used from old stocks. Old components such as batteries are often replaced by replicas from third-party manufacturers, allowing continued use of these mobile phones decades after their production.

The operating systems installed on obsolete mobile phones are often outdated and no longer developed. It is no longer possible to eliminate their software vulnerabilities by means of updates. The respective mobile phone manufacturer often no longer exists or has shifted its business to other markets. Therefore, it is often not possible to purchase original accessories and spare parts. In many cases, third-party manufacturers also no longer offer corresponding products for very old mobile phones. Even when third-party manufacturers do offer spare parts, there is no guarantee that these components will be of the same quality as the original parts. Replica batteries are often less powerful than the originals, for instance. In addition, it is often difficult to repair these devices or find a suitable contact person when one requires assistance.

3. Requirements

The specific requirements of module SYS.3.3 *Mobile Telephones* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions.

Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Responsible as a matter of principle	IT Operation Department
Further responsibilities	User

3.1. Basic Requirements

For module SYS.3.3 *Mobile Telephones*, the following requirements MUST be met as a matter of priority:

SYS.3.3.A1 Security Guidelines and Rules for the Use of Mobile Phones (B)

A security policy MUST be established with regard to the use and control of mobile phones. Each mobile phone user MUST be provided with a copy of the security policy. Regular checks MUST be carried out to ensure compliance with the security policy. The security policy on mobile phone use for business purposes SHOULD form part of the training provided to users on security safeguards.

SYS.3.3.A2 Blocking Lost Mobile Telephones [User] (B)

If a mobile phone is lost, the SIM card used in it MUST be blocked promptly. If possible, existing anti-theft mechanisms such as remote deletion or blocking SHOULD be used. All the information necessary to block the SIM card and mobile phone MUST be immediately at hand.

SYS.3.3.A3 Raising Employee Awareness and Providing Training on the Use of Mobile Telephones (B)

Employees MUST be made aware of the particular threats posed to information security by mobile phones. They MUST be familiar with the security features of mobile phones. Users MUST know how to lock mobile phones. Users MUST be advised on how mobile phones should be stored safely and correctly.

SYS.3.3.A4 Decommissioning and Properly Disposing of Mobile Telephones and the Memory Cards Used in Them (B)

Mobile phones MUST be reset to factory settings before disposal. A check MUST be carried out to confirm that all data has been deleted. It SHOULD also be ensured that mobile phones and any memory cards used in them are properly disposed of. If mobile phones and memory cards are collected and then disposed of at a later point in time and/or in larger quantities, they MUST be protected from unauthorised access until their disposal.

3.2. Standard Requirements

For module SYS.3.3 *Mobile Telephones*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

SYS.3.3.A5 Use of the Security Mechanisms of Mobile Telephones [User] (S)

The available security mechanisms SHOULD be used and pre-configured on mobile phones. SIM cards SHOULD be protected by secure PINs. The super PIN/PUK SHOULD only be used by the people in charge within the framework of defined processes. Mobile phones SHOULD be protected by device codes. If possible, devices SHOULD be reliant on their SIM cards (SIM lock).

SYS.3.3.A6 Mobile Telephone Updates [User] (S)

Regular checks SHOULD be carried out to determine whether there are any software updates for the mobile phones in use. The handling of updates SHOULD be regulated. If there are new software updates, the way in which users will be informed about them SHOULD be specified. Whether users are allowed to install updates themselves or are to hand in their mobile phones at a central location for this purpose SHOULD be specified.

SYS.3.3.A7 Acquisition of Mobile Telephones (S)

Before mobile phones components are acquired, a list of requirements SHOULD be created. The list of requirements SHOULD be used to evaluate the products available on the market. A product SHOULD be selected according to whether the manufacturer will offer updates for the planned period of use. It SHOULD be ensured that spare parts such as batteries and chargers can be procured in sufficient quality.

SYS.3.3.A8 Use of the Wireless Interfaces of Mobile Telephones [User] (S)

IrDA, WLAN, Bluetooth, and other wireless interfaces of mobile phones SHOULD be disabled as long as they are not needed.

SYS.3.3.A10 Secure Data Transmission via Mobile Phones [User] (S)

There SHOULD be rules defining the data which can be transmitted using mobile phones. The interfaces allowed for this SHOULD also be defined. A decision SHOULD also be made on how to encrypt the data as required.

SYS.3.3.A11 Precautions for Mobile Telephones [User] (S)

The data stored on mobile phones SHOULD be backed up to another medium at regular intervals. If a defective mobile phone needs to be repaired, all its data SHOULD be deleted and the device reset to the factory settings. Replacement devices SHOULD always be available to replace a failed mobile phone on short notice.

SYS.3.3.A12 Setting Up a Mobile Telephone Pool (S)

A device pool SHOULD be set up if the users of business mobile phones change regularly. The issue and return of mobile phones and accessories SHOULD be documented. Before they are issued, it SHOULD be ensured that mobile phones are charged and equipped with the programs and data the new owner will need. In addition, users SHOULD be made aware of

their obligation to comply with the relevant security policy. When devices are returned, they SHOULD be reset to factory settings.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.3 *Mobile Telephones* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.3.3.A9 Securing the Power Supply for Mobile Telephones [User] (H)

Appropriate measures SHOULD be taken to ensure a sustainable supply of energy to mobile phones. Replaceable batteries or power banks SHOULD be used as required.

SYS.3.3.A13 Protection Against Mobile Telephone Data Being Used to Create Movement Profiles [User] (H)

It SHOULD be clarified whether the creation of movement profiles by third parties can have a negative effect or is regarded as a problem. To prevent GPS positioning, this function SHOULD be switched off. To prevent tracking through the mobile communication network, mobile phones SHOULD be switched off and their batteries removed.

SYS.3.3.A14 Protection Against Call Number Identification During Use of Mobile Telephones [User] (H)

To prevent them from being associated with specific people, telephone numbers SHOULD be suppressed for outgoing calls. SMS and MMS messages SHOULD NOT be sent. Mobile phone numbers SHOULD NOT be published or passed on to unauthorised third parties.

SYS.3.3.A15 Protection Against Eavesdropping on Indoor Conversations Using Mobile Telephones (H)

To ensure that confidential information cannot be subject to eavesdropping, mobile phones SHOULD NOT be taken into rooms used for confidential meetings and conversations. If necessary, this mobile phone ban SHOULD be enforced by detectors.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for the use of mobile devices in the standard ISO/IEC 27001:2013, especially in annex A, A.6.2.1 (*Mobile Device Policy*).

The National Institute of Standards and Technology (NIST) has published NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4, December 2014.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.3.3 *Mobile Telephones*.

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.31 Incorrect Use or Administration of Devices and Systems

Federal Office
for Information Security

SYS.4.1 Printers, Copiers, and All-in-One Devices

1. Description

1.1. Introduction

Today's printers, copiers, and all-in-one devices are complex devices which, in addition to mechanical components, contain their own operating systems and provide server services and functions. Since these devices often process confidential information, they must be protected along with the rest of an organisation's print and scan infrastructure.

All-in-one devices are devices that offer several paper-processing functions, such as printing, copying, scanning, and sending and receiving fax documents.

For many business processes, paper is still used as an information medium today. This makes printers, copiers, and all-in-one devices important components of IT infrastructure. If such devices fail or falsified documents are printed out, this can sometimes affect critical processes and lead to considerable economic losses.

1.2. Objective

This module describes how printers, copiers, and all-in-one devices can be operated safely so that information is not extracted from these devices and the security of the rest of the internal IT infrastructure at hand is not impaired.

1.3. Scoping and Modelling

Module SYS.4.1. *Printers, Copiers, and All-in-One Devices* must be applied to each printer, copier, and all-in-one device in the information domain under consideration.

This module covers the security of printers, copiers, and all-in-one devices. Networked document scanners or those connected locally to IT systems are not explicitly considered. However, corresponding risks and requirements can be derived from those described for all-in-one devices. Similarly, networked fax machines are not considered separately. The risks and

requirements cited for fax functions in this module therefore also apply to this type of device. In addition, the requirements of module NET.4.3 *Fax Machines and Fax Servers* should be considered.

Printers, copiers, and all-in-one devices are often connected to data networks so that multiple users can use them. In addition to wired connections, some devices can also be connected directly to a WLAN. Recommendations for this are included in sub-layer NET *Networks and Communication* modules of the IT-Grundschutz Compendium, such as in module *NET.2.2 WLAN Usage*.

Printers, copiers, and all-in-one devices often contain confidential information that remains on the devices after they are taken out of service. Leased equipment is often replaced after a predetermined period or frequency of use, depending on the specific contract in question. At the latest, they are returned when the corresponding leasing contract expires. Paper and other equipment may also contain confidential information. Before these devices and resources are discarded, exchanged, repaired, or returned, all sensitive information must be deleted from them. Recommendations in this regard are not covered in this module. They can be found in module CON.6 *Deleting and Destroying Data and Devices*.

Print servers are systems with print queues, print job management features, and possible other functions, such as driver distribution or secure printing. For each print server, the general and operating-system-specific security requirements for servers must be met. Instead of being covered here, these requirements are described in module SYS.1.1 *General Server* and the respective operating-system-specific server modules.

An essential focus in securing printers, copiers, and all-in-one devices lies on regularly updating their software to close software vulnerabilities. This module does not deal with this aspect, however. Corresponding requirements are included in module OPS.1.1.3 *Patch and Change Management*.

2. Threat Landscape

For module SYS.4.1 *Printers, Copiers, and All-in-One Devices*, the following specific threats and vulnerabilities are of particular importance:

2.1. Unauthorised Access to Printed Documents

Printed documents often remain in the output tray of central printers and all-in-one devices for a longer period of time—for example, because users first print out several files and later collect them all together. It is also possible that the wrong printer was selected on a client and the documents are thus not in the expected location. Since floor or department printers are utilised by many users, unauthorised persons can also view sensitive information or take it with them.

Printouts left in the output trays of decentralised workstation printers that are located in the immediate vicinity of users' offices are also a risk. This is because people who have access to these rooms could also view or remove the printouts.

Fax documents and printed transmission logs in output trays pose a further risk: In addition to fax numbers, dates, times, and page numbers, they often contain a scaled-down image of the first page. Since such logs are only output after a fax has been sent or a transmission error has occurred, they could also remain in the machine for a longer period of time or not be picked up at all. This may leave confidential information unattended in the output tray where, in the worst case, it could be stolen.

Uncollected documents will also eventually be disposed of by users. Here, printouts are often thrown into a random waste basket nearby instead of being securely shredding (especially when they contain sensitive information). Such information can therefore reach the public waste disposal system and potentially fall into the hands of third parties.

Many teleworking locations are also equipped with a printer or an all-in-one device. This is another case in which sensitive information can be disclosed.

2.2. Visibility of Metadata

A print job usually includes metadata that contains the respective user ID, date, time, and the name of the print job. This data is displayed on the control panel and web server of many printers and all-in-one devices. The name of the print job is often derived from the name of the digital document in question. If a printer has an integrated web server, confidential processes can often be viewed via a browser. The metadata on print servers is also visible in plain text unless it is anonymised. This could allow third parties to obtain confidential information. Many devices also allow print jobs to be saved so that they can be printed out later after authentication with a PIN. This is another case in which the name of all available documents is displayed on the control panel of an output device.

Some printers and copiers print “yellow dots” (also referred to as machine identification code, tracking dots, or secret dots) on paper. These often undocumented watermarks, which may include the date, time, and the serial number of the printer, are hardly visible to the naked eye. In this way, a printout can be directly associated with an organisation or a specific user and thus traced back to the author. In addition to the consequences regarding data protection laws, information might accidentally leave an organisation in this way.

Fax logs can also be printed without access protection on many all-in-one devices. Even if they only list telephone numbers, dates, times and numbers of pages, they make it possible to draw conclusions about personal data or business transactions.

2.3. Insufficient Protection of Stored Information

Printers, copiers, and all-in-one devices are often equipped with non-volatile storage on which information is stored temporarily or for longer periods of time. For example, address books, documents, fax files, and print jobs are stored there. If this information is not adequately protected, third parties can access and read it. Under certain circumstances, attackers can even reconstruct information that has already been deleted if unsafe deletion methods were used.

Data can also be stored and read on a device via network protocols. Printers and all-in-one devices with storage media can often be used as unauthorised file servers if they are not

secured. In this way, uncontrolled information that is not taken into account in the respective backup concept can be stored in a decentralised manner.

2.4. Unencrypted Communication

Print and scan data is often transmitted over networks in unencrypted form. This allows attackers to intercept transmitted documents. Print files that are temporarily stored on print servers can also be read. This applies to central scanning and document processing systems, as well.

Unencrypted communication interfaces for the administration of such devices present further sources of danger. If, for example, printers are accessed via HTTP, SNMPv2, or Telnet, the information involved is not protected when it is transmitted. This endangers device passwords and other access information.

2.5. Unauthorised Sending of Information

Many all-in-one devices can send digitised paper documents by e-mail and fax. Without special precautions, information can be deliberately or accidentally transmitted to unauthorised recipients this way. Users could, for example, enter recipient addresses or telephone numbers incorrectly. As a result, sensitive data may be unintentionally sent to the wrong recipient. In addition, attackers can use an e-mail or fax function to quickly send confidential documents to the outside world.

Many networked printers can be configured to receive print jobs from the Internet via e-mail and send scanned documents as e-mail attachments. Here, the user-defined input field for the sender's address can be misused to send e-mails under a different name to internal and external recipients.

2.6. Uncontrolled Data Exchange via Memory Interfaces on Printers, Copiers, and All-in-One Devices

Documents on paper can be quickly copied using all-in-one devices. USB or SD ports also make it possible to digitise even large quantities of paper documents directly and store them on USB pen drives or SD cards without any controls. These interfaces also make it possible to print documents stored on such media.

If printers, copiers, or all-in-one devices are connected to a data network or directly to clients, IT systems can often also directly access the storage media connected to these devices. Even if the integration of storage media is technically prevented on IT systems themselves, this work-around via storage interfaces makes it possible to copy information in an uncontrolled manner.

In this way, (malicious) software can spread to the clients connected to all-in-one devices or into an organisation's data network via the devices' storage interfaces. Meanwhile, confidential (paper) documents can also be digitised unnoticed and stolen in an untraceable manner.

2.7. Inadequately Secured Network Access of Printers, Copiers, and All-in-One Devices

Firewalls between LANs and the Internet are often configured to allow entire subnets to access the Internet. At the same time, printers and all-in-one devices are often assigned to the same subnet as clients. This means, for example, that network printers can also access information on the Internet. Even if an organisation's IT systems only access the Internet via a proxy, printers, copiers, and all-in-one devices can use the proxy, as well. If connections from the Internet to the devices are not rejected by the firewall, this can allow leaks of sensitive information from the organisation's data network under some circumstances. By the same token, a network-capable printer could also receive and distribute unwanted data from the Internet. A network printer may therefore become an opening for attacks from the Internet.

2.8. Poor Access Protection for Device Administration

Networked printers, copiers, and all-in-one devices can be managed from their control panels and built-in web servers. When such devices are delivered, they usually have a manufacturer-specific default password (or none at all). If this password is not changed or none is set, a device can be accessed very easily.

Many organisations also use common passwords for all their printers and all-in-one devices are rarely change them. As a result, they are often known to many internal and external persons, which makes it easy for unauthorised third parties to access the devices.

In addition, printers and all-in-one devices can be reset to factory settings via boot menus. This also affects their security settings. For example, the device password often no longer exists after a printer or all-in-one device has been reset to its factory settings. Unprotected boot menus simplify administration, but reduce security at the same time.

Printers, copiers, and all-in-one devices are equipped with numerous network protocols. All these protocols are usually activated on delivery. This could allow attackers, for example, to access the device settings and modify them to extract sensitive information from the network.

Many devices can transfer their control panel to a support representative via the network. However, this can also be used to read confidential entries made by users on the control panel.

Larger organisations usually have multiple printers, copiers, and all-in-one devices. Device management software is often used to manage and monitor them efficiently. However, many organisations do not adequately protect this software from unauthorised access because it is perceived as a less critical system. This allows individual or all devices to be changed unintentionally or deliberately.

3. Requirements

The specific requirements of module SYS.4.1 *Printers, Copiers, and All-in-One devices* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions.

Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	Chief Information Security Officer (CISO)

3.1. Basic Requirements

For module SYS.4.1 *Printers, Copiers, and All-in-One Devices*, the following requirements MUST be implemented as a matter of priority:

SYS.4.1.A1 Planning the Use of Printers, Copiers, and All-in-One Devices (B)

Before printers, copiers, and all-in-one devices are procured, their secure use MUST be planned. In doing so, the following criteria should be taken into consideration:

- support of secure protocols for data transmission and administration
- encryption of stored information
- authentication of users directly on each device
- use of physical protection mechanisms, such as anti-theft eyelets or device locks
- existence of a reliable and efficient automatic page feeder on scanning units
- support for suitable data formats
- support for patch codes and bar codes for document separation and transfer of meta information (if required)
- existence of a function for secure storage deletion
- availability of regular updates and maintenance contracts

The locations where devices may be situated MUST be specified. In addition, it MUST be defined who may access printers, copiers, and all-in-one devices. The results should be documented in a basic concept.

SYS.4.1.A2 Suitable Siting and Access to Printers, Copiers, and All-in-One Devices (B)

The IT Operation Department MUST set up and secure printers, copiers, and all-in-one devices so that only authorised users can use the devices and access processed information. In addition, it MUST be ensured that only authorised persons can administer, maintain, and repair the devices. Confidentiality agreements MUST be established in writing with service providers (e.g. for maintenance).

Printers, copiers, and all-in-one devices MUST be set up with device passwords to block access to their web servers and administration control panels. They MUST comply with the respective organisation's identity and authorisation management requirements in this regard.

SYS.4.1.A3 ELIMINATED (B)

This requirement has been eliminated.

SYS.4.1.A12 ELIMINATED (B)

This requirement has been eliminated.

SYS.4.1.A13 ELIMINATED (B)

This requirement has been eliminated.

SYS.4.1.A22 Proper Disposal of Printed Documents (B)

Printed documents containing confidential information that are no longer required MUST be disposed of appropriately. If home workstations are equipped with printers, copiers, or all-in-one devices, it SHOULD be ensured that information printed there can also be suitably destroyed directly on site when it is no longer needed.

3.2. Standard Requirements

For module SYS.4.1 *Printers, Copiers, and All-in-One Devices*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

SYS.4.1.A4 Drawing Up a Security Policy for the Use of Printers, Copiers, and All-in-One Devices (S)

Organisations SHOULD develop a security policy for printers, copiers, and all-in-one devices. It SHOULD regulate the requirements and specifications for the information security of such devices and how they are to be met. It SHOULD also specify which functions may be administered or used by which users under which conditions.

SYS.4.1.A5 Drawing Up User Guidelines for Handling Printers, Copiers, and All-in-One Devices [Chief Information Security Officer (CISO)] (S)

A user guideline SHOULD also be created that summarises all the security requirements for handling printers and all-in-one devices in a clear and comprehensible manner. All users SHOULD be familiar with the guideline.

SYS.4.1.A6 ELIMINATED (S)

This requirement has been eliminated.

SYS.4.1.A7 Restriction of Remote Administrative Access to Printers, Copiers, and All-in-One Devices (S)

The IT Operation Department SHOULD ensure that only a clearly defined group of administrators and service technicians have remote administrative access to printers, copiers, and all-in-one devices. This SHOULD also be ensured if the organisation in question uses central device management software.

It SHOULD be specified whether control panel displays can be viewed via a data network. If this is desired, such displays SHOULD only be transferable to employees in the IT Operation Department. This SHOULD also be agreed with the users concerned.

SYS.4.1.A8 ELIMINATED (S)

This requirement has been eliminated.

SYS.4.1.A9 ELIMINATED (S)

This requirement has been eliminated.

SYS.4.1.A10 ELIMINATED (S)

This requirement has been eliminated.

SYS.4.1.A11 Restricting the Connection of Printers, Copiers, and All-in-One Devices (S)

The IT Operation Department SHOULD ensure that network-enabled printers, copiers, and all-in-one devices cannot be reached from external networks. When connecting all-in-one devices to the telephone network, it SHOULD be ensured that no uncontrolled data connections can be established between an organisation's data network and the telephone network. Network printers and all-in-one devices SHOULD be operated in their own network segment and kept separate from an organisation's clients and servers.

SYS.4.1.A15 Encryption of Information for Printers, Copiers, and All-in-One Devices (S)

If possible, all information stored on internal non-volatile storage media SHOULD be encrypted. Print jobs SHOULD also be transmitted in an encrypted form if possible.

SYS.4.1.A17 Protection of Payloads and Metadata (S)

Payload data and metadata such as print jobs and scan files SHOULD only be stored on devices for as short a time as possible. Data SHOULD be deleted automatically after a predefined amount of time. File servers on such devices and functions such as “scan to device memory” SHOULD be disabled by the IT Operation Department. The protocols and functions required for this SHOULD be blocked whenever possible.

In general, the IT Operation Department SHOULD ensure that no metadata is visible to unauthorised parties. Organisations SHOULD regulate how printouts with metadata are to be passed on to third parties.

SYS.4.1.A18 Configuration of Printers, Copiers, and All-in-One Devices (S)

All printers and all-in-one devices SHOULD only be configurable by the IT Operation Department. Unused device functions SHOULD be switched off. In particular, all unnecessary data and network interfaces of printers, copiers, and all-in-one devices SHOULD be disabled.

The devices SHOULD be managed exclusively via encrypted protocols such as HTTPS and SNMPv3. All protocols that allow unencrypted access to printers and all-in-one devices SHOULD be replaced by encrypted ones by the IT Operation Department or switched off. This SHOULD be implemented in particular for protocols that can be used to change a device's configuration (e.g. SNMP, Telnet, PJL).

SYS.4.1.A19 ELIMINATED (S)

This requirement has been eliminated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.4.1 *Printers, Copiers, and All-in-One Devices* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.4.1.A14 Authentication and Authorisation for Printers, Copiers, and All-in-One Devices (H)

Only authorised persons SHOULD be able to access printed or copied documents. If possible, only central printers, copiers, and all-in-one devices SHOULD be used that require user authentication before starting printing tasks ("secure print"). After users have authenticated themselves, only their own print jobs SHOULD be visible. Only the functions necessary for each respective user SHOULD be enabled.

SYS.4.1.A16 Reducing Downtimes for Printers, Copiers, and All-in-One Devices (H)

To minimise the downtime of printers, copiers, and all-in-one devices, the safeguards taken SHOULD include the following:

- replacement devices should be available
- an appropriate response time should be ensured in maintenance contracts
- a list of specialised suppliers should be maintained for the purpose of quickly purchasing replacement devices or spare parts
- a store of regularly required spare parts should be maintained if necessary

SYS.4.1.A20 Enhanced Information Protection for Printers, Copiers, and All-in-One Devices (C)

The names of print jobs SHOULD only be displayed in anonymised form on print servers. All interfaces for external storage media SHOULD be disabled. Furthermore, device-internal address books SHOULD be disabled and alternative addressing methods (e.g. address search via LDAP) offered to users.

Printers and all-in-one devices with e-mail functionality SHOULD ensure that e-mails can only be sent using the e-mail address of an authenticated user. Documents SHOULD also only be sent to internal e-mail addresses.

Incoming fax documents and transmission reports SHOULD only be accessible to authorised users.

SYS.4.1.A21 Extended Protection of Printers, Copiers, and All-in-One Devices (H)

The IT Operation Department SHOULD regularly check the security settings of printers, copiers, and all-in-one devices and correct them if necessary. If an automated control and correction system is available, it SHOULD be used.

In addition, there SHOULD be a restriction on devices being reset to factory settings via their boot menus. It SHOULD be ensured that no firmware or additional software can be installed on printers and all-in-one devices that has not been verified and approved by the respective manufacturer.

4. Additional Information

4.1. Useful Resources

Within the framework of the Alliance for Cyber Security, the BSI offers recommendations in “Drucker und Multifunktionsgeräte im Netzwerk BSI-CS 015” [Printers and All-in-One Devices in the Network, BSI-CS 015] and “Sichere Passwörter in Embedded Devices (BSI-CS 069)” [Secure Passwords in Embedded Devices, BSI-CS 069]. In-depth information on printers, copiers, and all-in-one devices can also be found in the white paper “Datenschutz und Sicherheit in Druckinfrastrukturen” [Data Protection and Security in Printing Infrastructures], which was published by the ACS partner company mc² management consulting GmbH.

The National Institute of Standards and Technology (NIST) describes requirements for output devices such as printers, copiers, and all-in-one devices in Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”, especially in section PE-5, "Access Control for Output Devices”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.4.1 *Printers, Copiers, and All-in-One Devices*.

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

SYS.4.3 Embedded Systems

1. Description

1.1. Introduction

Embedded systems are information-processing systems that are integrated into a larger system or product. They take over control, regulation, and data processing tasks and are often not directly perceived by the user. Embedded systems can be found both in the field of advanced technology—in the aerospace, medical engineering, telecommunications, and automotive engineering sectors, for example—and in consumer and household appliances.

An embedded system consists of software and hardware that forms a functional unit and performs only one defined task. The software of embedded systems is referred to as firmware and is, in most cases, stored on flash memory, EPROM, EEPROM, or ROM. It cannot be exchanged by the user or can only be exchanged with special means and/or functions. It essentially consists of a boot loader, an operating system, and an application. Specialised systems can also run without an operating system. Although embedded systems are specialised devices, they are universal computers in contrast to pure hardware implementations (ASIC). Different CPU architectures or flexible, highly integrated field programmable gate array (FPGA) components can be used as platforms.

Embedded systems either have no user interface or use special peripheral equipment, such as functional keys, rotary switches, or displays designed for the respective intended purpose. The scope of output units ranges from a simple signal lamp to LCDs and complex cockpit displays. Embedded systems frequently communicate via data buses which are networked heterogeneously in complex systems. In addition, peripheral components such as sensors and actuators can also be connected via several different and multi-channel input/output ports. Some types of embedded systems also have a web interface through which they can be configured via a browser.

1.2. Objective

The objective of this module is to provide information on typical threats to embedded systems and show how these systems can be used securely in organisations.

1.3. Scoping and Modelling

Module SYS.4.3 *Embedded Systems* must always be applied when embedded systems are used. It must be applied to all the embedded systems in the information domain under consideration.

This module deals with embedded systems in general. It is applicable to a wide range of different embedded systems. Dedicated security properties, such as those of operating and display systems or specific hardware and software architectures, are not described in more detail here. The security aspects of embedded systems used in industrial control systems are also not specifically addressed. In these areas, the modules of the IND *Industrial IT* layer should be consulted in addition to the present module. Specific security aspects of IoT systems are not part of this module either. IoT systems are networked devices or objects with additional smart functions that (unlike embedded systems) are not integrated into a larger system or product. Due to their wireless connections to data networks, such systems are subject to different security requirements. These are covered in SYS.4.4 *General IoT Devices*.

Chip cards are a special application of embedded systems. These cards are usually equipped with a processor, random access memory, and I/O interfaces. This module covers the general security aspects relating to chip cards, but not the specific aspects.

2. Threat Landscape

For module SYS.4.3 *Embedded Systems*, the following specific threats and vulnerabilities are of particular importance:

2.1. Inadequate Security Requirements for Developing Embedded Systems

For cost reasons, information security often plays a less important role during the development of embedded systems than, for example, performance or reliability. However, if security requirements are not sufficiently addressed in one or more development phases, the resulting embedded systems may have serious vulnerabilities.

2.2. Unprotected Input/Output Interfaces in Embedded Systems

The interfaces in embedded systems are potential points of attack. This applies to interfaces on all levels of the ISO/OSI layer model and all transmission media used. If access via these interfaces is not controlled or if the control mechanisms used are too weak, attackers could infiltrate the system, read and write data without authorisation, and initiate subsequent attacks. They could also connect spying or sabotage devices such as miniaturised controllers or data loggers without anyone noticing.

If such devices are connected to a system's I/O ports at the microcontroller level, signals could be fed into the I/O registers via the I/O lines or output signals could be recorded.

If there is a reset input, attackers could control it and temporarily shut down the system.

2.3. Inadequate Physical Protection of Embedded Systems

If embedded systems are easy to access physically, attackers could destroy or damage them (e.g. using mechanical force, short circuits, or excess voltage). They could also access the electronic components (e.g. IC pins or contacts) and thus record electrical signals unnoticed with corresponding measuring and analysis tools, or feed in signals themselves. When attackers gain possession of an embedded system, they can use physical procedures to read and manipulate data or access data that has not been securely deleted. This may result in the confidentiality, integrity, or availability of the information stored on the embedded system being compromised.

2.4. Hardware Failure and Hardware Errors with Embedded Systems

Environmental influences such as electromagnetic interference, temperature fluctuations, an unstable power supply, manufacturing defects, and production tolerances can cause embedded systems to fail. Normal or premature wear can also cause such systems to fail. This could also severely affect the surrounding systems.

2.5. Installation (Flashing) of Manipulated Software Updates on Embedded Systems

Many embedded systems store their software on flash memory or EEPROM and provide the ability to update their firmware by connecting a programming device via a data interface or network connection. However, an attacker can also use this to import manipulated software updates and thus change how a system functions. The original tasks of a system can thus be interrupted or manipulated.

2.6. Side-Channel Attacks on Embedded Crypto Systems

Attackers could use a side-channel attack to break encryptions or signatures by exploiting observable properties of the physical implementation of a cryptosystem. For example, they could use the energy consumption of a microprocessor during cryptographic calculations to draw conclusions about related keys and the operations being carried out. They could also conduct computational timing attacks, microarchitectural attacks, or (semi-) invasive attacks. In 2011, scientists managed to identify the secret key of a TLS/SSL server that was using the Digital Signature Algorithm (DSA) with elliptic-curve cryptography. The attack was based on the fact that the time required for multiplication makes it possible to draw conclusions about the corresponding operands.

2.7. Penetration and Manipulation via the Communication Interface of Embedded Systems

Embedded systems are often limited with regard to code size, time behaviour, energy consumption, and size and weight. They are thus often not equipped with sufficient security functions, such as strong cryptography. However, modern embedded systems are increasingly interconnected by widespread techniques and protocols, and are therefore potentially vulnerable.

Attackers could try to manipulate the data or software on an embedded system by abusing the default communication interfaces and protocols for their own purposes. If IP communications and Ethernet, WLAN, Bluetooth, and mobile or digital radio interfaces are not sufficiently secured, for example, an attacker may take over connections, forge messages, or enter a system and perform subsequent attacks. Furthermore, an attacker can also try to enter a system using other available communication interfaces, such as USB ports.

2.8. Use of Forged Components

During the production process or when components are replaced during servicing, forged components may be installed in embedded systems. Since counterfeits of many components are in circulation, this can also happen unintentionally. Counterfeit components often work less reliably than the original components. As a result, functions may fail or work incorrectly. Attackers may also develop a device or component that looks exactly the same as the original, but contains manipulated functions. Such components could create backdoors, manipulate individual functions, or reduce availability, for example.

3. Requirements

The specific requirements of module SYS.4.3 *Embedded Systems* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Planner, Procurement Department, Developer

3.1. Basic Requirements

For module SYS.4.3 *Embedded Systems*, the following requirements MUST be met as a matter of priority:

SYS.4.3.A1 Rules for Handling Embedded Systems (B)

A person MUST be appointed to be in charge of embedded systems in order for them to operate smoothly. All users and administrators MUST be informed of any codes of conduct and reporting channels in the event of failures, malfunctions, or suspected security incidents.

Embedded systems MUST be configured securely. These configurations SHOULD be documented. Regulations SHOULD be defined for testing integrity and functionality.

SYS.4.3.A2 Disabling Unused Interfaces and Services of Embedded Systems [Developer] (B)

It MUST be ensured that only required interfaces can be accessed. Only the required services MAY be activated. Access to application interfaces MUST be protected by means of secure authentication.

SYS.4.3.A3 Logging Security-Relevant Events in Embedded Systems (B)

Security breaches MUST be logged (see OPS.1.1.5 *Logging*). If electronic logging is not feasible or only possible to a very limited extent, alternative organisational rules SHOULD be created and implemented.

3.2. Standard Requirements

For module SYS.4.3 *Embedded Systems*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

SYS.4.3.A4 Creating Procurement Criteria for Embedded Systems [Procurement Department] (S)

Before an embedded system is procured, a requirements list MUST be drawn up that can be used to evaluate the systems or components available on the market. The requirements list SHOULD include the following security-relevant aspects at minimum:

- aspects of material security
- requirements for hardware security properties
- requirements for software security properties
- support for a Trusted Platform Module (TPM) through the operating system
- security aspects of the development environment
- organisational security aspects

SYS.4.3.A5 Protecting Embedded Systems Against Damaging Environmental Influences [Developer, Planner] (S)

It SHOULD be ensured that embedded systems are adequately protected from harmful environmental influences according to their intended use and location. The requirements for this SHOULD be analysed right from the planning phase. It SHOULD also be ensured that the precautions taken to protect individual components from dust and contamination are compatible with the requirements of the overarching system at hand.

SYS.4.3.A6 Preventing Debugging Options for Embedded Systems [Developer] (S)

Possible debugging options SHOULD be removed from embedded systems as completely as possible. If on-chip debugging is used, it MUST be ensured that debugging functions cannot be used or activated by unauthorised persons.

It SHOULD also be ensured that no input interfaces for test signals or measuring points for connecting analysers can be activated or used by unauthorised persons. All hardware debugging interfaces SHOULD also be disabled.

SYS.4.3.A7 Hardware Realisation of the Features of Embedded Systems [Developer, Planner, Procurement Department] (S)

If embedded systems are developed in-house, security aspects SHOULD be taken into account when taking decisions on hardware and software design. Security aspects SHOULD also be taken into account when deciding to implement a particular hardware technology.

SYS.4.3.A8 Using a Secure Operating System for Embedded Systems [Developer, Planner, Procurement Department] (S)

The operating system used and the configuration of an embedded system SHOULD be suitable for its intended operation. The operating system SHOULD thus have sufficient security mechanisms for the task at hand. The required services and functions SHOULD be activated. The operating system SHOULD support the use of a Trusted Platform Module (TPM).

SYS.4.3.A9 Use of Cryptographic Processors or Coprocessors in Embedded Systems [Developer, Planner, Procurement Department] (S)

If an additional microcontroller is used for cryptographic calculations, its communication with the system microcontroller SHOULD be adequately secured. The required trust anchors SHOULD be realised for the embedded system in question. A chain of trust SHOULD also be implemented.

SYS.4.3.A10 Recovery of Embedded Systems (S)

Embedded systems SHOULD have rollback capabilities.

SYS.4.3.A11 Secure Disposal of Embedded Systems (S)

Prior to the disposal of embedded systems, all their data SHOULD be securely deleted. Their deletion (or destruction) SHOULD be documented.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.4.3 *Embedded Systems* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.4.3.A12 Selection of a Trustworthy Supplier and Logistics Chain and a Qualified Manufacturer for Embedded Systems [Procurement Department] (H)

Effective controls SHOULD be carried out in the logistics chain to ensure the following:

- embedded systems do not include any manipulated, falsified, or replaced components.
- embedded systems meet the respective specifications and no hidden functions have been implemented during manufacture.

- confidential information on embedded systems cannot be accessed by unauthorised persons

The companies involved SHOULD be demonstrably qualified.

SYS.4.3.A13 Use of a Certified Operating System [Developer, Planner, Procurement Department] (H)

The operating system in use SHOULD be evaluated at an adequate level according to a recognised standard.

SYS.4.3.A14 Secured and Authenticated Boot Process for Embedded Systems [Developer, Planner, Procurement Department] (H)

The boot process of an embedded system SHOULD be secured by the boot loader based on its ability to check the integrity of the operating system and only load it when it is classified as correct. By the same token, the operating system SHOULD also check the integrity of the boot loader.

A multi-stage boot concept SHOULD be used that can check the individual steps in a cryptographically secure manner. Secure hardware trust anchors SHOULD also be used. ARM Secure Boot SHOULD be used in ARM-based embedded systems. Secure Boot SHOULD be used with a Unified Extensible Firmware Interface (UEFI).

SYS.4.3.A15 Storage Protection in Embedded Systems [Developer, Planner, Procurement Department] (H)

Memory protection mechanisms SHOULD be considered right from the design of embedded systems. The type of storage protection and the number and size of the protected areas SHOULD be appropriate for this purpose.

SYS.4.3.A16 Tamper Protection for Embedded Systems [Planner] (H)

A tamper protection concept SHOULD be developed for embedded systems. Adequate mechanisms SHOULD be established to detect, record, and prevent tampering. Adequate guidelines SHOULD also be established on how to respond to tampering.

SYS.4.3.A17 Automatic Monitoring of Assembly Functions [Planner, Procurement Department] (H)

All the assemblies of an embedded system with higher availability and integrity requirements SHOULD be equipped with integrated self-testing equipment (built-in self-test, BIST). Tests SHOULD check the integrity of the system when it is turned on and at adequate intervals during its operation. Where possible, the self-test functions SHOULD also check assemblies' security functions and properties.

The integrity of the memory and I/O components SHOULD be checked regularly within the framework of the BIST. Existing BIST functions SHOULD be supplemented by the functions required if possible.

SYS.4.3.A18 Resistance of Embedded Systems to Side-Channel Attacks [Developer, Procurement Department] (H)

To make embedded systems resistant to side-channel attacks, appropriate precautions SHOULD be taken against non-invasive and (semi-) invasive side-channel attacks.

4. Additional Information

4.1. Useful Resources

In its document “ICS Security Compendium – Test Recommendations and Requirements for Component Suppliers”, the BSI provides assistance in testing ICS components and presents measures to avoid and detect vulnerabilities.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.4.3 *Embedded Systems*.

G 0.4 Pollution, Dust, Corrosion

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.46 Loss of Integrity of Sensitive Information

SYS.4.4 General IoT Devices

1. Description

1.1. Introduction

In contrast to classic end devices, those with Internet of Things (IoT) functions are networked devices or objects that have additional “smart” functions. IoT devices are usually connected wirelessly to data networks. Most of these devices can access information on the Internet and be reached via the same means. As a consequence, they may have effects on the information security of the entire corresponding information domain.

IoT devices such as smartwatches or other wearables can enter organisations when they are worn by employees or visitors. However, many organisations also procure and operate IoT devices themselves—including detectors for fire, gas, and other hazards; coffee machines; or building management elements such as cameras and HVAC (heating, ventilation and air conditioning) systems.

In general, a differentiation can be made between IoT devices that may be addressed directly and IoT devices that require a central controller. Devices that can be addressed directly are usually connected to a LAN with their own IP address and can act autonomously, or are managed by a central control unit. There are also IoT devices that communicate only directly with controllers (e.g. via radio networks such as Bluetooth or ZigBee) and thus do not connect directly to existing data networks.

1.2. Objective

The objective of this module is to secure IoT devices such that they impair neither the information security of one’s own organisation nor the security of external parties. As a consequence, both unauthorised data leaks and any manipulation of these devices should be avoided, especially with regard to attacks through third parties.

1.3. Scoping and Modelling

Module SYS.4.4 *General IoT Devices* must be applied to every device with functions related to the Internet of Things (IoT).

This module addresses IoT devices in general and should thus be applicable to a wide range of such devices. Dedicated security properties, such as those of operating and display systems or specific hardware and software architectures, are not described in more detail here.

Depending on the characteristics of the IoT devices, their interfaces to industrial control systems (ICS systems) or embedded systems may be fluid. Requirements for devices used in production and manufacturing can be found in the modules of the IND *Industrial IT* layer.

Embedded systems, on the other hand, are information-processing systems which are integrated into a larger system or product; assume control, regulation, and data processing tasks there; and are often not recognised directly by the user. Module SYS.4.3 *Embedded Systems* must be implemented for these systems.

Requirements for the radio links often used in connection with IoT devices can be found in the modules of the layer NET.2 *Radio Networks*.

The IoT devices used in the information domain under consideration must also be taken into account in identity and access management. To that end, module ORP.4 *Identity and Access Management* should be implemented.

2. Threat Landscape

For module SYS.4.4 *General IoT Devices*, the following specific threats and vulnerabilities are of particular importance:

2.1. Espionage using IoT Devices

The aspect of information security is typically given little or no attention in the development of IoT devices. As a consequence, it has often been possible in the past to misuse IoT devices to collect information on users and their areas of activity. For example, there have been repeated incidents in connection with networked and IP-based surveillance cameras:

- In 2013, several banks in various countries were compromised in the course of the "Carbanak" campaign with the help of surveillance cameras. The attackers obtained hundreds of millions. Within the framework of these attacks, the cameras were used to capture screen contents and keyboard input in the banks targeted.
- In 2014, the "Insecam" website was used to publicly disclose video images and streams from 73,000 poorly protected webcams.
- In 2015, the "Conficker" malware (which was already eight years old at the time) infected numerous bodycams of different federal and state police forces in Germany.

2.2. Use of UPnP

IoT devices integrated into LANs often automatically establish a connection to the Internet by configuring routers in their network using UPnP (universal plug-and-play) to facilitate port forwarding. The devices can then not only communicate in the local network, but are also visible and accessible outside the LAN. If a vulnerability in an IoT device is then exploited by an attacker, this device could become part of a botnet. In addition, further malware could be

infiltrated into the corresponding information domain. This vulnerability could also be exploited at a later time for further malicious activities.

2.3. Distributed Denial of Service (DDoS)

If IoT devices are not patched at regular intervals, known vulnerabilities will remain open and may be used for extensive attacks. One objective of an attack may be to integrate IoT devices into a bot network. In this case, they might be misused to execute DDoS attacks and restrict the availability of services, for example.

A DDoS attack of this kind was carried out on an Internet service provider at the end of October 2016. A botnet was used that consisted largely of IoT devices. Due to the large number of devices, the so-called Mirai bot network reached a bandwidth that vastly exceeded the previously known bot networks. The webcams, cameras, digital video recorders, routers, and printers that were already part of the botnet automatically scanned the Internet for further devices in order to infect them with malware and add them to the network.

2.4. Espionage Attacks Through Backdoors in IoT Devices

At the end of September 2016, it came to light that some models of surveillance cameras and room sensors had backdoors that allowed for espionage. In particular, this affected surveillance cameras used in data centres and server rooms. The backdoors apparently made it possible to access the image and video data of the cameras and copy this data to servers on the Internet. In this way, user and administration passwords may be compromised or device configurations, infrastructure details, and other confidential information may be made available to third parties, for example. This facilitates more comprehensive attacks by exploiting the habits of employees.

3. Requirements

The specific requirements of module SYS.4.4 *General IoT Devices* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Procurement Department, Building Services

3.1. Basic Requirements

For module SYS.4.4 *General IoT Devices*, the following requirements MUST be met as a matter of priority:

SYS.4.4.A1 Criteria for Using IoT Devices (B)

IoT devices MUST have update functions. The respective manufacturers MUST provide an update process. The devices MUST allow for appropriate authentication. Hard-coded access data MUST NOT be present in the devices.

SYS.4.4.A2 Authentication (B)

Appropriate authentication MUST be activated. IoT devices MUST be integrated into the corresponding organisation's identity and access management system.

SYS.4.4.A3 ELIMINATED (B)

This requirement has been eliminated.

SYS.4.4.A4 ELIMINATED (B)

This requirement has been eliminated.

SYS.4.4.A5 Restriction of Network Access (B)

The network access of IoT devices MUST be restricted to the required minimum. This SHOULD be monitored regularly. The following aspects should be taken into consideration in this regard:

- For traffic control at network gateways (e.g. by means of rules on firewalls and access control lists (ACLs) on routers), the incoming and outgoing connections permitted MUST be defined in advance.
- Routings on IoT devices and sensors SHOULD be configured restrictively, especially with regard to the suppression of default routes.
- IoT devices and sensors SHOULD be operated in a separate network segment that is only allowed to communicate with the network segment for management.
- Virtual private networks (VPNs) between networks with IoT devices, sensor networks, and management networks SHOULD be configured restrictively.
- The UPnP feature MUST be disabled on all routers.

3.2. Standard Requirements

For module SYS.4.4 *General IoT Devices*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

SYS.4.4.A6 Integration of IoT Devices into Organisation Security Policies (S)

Requirements for IoT devices SHOULD be specified in organisations' general security policies. This policy SHOULD be known to all persons who procure and operate IoT devices and be integral to their work. The implementation of the rules required by the policy SHOULD be reviewed regularly and the results documented in a sensible way.

SYS.4.4.A7 Planning the Use of IoT Devices (S)

To ensure secure operation of IoT devices, where and how these devices should be used SHOULD be planned in advance. Besides addressing aspects usually associated with

information security in the traditional sense, this planning SHOULD also consider normal operational aspects that entail requirements in the area of security. All decisions taken in the planning phase SHOULD be documented appropriately.

SYS.4.4.A8 Procurement Criteria for IoT Devices [Procurement Department] (S)

The CISO SHOULD also be involved in procuring IoT devices that do not have any obvious IT functionality. Prior to procuring IoT devices, the security requirements they must meet SHOULD be specified. When procuring IoT devices, aspects of material security and requirements regarding the security characteristics of the devices' software SHOULD be sufficiently considered. A requirements list SHOULD be drawn up that can be used to evaluate the products available on the market.

SYS.4.4.A9 Controlling the Use of IoT Devices (S)

A person SHOULD be put in charge of the operation of every IoT device. The persons in charge SHOULD be appropriately informed about handling their IoT devices.

SYS.4.4.A10 Secure Installation and Configuration of IoT Devices (S)

The framework conditions applicable to the installation and configuration of IoT devices SHOULD be defined. IoT devices SHOULD only be installed and configured by authorised persons (persons in charge of IoT devices, administrators, or service providers bound by contracts) in accordance with a defined process. All installation and configuration steps SHOULD be documented such that they can be understood and repeated by a qualified third party based on the documentation.

The basic settings of IoT devices SHOULD be checked and, where necessary, adapted to the specifications of the security policy in question. If possible, IoT devices SHOULD only be connected to data networks after installation and configuration are complete.

SYS.4.4.A11 Using Encrypted Data Transmission (S)

IoT devices SHOULD only transfer encrypted data.

SYS.4.4.A12 ELIMINATED (S)

This requirement has been eliminated.

SYS.4.4.A13 Deactivation and Uninstallation of Unnecessary Components (S)

Once IoT devices have been installed, the protocols, applications, and other tools that have been installed and enabled on them SHOULD be checked. Protocols, services, user IDs, and interfaces that are not required SHOULD be disabled or uninstalled entirely. The use of wireless interfaces that are not needed SHOULD be prevented.

If this is not possible using the device itself, services that are not required SHOULD be restricted using the corresponding firewall. The decisions taken SHOULD be documented such that the configurations selected for IoT devices can be determined.

SYS.4.4.A14 ELIMINATED (S)

This requirement has been eliminated.

SYS.4.4.A15 Restrictive Granting of Access Rights (S)

Access authorisations for IoT devices SHOULD be granted as restrictively as possible. If this is not possible using IoT devices themselves, it SHOULD be considered via the network.

SYS.4.4.A16 Elimination of Malware on IoT Devices (S)

The IT Operation Department SHOULD regularly obtain information as to whether the IoT devices used could become infected with malware and how it can be removed. Malware SHOULD be eliminated immediately. If the cause of an infection cannot be eliminated or a new infection cannot be effectively prevented, the affected IoT devices SHOULD no longer be used.

SYS.4.4.A17 Monitoring Network Traffic on IoT Devices (S)

Whether IoT devices or sensor systems communicate only with IT systems that are necessary for their operation SHOULD be monitored.

SYS.4.4.A18 Logging Security-Relevant Events on IoT Devices (S)

Security-relevant events SHOULD be logged automatically. If this is not possible using IoT devices themselves, routers and logging mechanisms of other IT systems SHOULD be used. The log data SHOULD be evaluated appropriately.

SYS.4.4.A19 Protection of Administration Interfaces (S)

Depending on whether IoT devices are administered locally; directly using the respective network; or using central, network-based tools, appropriate security precautions SHOULD be taken. Access to the administration interfaces of IoT devices SHOULD be restricted as follows:

- Network-based administration interfaces SHOULD be limited to authorised IT systems or network segments.
- Preference SHOULD be given to local administration interfaces on IoT devices or administration interfaces via local networks.

The methods used for administration SHOULD be defined in the corresponding security policy. IoT devices SHOULD be administered according to this security policy.

SYS.4.4.A20 Controlled Decommissioning of IoT Devices (S)

There SHOULD be an overview of the data stored in each location on IoT devices. A checklist which can be completed when decommissioning IoT devices SHOULD be created. This checklist SHOULD, at minimum, include aspects of backing up data that is still needed and the subsequent secure deletion of all data.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.4.4 *General IoT Devices* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.4.4.A21 Operational Environment and Power Supply [Building Services] (H)

It SHOULD be clarified whether IoT devices may be operated in the intended operational environment (i.e. taking the protection needs of other IT systems and data protection into account). IoT devices SHOULD be protected against theft, destruction, and manipulation in their operational environment.

It SHOULD be clarified whether an IoT device has certain requirements regarding its physical operational environment (e.g. humidity, temperature, energy supply). If required, additional safeguards SHOULD be implemented regarding the infrastructure at hand.

If IoT devices are operated using batteries, a procedure SHOULD be specified for regular functional testing and replacement of the batteries.

IoT devices SHOULD be protected against dust and pollution in accordance with their intended type and place of use.

SYS.4.4.A22 System Monitoring (H)

IoT devices SHOULD be integrated into an appropriate system monitoring concept. This concept SHOULD continuously monitor the system status and functionality of the IoT devices in use and report error states and threshold violations to the respective operating personnel. Whether the devices used meet the availability requirements at hand SHOULD be checked. Alternatively, it SHOULD be checked whether further safeguards are required, such as setting up a cluster or procuring standby devices.

SYS.4.4.A23 Auditing of IoT Devices (H)

All IoT devices in use SHOULD be checked at regular intervals.

SYS.4.4.A24 Secure Configuration and Usage of an Embedded Web Server (H)

Web servers integrated into IoT devices SHOULD be configured as restrictively as possible. Whenever possible, a web server of this kind SHOULD NOT be operated using a privileged account.

4. Additional Information

4.1. Useful resources

In the document “Security of IP-Based Surveillance Cameras”, the BSI provides an overview of the basic best practices for the secure operation of IP-based surveillance cameras.

The United States Department of Homeland Security (DHS) has published strategic principles for the security of IoT devices.

The Open Web Application Security Project (OWASP) Foundation offers best practices for the security of IoT devices.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.4.4 *General IoT Devices*.

G 0.2 Unfavourable Climatic Conditions

G 0.4 Pollution, Dust, Corrosion

G 0.8 Failure or Disruption of the Power Supply

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.40 Denial of Service

SYS.4.5 Removable Media

1. Description

1.1. Introduction

Removable media are often used to transport, store, or access data while on the move. Removable media include external hard drives, CD-ROMs, DVDs, memory cards, magnetic tapes, and USB pen drives.

Storage media can be classified according to whether they are read-only, write-once, or rewritable. There are also differences in the type of data storage (analogue or digital), the processing options available, and the form factor of media. There are removable storage media (e.g. built-in hard disks) and external data storage media (e.g. USB pen drives), for example.

1.2. Objective

This module is designed to show how removable media can be used in a secure manner. It also describes how to prevent the unintentional disclosure of information via removable media.

1.3. Scoping and Modelling

The SYS.4.5 *Removable Media* module must be applied to all removable media in the information domain under consideration.

This module deals with the security properties of removable media. The protection of the IT systems to which removable media can be connected is not covered in this module. Recommendations for this can be found in the modules SYS.1.1 *General Server* or SYS.2.1 *General Client*, as well as in the operating-system-specific modules.

Removable media store data electronically, magnetically, or in other ways that are not directly perceptible. They do not process any data themselves. The requirements for devices that are capable of this, such as smartphones and tablets, are listed in SYS.3.2.1 *General Smartphones and Tablets*. Removable media do not include cloud storage. Requirements for cloud environments can be found in the OPS.2.2 *Cloud Usage* module.

Removable media can be exchanged in person or by conventional post. The secure exchange of digital and analogue storage media to transmit information between different communication partners and IT systems is not considered in this module. The requirements of module CON.9 *Information Exchange* must be met in this regard.

2. Threat Landscape

For module SYS.4.5 *Removable Media*, the following specific threats and vulnerabilities are of particular importance.

2.1. Carelessness in Handling Information

Although organisations often have organisational regulations and technical security procedures for removable media, these are often circumvented by careless handling on the part of employees. Removable media can be left unattended in a meeting room during a break or even in a train compartment, for example.

2.2. Insufficient Knowledge of Rules and Procedures

If employees are not adequately familiar with the rules on the proper handling of removable media, they will not be able to adhere to them. This poses numerous threats to information security—for example, if untested USB pen drives are connected to an organisation's IT systems.

2.3. Theft or Loss of Removable Media

With removable media, the risk of losing data is higher than with stationary systems because such media are more likely to be lost or stolen. The information on a lost storage medium is often irretrievably lost. This information can also fall into the hands of third parties.

2.4. Defective Storage Media

Removable media are prone to damage, errors, and failures due to their size and areas of application. Ever-changing operational environments and mechanical impacts are just two of the reasons why.

2.5. Degradation due to Changing Operational Environments

Removable media are used in a very wide range of environments and are therefore subject to many threats. These threats include damaging environmental conditions such as excessively high or low temperatures, as well as dust and moisture. Transport damage is another example. Another important aspect is that storage media are often used in areas with different levels of security.

2.6. Spreading of Malware

Removable media are often used to exchange data between different devices and a workplace. Malware could compromise data on removable media and thereby spread to workplace systems.

3. Requirements

The specific requirements of module SYS.4.5 *Removable Media* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Process Owner, User

3.1. Basic Requirements

For module SYS.4.5 *Removable Media*, the following requirements MUST be implemented as a matter of priority:

SYS.4.5.A1 Raising Staff Awareness of Secure Handling of Removable Media (B)

All employees MUST be made aware of how to handle removable media in a secure manner. Employees MUST be specifically advised on how to handle removable media to prevent loss and theft and ensure longevity.

An organisation MUST inform its staff that they are not allowed to connect removable media from unknown sources to their systems.

SYS.4.5.A2 Reporting Losses / Tampering [User] (B)

Users MUST immediately report a removable storage device that has been stolen or become a suspected target of tampering. In such reports, users MUST specify the information stored on device in question. There SHOULD be clear reporting paths and contact persons in every organisation for this purpose.

SYS.4.5.A3 ELIMINATED (B)

This requirement has been eliminated.

SYS.4.5.A10 Encryption of Storage Media (B)

If removable media is used or transported outside a secure area and contains confidential data, it MUST be encrypted using a secure method.

SYS.4.5.A12 Protection Against Malware [User] (B)

Data MUST be checked for malware before being transferred to removable media. Data from removable media MUST also be scanned for malware before being processed.

3.2. Standard Requirements

For module SYS.4.5 *Removable Media*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

SYS.4.5.A4 Drawing Up a Policy for the Secure Handling of Removable Media (S)

A policy on the proper handling of removable media SHOULD be established. The following fundamental aspects SHOULD be taken into account:

- which removable media can be used and by whom
- which data may be stored on removable media
- how data stored on removable media will be protected against unauthorised access, tampering, and loss
- how data on removable media is to be deleted
- whether and how private storage media are allowed to be used
- the external employees or service providers with whom storage media may be exchanged and which security regulations are to be observed
- how storage media are to be sent
- how to prevent the spread of malware via removable media

An organisation SHOULD also specify the conditions in which storage media are to be stored in its security policy. In particular, it SHOULD specify that only authorised users have access to the storage media described. It SHOULD also specify that the respective manufacturers' instructions on handling media should be taken into account.

Regular checks SHOULD be carried out to ensure that the security specifications for handling removable media are still up to date.

SYS.4.5.A5 Rules on the Transport of Removable Media (S)

There SHOULD be clear written rules on whether, how, and on what occasions removable media may be transported. These SHOULD specify which media may be taken off-site, by whom, and what security safeguards are to be observed.

SYS.4.5.A6 Storage Media Management [Process Owner] (S)

Management procedures SHOULD be in place for removable media. Storage media SHOULD be labelled in a uniform manner. The storage media management concept in place SHOULD ensure that removable media are handled and stored appropriately and used and transported properly.

SYS.4.5.A7 Secure Deletion of Storage Media Before and After Use [Process Owner] (S)

Before rewritable media are passed on, reused, or discarded, they SHOULD be erased in an appropriate manner.

SYS.4.5.A8 ELIMINATED (S)

This requirement has been eliminated.

SYS.4.5.A13 Appropriate Labelling of Storage Media for Shipping [User] (S)

Users SHOULD mark storage media to be sent in such a way that the sender and recipient can immediately identify them. The labelling of the media or their packaging SHOULD be unambiguous for the recipient. The labelling of storage media containing sensitive information SHOULD ensure that third parties cannot draw any conclusions regarding the type or contents of the information.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.4.5 *Removable Media* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

SYS.4.5.A9 ELIMINATED (H)

This requirement has been eliminated.

SYS.4.5.A11 Protecting Integrity Using Checksums or Digital Signatures (H)

A procedure SHOULD be in place to protect against accidental or intentional alterations and thereby ensure the integrity of confidential information. Procedures designed to prevent such changes SHOULD conform to the current state of the art.

SYS.4.5.A14 Secure Shipping and Packaging (H)

Organisations SHOULD review how confidential information can be adequately protected during shipping. Users SHOULD use secure shipping packaging for data media where tampering is immediately detectable. The sender SHOULD inform all the employees involved of the types of shipping and packaging that are required.

SYS.4.5.A15 Certified Products (H)

Organisations SHOULD only use removable media that are certified. This certification SHOULD take particular account of a given medium's ability to preserve the integrity of data and any encryption that may be in place.

SYS.4.5.A16 Use of Dedicated Systems for Data Scanning (H)

Organisations SHOULD use dedicated systems such as data locks in which data is transferred from one removable storage device to another and scanned for malware.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization describes how removable media can be used securely in standard ISO/IEC 27001:2013, section A.8.3.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module SYS.4.5 *Removable Media*.

G 0.2 Unfavourable Climatic Conditions

G 0.4 Pollution, Dust, Corrosion

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.29 Violation of Laws or Regulations

G 0.39 Malware

G 0.46 Loss of Integrity of Sensitive Information

Federal Office
for Information Security

IND.1 Process Control and Automation Technology

1. Description

1.1. Introduction

Process control and automation technology (also known as operational technology, OT) is hardware and software that monitors and controls the physical devices, processes, and events at a given organisation.

In terms of industry—which also includes critical infrastructures—this particularly refers to industrial control systems (ICS) and automation solutions that handle control and feedback control functions of all kinds. Other examples include laboratory equipment such as automated microscopes or analysis tools, logistics systems like barcode scanners with microcomputers, or building management systems.

While the physical separation of OT from other IT systems and data networks in office applications was common in the past, this can only be applied in exceptional cases involving elevated protection needs today. Multi-stage production steps and the overarching control thereof are making open OT increasingly necessary, including across organisational boundaries. This development is being accelerated by the trend towards the optimisation of production processes, especially in the context of Industry 4.0.

Since OT is increasingly employing components of office IT, this area is now facing similar risks. At the same time, OT differs from conventional IT in fundamental ways, which makes it more difficult to apply established security procedures. Due to manufacturer specifications or legal requirements, there may be restrictions that prevent or impede changes to components, such as the installation of security updates or subsequent hardening measures. OT also usually has much longer lifecycles that can even extend beyond the respective manufacturer's support, which can mean that security updates are not always available.

Another key difference in OT is that it is often subject to high availability and integrity requirements. In comparison, confidentiality tends to be of secondary importance for office

IT. Malfunctions of OT systems can result in hazards to life, limb, and the environment, and they cannot be remedied by a restart in most cases.

1.2. Objective

The objective of this module is to present appropriate requirements for OT information security. It contains cross-component, design-related, and architectural security requirements.

1.3. Scoping and Modelling

Module IND.1 *Process Control and Automation Technology* must be applied at least once to all process control and automation technology in the entire information domain under consideration.

The module must be implemented comprehensively. If there are different security requirements for information security in individual areas where process control and automation technology is used, the module should be applied separately to each IT system.

Even in comparable use cases, the design of OT can vary greatly depending on the purpose, industry, IT systems, and technology at hand, as well as due to the long period of use of such technology. If security safeguards are selected on the basis of the requirements from this module, these special features must be taken into account. They can significantly influence the design of the security concept at hand. For this reason, risk analysis can also be very important early on in the process of drawing up a security concept for normal protection needs.

Operating personnel should be trained and made aware of the relevant threats. To that end, module ORP.3 *Awareness and Training in Information Security* should be implemented.

In addition to this module, the infrastructure surrounding OT (e.g. sites, systems, buildings, and rooms) must be modelled by modules that are as specific as possible in order to enhance the protective effect of the present module.

Module OPS.1.1.5 *Logging* should be implemented to ensure appropriate logging with regard to process control and control technology.

ICS systems should also be considered as a matter of principle if module ORP.4 *Identity and Access Management* is implemented.

2. Threat Landscape

For module IND.1 *Process Control and Automation Technology*, the following specific threats and vulnerabilities are of particular importance:

2.1. Impairment Due to Harmful Environmental Influences

ICS components are often exposed to special conditions in industrial environments that can impair secure operations. These can include extreme heat, cold, humidity, dust, vibration, and environments with corrosive or caustic effects. In many cases, several of these factors are

present simultaneously. ICS components may wear more quickly and fail earlier due to such harmful influences.

2.2. Inappropriate Integration of OT into the Security Organisation

Due to different framework conditions, knowledge, and approaches in the areas of office IT and OT, problems can arise in the implementation of overarching security requirements. On the one hand, security specifications from the area of office IT may not be implemented due to technical or procedural particularities of ICS systems. On the other, the information security officer responsible for office IT may not be familiar with ICS-specific information security and safety aspects (that is, aspects of functional security). This can lead to friction in communication and implementation. It can also result in risks not being recognised or inadequately addressed.

2.3. Inappropriate Integration of OT into Operating Procedures

Despite the increasing convergence of OT and IT, particularities remain that make it difficult to transfer established operational processes between the two areas. In the context of change and incident management activities that are designed to support secure configuration, troubleshooting, or the installation of security updates, for example, operational interventions can entail another official approval or the loss of manufacturer support. Unauthorised changes can influence how a given component works and thus potentially impact its safety functions, as well.

OT is used to monitor, control, and automate technical processes. Malfunctions of these systems can lead to production downtime or damage to technical equipment, personnel, or the environment. These potential impacts must be considered in connection with operational interventions.

2.4. Insufficient Access Protection

Industrial control systems that are operated without any connection to the outside world are becoming increasingly rare. Modern manufacturing and production processes need to exchange information with upstream and downstream production steps and are often connected to central production planning and control systems in an organisation. To exchange information electronically, the production facilities must also be connected to third-party networks, such as the organisation's office IT or the networks of partners and service providers. Interactive access from office or mobile workstations and the operational electronic exchange of data (e.g. for the provision of software and updates) entail further networking with the outside world. Setting up remote accounts for on-call employees or service providers can also make external access possible.

If the required communication channels are too broad or insufficiently secured, attackers can exploit and compromise them. Industrial control systems can be affected by targeted malware attacks. They can also be compromised by malware actually seeks to manipulate office IT. Malware can reach the systems due to a lack of segmentation or control of data traffic.

That said, the use of anti-virus software can also pose a risk to OT if there is no manufacturer approval for the environment in question or if error detections and active system

interventions endanger operations, for example. The operation of network-based intrusion prevention systems (IPS) poses a comparable risk of disruption because such systems can interrupt connections.

2.5. Insecure Process for Project Planning or Application Development

Adjustments and further developments of IT systems, applications, and control programs can represent critical interventions in the corresponding control system. Disruptions can be caused by functional errors in inadequate testing and validation steps, faulty or manipulated project planning data, or weaknesses in software. Important security functions such as input and output or authorisation checks can be insufficiently implemented, for example.

Other threats can result from insecure development environments; unsuitable storage of program code, documentation, or project data; or from data transfer interfaces.

2.6. Insecure Administration Concept and Remote Administration

In some cases, network access is used for the administration of industrial control systems. In this respect, different public and private networks, such as telephone networks, radio networks, mobile networks, and increasingly the Internet are used. If such access is planned inadequately, configured insecurely, or not monitored, attackers might be able to access individual OT components or the corresponding infrastructure in an unauthorised manner under certain circumstances. This could allow them to bypass the security mechanisms at the perimeter.

2.7. Inadequate Monitoring and Detection Procedures

An essential function of industrial control systems is monitoring the operation of automated processes. They issue warnings if a fill level falls below a certain threshold or temperatures or valve positions deviate from their norms, for example. The supporting IT infrastructure, on the other hand, is often not sufficiently monitored.

If unusual or security-relevant events in such operational environments are monitored inadequately (or not at all), attempted attacks, network bottlenecks, or foreseeable failures cannot be detected at an early stage. Moreover, poor evaluation or unclear presentation of the events may also lead to warnings and errors being detected too late.

2.8. Inadequate Test Concept

Industrial control systems are often subject to high availability requirements. Under certain circumstances, malfunctions or technical failures might result in serious damage and high subsequent costs. For this reason, OT systems are often designed to be fail-safe.

If changes to such an environment are not carefully planned, coordinated, and tested in a realistic environment, there is the risk that logical or software-related errors will be overlooked and malfunctions will occur in the system. Even updates released by the manufacturer can cause malfunctions in the system when modifications are made or parameters adjusted.

2.9. Lack of Lifecycle Concepts

In addition to specific ICS components, office IT components and software are increasingly being used in ICS solutions. Due to the very long lifecycles in OT, these components are usually operated much longer than is common for office IT—even beyond the support cycles provided by product suppliers in some cases.

In these instances, updates that address vulnerabilities are no longer provided after the supplier's support has expired. Meanwhile, these vulnerabilities and the tools available to exploit them are often publicly documented. This makes it possible for even inexperienced attackers to successfully compromise the OT systems affected. The same applies if updates are not installed or installed only after a very long delay.

Furthermore, long periods of use can cause problems in procuring spare parts (if they are no longer produced, for example). This may also apply to knowledge regarding the care and maintenance of legacy systems, which new employees will not have.

ICS components also frequently contain detailed information on the processes they control or monitor. This information may be partially reconstructed from other transmitted values such as measurement or control data, as well. The same holds true for control programs or parameters. Attackers can access confidential information in this way.

2.10. Insufficient Security Requirements in Procurement

Information security is often not considered during procurement due to insufficient security requirements or cost considerations. As a result, ICS components can sometimes contain serious vulnerabilities (e.g. in hardware or software) which are very difficult to fix later.

2.11. Use of Insecure Protocols

ICS components communicate with each other using different network protocols and standards. OT-specific protocols are used in addition to protocols and standards from office IT, such as Ethernet, TCP/ IP, WLAN, or GSM. Not all of these elements have been developed from the perspective of information security, and some thus offer limited security mechanisms (or none at all). Information is frequently transmitted as plain text without means of authentication or securing its integrity.

An attacker with access to a given network could read or change the contents of communications and thus influence processes—by faking sensor data or forging control commands, for example. This applies in particular to protocols that are used for communication via freely accessible areas, such as for radio protocols or as part of location networking.

2.12. Insecure Configuration of ICS Components

Security measures are not always activated in the standard configurations of ICS components. This means unauthorised persons may be able to access them with ease. The operation of insecurely configured components can also be a threat to the security of other components in

a given environment, such as when access data for these components can be read or the components are in a trust relationship with other systems.

For example, default passwords could be used, clear text protocols could be implemented for system management, services that are not required could be operated, unsecured interfaces such as USB or FireWire ports could be used, or security functions could be disabled.

2.13. Dependencies between OT and IT Networks

Today, OT is being operated less and less frequently in a completely independent environment. If there are dependencies with other systems, networks, or services, failures or security incidents in the IT network in question might also affect OT.

The availability of the OT and its processes can be severely affected, especially if these systems and networks are not under the direct control of the operator. Furthermore, incidents or errors usually require external support.

Examples of dependencies with other systems and networks include Internet connections, shared infrastructure components, operational management and monitoring by service providers, or the increasing use of cloud services.

3. Requirements

The specific requirements of module IND.1 *Process Control and Automation Technology* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibility	**Role**
Overall responsibility	ICS Information Security Officer
Further responsibilities	Employee, Planner, IT Operation Department, OT Operations

3.1. Basic Requirements

For module IND.1 Process Control and Automation Technology, the following requirements MUST be met as a matter of priority:

IND.1.A1 Integration into the Security Organisation (B)

An information security management system (ISMS) for the operation of OT infrastructure MUST exist either as a stand-alone ISMS or as part of an overall ISMS.

A person MUST be appointed with overall responsibility for OT information security. The details of this appointment MUST be publicised within the organisation in question.

IND.1.A2 ELIMINATED (B)

This requirement has been eliminated.

IND.1.A3 Protection Against Malware (B)

When using anti-virus software on OT components, consideration MUST be given to whether and in which configuration the operation of anti-virus software is supported by its manufacturer. If this is not the case, the need for alternative protection methods MUST be checked.

Virus signatures MUST NOT be obtained by OT systems directly from the Internet.

IND.1.A18 Logging [OT Operations)] (B)

Every change made to ICS components MUST be logged. In addition, all attempts to access to ICS components MUST be logged.

IND.1.A19 Creating Backups [Employee, OT Operations] (B)

Programs and data MUST be backed up regularly. A backup MUST also be made after each system change made to OT components.

3.2. Standard Requirements

For module IND.1 *Process Control and Automation Technology*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

IND.1.A4 Documentation of OT Infrastructure (S)

All the security-relevant parameters of the OT infrastructure at hand SHOULD be documented. All software and system components SHOULD be documented in an inventory list. This list SHOULD state the product and protocol versions used, as well as the respective responsibilities. For the components used, any applicable manufacturer restrictions or regulatory conditions SHOULD be defined. This documentation and a system inventory SHOULD be maintained—for example, in a control system.

In addition to this, an up-to-date network plan SHOULD document zones, zone transitions (conduits), and the communication protocols and methods used, as well as the external interfaces. For the interfaces, active network components and manual data transfer methods (e.g. using removable media) SHOULD be taken into account. Automation solutions SHOULD be structured into cells and communication channels to enable the zones and conduits at hand to protect the OT infrastructure.

IND.1.A5 Development of a Suitable Zone Concept [Planner] (S)

OT infrastructure SHOULD also be segmented horizontally into independent functional areas such as facilities. The individual zones SHOULD be as independent of one another as possible during operations. In particular, the zones where the respective technical process is controlled SHOULD continue to function for a certain period of time if the other zones fail. Decoupling SHOULD also continue to function after an attack. This period SHOULD be suitably defined

and documented. The network SHOULD be designed to be resistant to errors and manipulation.

IND.1.A6 Change Management in OT Operations (S)

A suitable change process SHOULD be defined, documented, and used actively when making changes to OT.

IND.1.A7 Establishing Comprehensive Authorisation Management Across OT and Office IT (S)

An organisation SHOULD establish a process for managing user access and assigned authorisations for OT. A corresponding authorisation management system SHOULD cover this process, along with the implementation and documentation of activities involved in applying for, configuring, and withdrawing authorisations.

The authorisation management system SHOULD ensure that authorisations are granted according to the minimum principle and checked at regular intervals. In the authorisation management system, access to IT systems SHOULD be regulated for employees, administrators, and third parties. Everyone involved SHOULD be made aware of the rules to be followed at regular intervals. Compliance SHOULD be checked. Misconduct SHOULD be sanctioned.

IND.1.A8 Secure Administration [IT Operation Department] (S)

For the initial configuration, administration, and remote maintenance of OT, either secure protocols or separate administration networks with corresponding protection needs SHOULD be used. Access to these interfaces SHOULD be restricted to the persons authorised. The access granted to systems and functions SHOULD be limited to the requirements for the respective administration tasks.

The systems and communication channels used to carry out administration or remote maintenance SHOULD have the same level of protection as the OT components administered.

IND.1.A9 Restrictive Use of Removable Media and Mobile Devices in ICS Environments (S)

Rules for handling removable media and mobile devices SHOULD be established and communicated. The use of removable media and mobile devices in ICS environments SHOULD be restricted. For the media and devices of service providers, an approval process and a requirements list SHOULD be available. Each service provider SHOULD be familiar with the specifications and confirm them in writing.

On OT components, all interfaces that are not required SHOULD be disabled. The usage of active interfaces SHOULD be restricted to certain devices or media.

IND.1.A10 Monitoring, Logging, and Detection [OT Operations] (S)

Operational and security-relevant events SHOULD be identified promptly. For this purpose, a suitable approach to log and event management SHOULD be developed and implemented. Log and event management SHOULD include adequate measures to detect and record security-relevant events. It SHOULD also include a security incident response plan.

The response plan SHOULD define procedures for handling security incidents. This plan SHOULD cover the classification of events, reporting channels and the definition of the organisational units to be involved, response plans to limit damage, the analysis and restoration of systems and services, and the documentation of and follow-up process for incidents.

IND.1.A11 Secure Procurement and System Development (S)

If OT systems are to be procured, planned, or developed, information security regulations SHOULD be established in this regard. The documents SHOULD be part of any related tender.

During procurement, planning, or development, information security SHOULD be taken into consideration through the entire lifecycle. Prerequisites and implementation instructions for the secure operation of ICS components by manufacturers SHOULD be planned and implemented at an early stage. Uniform requirements for information security that correspond to the protection needs at hand SHOULD be defined for ICS components. These SHOULD be taken into consideration when procuring new ICS components. Compliance and implementation SHOULD be documented.

The organisation in question SHOULD document how the system fits into its concepts for zoning, authorisation, and vulnerability management (as well as for virus protection) and adapt them if necessary. A plan for maintaining operations should a given partner stop providing its services SHOULD be formulated.

IND.1.A12 Establishing Vulnerability Management (S)

To ensure the secure operation of its OT environment, an organisation SHOULD establish a vulnerability management approach. Vulnerability management SHOULD identify gaps in software, components, protocols, and external interfaces in the environment under consideration. It SHOULD also make it possible to derive, assess, and implement necessary actions.

This SHOULD be based on reports on vulnerabilities from manufacturers and publicly available CERT messages. In addition, organisational and technical audits SHOULD be performed for vulnerability analysis.

IND.1.A20 System Documentation [Employee, OT Operations] (S)

Advanced system documentation SHOULD be drawn up. It SHOULD record particularities in operations and options for system administration. In addition, any changes made to ICS components SHOULD be documented.

IND.1.A21 Documentation of Communication Relationships [OT Operations (Operational Technology, OT)] (S)

The systems with which an ICS component exchanges data and the data exchanged in this regard SHOULD be documented. Furthermore, the communication links of newly integrated ICS components SHOULD be documented.

IND.1.A22 Central System Logging and System Monitoring [OT Operations] (S)

Log data of ICS components SHOULD be stored centrally. In case of security-critical events, alarms SHOULD be raised automatically.

IND.1.A23 Disposal of ICS Components [OT Operations] (S)

Sensitive data SHOULD be erased prior to the disposal of old or defective ICS components. In particular, it SHOULD be ensured that all access data has been permanently removed.

3.3. Requirements in case of increased protection needs

Generic suggestions for module IND.1 *Process Control and Automation Technology* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

IND.1.A13 Contingency Planning for OT (H)

Business continuity plans SHOULD be defined, documented, tested after each major change, and drilled regularly for each zone to address the possibility of it failing or becoming compromised.

An effective substitute procedure SHOULD also be defined, documented, and tested in case the option of (remote) administration fails.

IND.1.A14 Strong Authentication for OT Components (H)

A central directory service SHOULD be set up for the secure authorisation of privileged users in the control systems at hand (see module ORP.4 *Identity and Access Management*). Authentication SHOULD be secured further using several factors, such as knowledge, ownership, or biometrics.

During planning, it SHOULD be ensured that any resulting dependencies in user authentication are known and taken into consideration when implementing a corresponding solution.

It SHOULD be ensured that operationally required technical accounts can be authorised in emergencies.

IND.1.A15 Monitoring of Wide-Ranging Authorisations (H)

Organisations SHOULD maintain an inventory of all the access rights that have been granted for critical systems. This inventory SHOULD list the rights a particular user effectively has and who has what rights on a particular system.

All critical administrative activities SHOULD be logged. The IT Operation Department SHOULD NOT be able to delete or manipulate the logs.

IND.1.A16 Stronger Compartmentalisation of Zones (H)

Interface systems with security checking functions SHOULD be used as a preventive measure in ICS environments that are highly sensitive or are difficult to secure.

Continuous external connections SHOULD be terminated by implementing one or more connection zones (DMZ) in a P-A-P structure. Required security checks SHOULD be carried out in such a way that the respective ICS system does not have to be adapted.

IND.1.A17 Regular Security Vetting (H)

The security configurations of OT components SHOULD be checked regularly and as needed in the case of sudden threats which were previously unknown. This security vetting SHOULD at least cover exposed systems that involve external interfaces or user interaction. The implemented security concept SHOULD also be checked at regular intervals. Security vetting SHOULD be carried out as a configuration review, or also through automated conformity evaluations.

IND.1.A24 Communication in the Event of Incidents [OT Operations] (S)

Alternative and independent communication options SHOULD be established and operated.

4. Additional Information

4.1. Useful resources

The BSI has published assistance on securing ICS environments in the document "Recommendations for Further Education and Qualification Measures in ICS Environments".

In the "ICS Security Compendium", the Federal Office for Information Security (BSI) provides assistance for manufacturers and integrators of ICS in terms of testing components and IT security safeguards in ICS.

The International Organization for Standardization (ISO) provides specifications on securing energy utilities in the standard ISO/IEC 27019, "Information Technology – Security Techniques – Information Security Controls for the Energy Utility Industry".

The German Association of Energy and Water Industries (BDEW) and Oesterreichs E-Wirtschaft offer assistance on the secure operation of control and telecommunication systems in the white paper "Requirements for Secure Control and Telecommunication Systems".

The international standard IEC 62443-2-1:2010, "Industrial Communication Networks – Network and System Security: Part 2-1: Establishing an Industrial Automation and Control System Security Program, International Electrotechnical Commission (IEC)", specifies what is necessary to establish IT security in networks and systems.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security

objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module IND.1 *Process Control and Automation Technology*.

G 0.5 Natural Disasters

G 0.6 Catastrophes in the Vicinity

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.46 Loss of Integrity of Sensitive Information

IND.2.1 General ICS Components

1. Description

1.1. Introduction

An ICS component is an electronic component that controls or regulates a machine or system. It is thus part of an industrial control system (ICS) or, in more general terms, operational technology (OT). These components may include programmable logic controllers (PLC), sensors, actuators, a machine, or other parts of an ICS.

Due to the typically high availability requirements in OT environments and the often extreme environmental conditions (such as heat, cold, dust, vibration, or corrosion), ICS components have always been designed to be robust devices with high reliability and long service life.

ICS components are normally configured and programmed using special software from the respective manufacturer. This is performed either using programming devices (e.g. as an application under Windows or Linux) or via an engineering station that loads application programs into the programmable logic controllers.

The Information Security Officer role may have different names in the field of industrial automation depending on the type and orientation of the organisation in question. These alternative names include "ICS Information Security Officer (ICS-ISO)" and "Industrial Security Officer".

1.2. Objective

The objective of this module is to secure all kinds of ICS components regardless of their manufacturer, type, purpose, and application site. The module may be used for an individual device or for a modular device consisting of several components.

1.3. Scoping and Modelling

Module IND.2.1 *General ICS Components* must be applied to each ICS component used in the information domain under consideration.

The requirements have been drawn up for a generic ICS component. Additional modules are available for specific ICS components such as sensors and actuators or machines; see, for example, IND.2.3 *Sensors and Actuators* or IND.2.4 *Machine*. These describe requirements that go beyond the general requirements of this module and must be met additionally.

This module does not contain organisational requirements for safeguarding an ICS component. The requirements of module IND.1 *Process Control and Automation Technology* must be implemented for this purpose.

2. Threat Landscape

For module IND.2.1 *General ICS Components*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insecure System Configuration

The default configuration of ICS components is typically designed to ensure that the components work properly and can be put into operation easily. Security mechanisms often play a subordinate role in this regard. All services, protocols, and connections are usually activated and remain active in the default setting even if they are not used. Preset authorisations often remain unchanged, as well.

For attackers, it is easy to take over and manipulate such ICS components. It is also possible for an attacker to exploit an insecure system configuration in order to use the ICS component as a starting point for additional attacks. As a result, critical information may be leaked or the entire operation of the organisation in question may be impaired.

2.2. Insufficient User and Authorisation Management

Some ICS components have their own user and authorisation management system. If this is inadequately designed, employees may share the same user accounts, or the authorisations of employees who have left the company or service providers no longer working for the company may not be deleted. This may ultimately allow unauthorised persons to access ICS components.

2.3. Insufficient Logging

Logging related to ICS components is often limited to process-relevant events. Data relevant to information security is often not recorded. As a consequence, security incidents can only be detected with difficulty and cannot be reconstructed after the fact.

2.4. Manipulation and Sabotage of an ICS Component

The manifold interfaces of ICS components put IT systems, software, and transmitted information at an increased risk of manipulation. Depending on the motivation and knowledge of a potential attacker, this may have effects locally or across multiple locations.

Furthermore, status and alarm messages or other measured values may be suppressed or changed.

Manipulated measurements may cause ICS components or the personnel operating them to make improper decisions. Manipulated systems may be used to attack other systems or locations, or to cover up an ongoing manipulation.

2.5. Use of Insecure Protocols

Some of the protocols used within the framework of industrial control systems only offer limited security mechanisms (or none at all). Technical information such as measured and control values are often transmitted in plain text and without integrity protection or authentication. An attacker with access to the transmission medium may, in this case, read out and modify the communication contents or implement control commands. This could provoke actions or directly influence operations. An attack at the protocol level is possible even if the ICS component is configured securely otherwise and does not have any vulnerabilities.

2.6. Denial-of-Service (DoS) Attacks

An attacker may impair operations of ICS components using DoS attacks. For processes that run under real-time conditions, even a short disruption can lead to a loss of information or control.

2.7. Malware

The threat of malware is also increasingly severe for industrial control systems. Opportunities for infection arise through interfaces to office IT (vertical integration) and to the outside world. Mobile end devices such as service laptops or removable media used for programming and maintaining ICS components also pose a threat. The latter can introduce malware into isolated environments, as well.

2.8. Interception of Information/Espionage

ICS components frequently contain detailed information on the processes they control or monitor. This information may also be partially reconstructed from other transmitted values such as measured or control data. The same holds true for control programs or parameters.

Attackers could obtain trade secrets such as recipes, processes, or other intellectual property in the context of industrial espionage. They may also obtain information on the mode of operation of an ICS component and its security mechanisms and use this for additional attacks.

2.9. Manipulated Firmware

In addition to application programs, the operating system (firmware) of ICS components can be changed. This can enable manipulated software to enter the system. Internal memory could be changed by an attacker by means of a compromised programming device, a local data interface (e.g. USB), or any other existing network connection. A software update might also

have been manipulated along its path from the manufacturer to the operator. Ultimately, the operator might receive an ICS component whose firmware has already been compromised—for example, in the event of a manipulated supply chain or in procuring components from insecure sources. As a consequence, an attacker may modify or falsify processes and procedures.

3. Requirements

The specific requirements of module IND.2.1 *General ICS Components* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibility	**Role**
Overall responsibility	ICS Information Security Officer
Further responsibilities	Employee, Planner, Maintenance Personnel, OT Operations (Operational Technology, OT)

3.1. Basic Requirements

For module IND.2.1 *General ICS Components*, the following requirements MUST be met as a matter of priority:

IND.2.1.A1 Restriction of Access to Configuration and Maintenance Interfaces [OT Operations] (B)

Passwords set by default or by the manufacturer MUST be changed (see ORP.4 *Identity and Access Management)*. These changes MUST be documented. Passwords MUST be stored securely.

It MUST be ensured that only authorised employees are allowed to access the configuration and maintenance interfaces of ICS components. The configuration of an ICS component MUST ONLY be changed after the approval or authentication of the person in charge.

IND.2.1.A2 Using Secure Transmission Protocols for Configuration and Maintenance [Maintenance Personnel, OT Operations] (B)

Secure protocols MUST be implemented for configuring and maintaining ICS components. Information MUST be protected during transmission.

IND.2.1.A3 ELIMINATED (B)

This requirement has been eliminated.

IND.2.1.A4 Disabling or Uninstalling Unused Services, Functions, and Interfaces [Maintenance Personnel, OT Operations] (B)

All services, features, and interfaces of ICS components that are not being used MUST be disabled or uninstalled.

IND.2.1.A5 ELIMINATED (B)

This requirement has been eliminated.

IND.2.1.A6 Network Segmentation [OT Operations, Planner] (B)

ICS components MUST be separated from office IT. If ICS components depend on other components in the network in question, this SHOULD be documented sufficiently. ICS components SHOULD communicate as little as possible with other ICS components.

3.2. Standard Requirements

For module IND.2.1 *General ICS Components*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

IND.2.1.A7 Creating Backups [OT Operations] (S)

Backups MUST be created prior to each system change in an ICS component.

IND.2.1.A8 Protection Against Malware [OT Operations] (S)

ICS components SHOULD be protected against malware by suitable mechanisms (see OPS.1.1.4 *Protection Against Malware*). If an anti-virus protection program is used in this regard, the program and the virus signatures approved by the manufacturer SHOULD always be up to date.

If the resources on the ICS component are not sufficient or real-time requests could be endangered by the use of anti-virus protection programs, alternative safeguards (such as the isolation of the ICS component or the production network) SHOULD be implemented.

IND.2.1.A9 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A10 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A11 Maintenance of ICS Components [Employee, OT Operations, Maintenance Personnel] (S)

The latest approved security updates SHOULD always be installed when maintaining an ICS component. Updates for the respective operating system SHOULD only be installed following approval by the manufacturer of a given ICS component. Alternatively, updates SHOULD be checked in a test environment before they are used in a productive ICS component. Maintenance SHOULD be performed on short notice for critical security updates.

IND.2.1.A12 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A13 Appropriate Commissioning of ICS Components [OT Operations] (S)

Before they are commissioned, ICS components SHOULD correspond to the latest internally approved firmware, software, and patch status.

New ICS components SHOULD be integrated into existing operating, monitoring, and information security management processes.

IND.2.1.A14 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A15 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A16 Protecting External Interfaces [OT Operations] (S)

Externally accessible interfaces SHOULD be protected against misuse.

IND.2.1.A17 Use of Secure Protocols for the Transmission of Measurement and Control Data [OT Operations] (S)

Measurement or control data SHOULD be protected against unauthorised access or changes during transmission. Whether this is necessary or feasible SHOULD be checked in situations involving applications with real-time requirements. If measurement or control data is transmitted using public networks, it SHOULD be protected appropriately.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module IND.2.1 *General ICS Components* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

IND.2.1.A18 Communication in the Event of Incidents [OT Operations, Employee] (S)

There SHOULD be alternative and independent communication options that an organisation can use to maintain its ability to function in the event of malfunctions.

IND.2.1.A19 Security Tests [OT Operations] (H)

Regular security tests SHOULD be carried out to check whether the technical security safeguards in place are still implemented efficiently. The security tests SHOULD NOT be carried out while the system is running. Such tests SHOULD be scheduled for maintenance periods. The results SHOULD be documented. Identified risks SHOULD be evaluated and addressed.

IND.2.1.A20 Trustworthy Code [OT Operations] (H)

Firmware updates or new control programs SHOULD ONLY be installed after their integrity has been checked. They SHOULD only come from trusted sources.

4. Additional Information

4.1. Useful Resources

In the “ICS Security Compendium”, the Federal Office for Information Security (BSI) provides assistance for manufacturers and integrators of ICS in terms of testing components and IT security safeguards in ICS.

The German Association of Energy and Water Industries (BDEW) and Oesterreichs E-Wirtschaft offer assistance on the secure operation of control and telecommunication systems in the white paper “Requirements for Secure Control and Telecommunication Systems”.

NIST Special Publication 800-82, “Guide to Industrial Control Systems (ICS) Security”, describes how IT security can be implemented for industrial control systems.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module IND.2.1 *General ICS Components*.

G 0.2 Unfavourable Climatic Conditions

G 0.4 Pollution, Dust, Corrosion

G 0.8 Failure or Disruption of the Power Supply

G 0.9 Failure or Disruption of Communication Networks

G 0.10 Failure or Disruption of Supply Networks

G 0.12 Electromagnetic Interference

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.40 Denial of Service

G 0.41 Sabotage

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

IND.2.2 Programmable Logic Controller (PLC)

1. Description

1.1. Introduction

A programmable logic controller (PLC) is an ICS component. It performs control tasks in the context of operational technology (OT). The boundaries between different device classes and designs with regard to PLCs are fluid. For example, a remote terminal unit (RTU) may take on the functions of a PLC, or a programmable automation controller (PAC) may try to combine the benefits of a PLC and an industrial PC. However, the PLC is still the classic automation device, which is why the terms "PLC", "RTU", and "PAC" are used synonymously in this module.

A PLC has digital inputs and outputs, a real-time operating system (firmware), and further interfaces for Ethernet or fieldbuses. In connects to sensors and actuators via analogue or digital inputs and outputs, or via a fieldbus. Communication with the process control system typically occurs via the Ethernet interface and IP-based networks.

The possible realisations are manifold: A programmable logic controller can be used as an assembly, a single device, a PC plug-in card (slot PLC), or as software emulation (soft PLC). Modular programmable logic controllers composed of various functional plug-in modules are the most frequent type. Further functions like visualisation, alerting, and logging are also performed increasingly by PLCs.

Due to the typically high availability requirements in OT environments and the often extreme environmental conditions (such as heat, cold, dust, vibration, or corrosion), ICS components have always been designed to be robust devices with high reliability and long service life.

A PLC is normally configured and programmed using special software from the respective manufacturer. This is performed either by programming devices (such as an application under Windows or Linux) or by an engineering station that distributes the data via a network.

1.2. Objective

The aim of this module is to protect all types of programmable logic controllers regardless of their manufacturer, type, purpose, and place of use.

1.3. Scoping and Modelling

Module IND.2.2 *Programmable Logic Controller (PLC)* must be applied once to every PLC component.

This module is to be used to protect all types of programmable logic controllers and devices with similar functions. It supplements module IND.2.1 *General ICS Components*, which must also be taken into account.

This module does not contain organisational requirements for safeguarding an ICS component. The requirements of module IND.1 *Process Control and Automation Technology* must be implemented for this purpose. Functional security is not addressed either; module IND.2.7 *Safety Instrumented Systems* must be applied in this regard.

2. Threat Landscape

For module IND.2.2 *Programmable Logic Controller (PLC)*, the following specific threats and vulnerabilities are of particular importance:

2.1. Incomplete Documentation

Programmable logic controllers are often documented incompletely, which means not all their functions are known. In particular, the information on services, protocols, communication ports, and authorisation management is often incomplete. This complicates the analysis of threats because interfaces, functions, and security-relevant mechanisms can be overlooked. Potential dangers may not be considered as a result. Furthermore, if new vulnerabilities are not documented, an organisation may only be able to respond to them to a limited extent (if at all).

3. Requirements

The specific requirements of module IND.2.2 *Programmable Logic Controller (PLC)* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibility	Role
Overall responsibility	ICS Information Security Officer
Further responsibilities	OT Operations (Operational Technology, OT)

3.1. Basic Requirements

No Basic Requirements are defined for module IND.2.2 *Programmable Logic Controller (PLC)*.

3.2. Standard Requirements

For module IND.2.2 *Programmable Logic Controller (PLC)*, the following requirements correspond to the state-of-the-art technology. They SHOULD be met as a matter of principle.

IND.2.2.A1 Extended System Documentation for Programmable Logic Controllers [OT Operations] (S)

Control programs and configurations SHOULD always be backed up before they are changed. Changes in configurations and the replacement of components SHOULD be fully documented.

IND.2.2.A2 ELIMINATED (S)

This requirement has been eliminated.

IND.2.2.A3 Time Synchronisation [OT Operations] (S)

The system time SHOULD be set automatically through centrally automated time synchronisation.

3.3. Requirements in Case of Increased Protection Needs

No requirements with increased protection needs are defined for module IND.2.2 *Programmable Logic Controller (PLC)*.

4. Additional Information

4.1. Useful Resources

No additional information is available for module IND.2.2 Programmable Logic Controller.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the

requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module IND.2.2 *Programmable Logic Controller (PLC)*.

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.41 Sabotage

IND.2.3 Sensors and Actuators

1. Description

1.1. Introduction

Sensors are electronic components featuring a microprocessor and software that serve as measuring transducers capable of converting a physical magnitude into an electrical output value. This value is provided as a standardised unit signal (often 4 to 20mA, 0 to 10V) to a serial interface, or as digital information transmitted via a fieldbus or Ethernet protocols. Along with measurements, measuring transducers often provide interfaces for performing diagnosis and parametrisation. In addition to producing electronic output values, a sensor may also have further interfaces, such as WLAN, Bluetooth, or wireless HART interfaces for parametrisation and diagnosis.

There are many different sensors available on the market (e.g. for measuring physical values). Depending on the task at hand, the functions and performance of a sensor vary significantly. The range includes sensors that only provide measurements and do not need to be configured. However, some also allow calibration, configuration, or pre-processing of data, or even complete signal processing (smart sensors).

1.2. Objective

The aim of this module is to protect all types of sensors regardless of their manufacturer, type, purpose, and place of use. It can be applied to an individual sensor or a combined sensor assembly.

1.3. Scoping and Modelling

Module IND.2.3 *Sensors and Actuators* must be applied once to sensors and actuators.

It must be used to protect sensors. It supplements the generic module IND.2.1 *General ICS Components*, which is a prerequisite of the present module.

Simple sensors that do not have configuration interfaces or more complex processing logic are not covered by this module. The potential protective measures for such sensors are limited to securing access to them and monitoring whether they are active.

The module also does not address the protection of complex wireless sensor networks. It only describes the protection of individual sensors. It does not describe the security requirements for process control and automation technology. On this subject, module IND.1 *Process Control and Automation Technology* must be implemented.

2. Threat Landscape

For module IND.2.3 *Sensors and Actuators*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Security Requirements in Procurement

Sensors for ICS components in industrial environments are frequently subject to particular conditions that affect their secure operation. Examples of this include extreme heat, cold, humidity, dust, vibration, or atmospheres with a corrosive or caustic effect. In many cases, several of these factors are present simultaneously. Such harmful environmental impacts may result in the sensors of ICS components wearing more rapidly, failing earlier, or producing incorrect measurements.

Information security is often not considered during procurement and installation due to a lack of risk awareness or for cost-related reasons. Sensors might thus include serious vulnerabilities that can only be addressed with significant effort later on.

3. Requirements

The specific requirements of module IND.2.3 *Sensors and Actuators* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibility	**Role**
Overall responsibility	ICS Information Security Officer
Further responsibilities	Maintenance Personnel, OT Operations (Operational Technology, OT)

3.1. Basic Requirements

For module IND.2.3 *Sensors and Actuators*, the following requirements MUST be met as a matter of priority:

IND.2.3.A1 Installation of Sensors [OT Operations, Maintenance Personnel] (B)

Sensors MUST be appropriately installed and be sufficiently robust. They MUST be able to provide reliable measurements despite extreme environmental conditions related to heat, cold, dust, vibration, or corrosion.

3.2. Standard Requirements

For module IND.2.3 *Sensors and Actuators*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

IND.2.3.A2 Calibration of Sensors [Maintenance Personnel] (S)

If necessary, sensors SHOULD be calibrated regularly. Calibrations SHOULD be documented appropriately. Access to a sensor's calibration functions MUST be protected.

3.3. Requirements in case of increased protection needs

Generic suggestions for module IND.2.3 *Sensors and Actuators* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

IND.2.3.A3 Wireless Communication (H)

Wireless management interfaces such as Bluetooth, WLAN, or NFC SHOULD NOT be used. Any unused communication interfaces SHOULD be disabled.

4. Additional Information

4.1. Useful Resources

No additional information is available for module IND.2.3 *Sensors and Actuators*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module IND.2.3 *Sensors and Actuators*.

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.21 Manipulation of Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

IND.2.4 Machine

1. Description

1.1. Introduction

A machine is a technical device that performs automated tasks. A machine tool processes workpieces in a pre-defined manner, for example. It is controlled by an IT system that provides the corresponding work instructions and steps. Such machines are also referred to as automatons.

In most cases, machines are designed by mechanical engineers and provided with pre-defined functions. However, the operator of a machine can also define the parameters it follows when working. Shapes to be milled or calibrations for certain materials can thus be set. Some machines have various interfaces (e.g. for removable media, specialised programming devices, or network access) that enable the operator to change their parameters.

In many cases, mechanical engineers also offer remote maintenance services to detect wear early on or respond quickly in case of problems.

1.2. Objective

This module describes how electronically controlled, semi- or fully automatic machines (e.g. CNC machines) can be protected regardless of their manufacturer, type, specific purpose, and place of use.

1.3. Scoping and Modelling

Module IND.2.4 *Machine* must be applied once to each machine in use.

This module supplements the generic module IND.2.1 *General ICS Components* and requires its prior implementation. Furthermore, it only defines requirements for machines whose internal structures cannot be accessed by an organisation.

Security requirements for process control and automation technology are also not described. Module IND.1 *Process Control and Automation Technology* must be implemented in this

regard. The area of functional safety is also not addressed. More details on this are published in IND.2.7 *Safety Instrumented Systems*.

2. Threat Landscape

For module IND.2.4 *Machine*, the following specific threats and vulnerabilities are of particular importance:

2.1. Failure or Disruption due to Insufficient Maintenance

If machines are not maintained regularly, they may stop functioning correctly at an early stage or fail altogether. Malfunctions may endanger employees, for example, or significantly impair production.

2.2. Targeted manipulations

If the interfaces of a machine are protected insufficiently, attackers may manipulate the machine (e.g. via local programming devices or network services). This may damage workpieces or result in entire product series that are defective. However, the attackers may also damage the machine itself, resulting in an economic loss, as well.

3. Requirements

The specific requirements of module IND.2.4 *Machine* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibility	**Role**
Overall responsibility	ICS Information Security Officer
Further responsibilities	OT Operations (Operational Technology, OT)

3.1. Basic Requirements

For module IND.2.4 *Machine*, the following requirements MUST be met as a matter of priority:

IND.2.4.A1 Remote Maintenance by Mechanical and System Engineers [OT Operations] (B)

There MUST be a central policy for remote maintenance of a machine. This MUST regulate how the respective remote maintenance solutions should be used. The policy MUST also

specify how communication links should be protected. It MUST describe the activities to be monitored during remote maintenance, as well.

Moreover, it SHOULD NOT be possible to access other IT systems or machines of the organisation in question via remote maintenance of a machine.

If a service provider is to be used in this regard, the manner in which the information stored in the machine is to be processed MUST be agreed.

IND.2.4.A2 Operation After End of Warranty [OT Operations] (B)

A process designed to ensure that a given machine can be securely operated beyond its warranty period MUST be established. To this end, further support services MUST be contractually agreed with the supplier.

3.2. Standard Requirements

No standard requirements are defined for module IND.2.4 *Machine*.

3.3. Requirements in Case of Increased Protection Needs

No requirements with increased protection needs are defined for module IND.2.4 *Machine*.

4. Additional Information

4.1. Useful Resources

No additional information is available for module IND.2.4 *Machine*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module IND.2.4 *Machine*.

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.39 Malware

IND.2.7 Safety Instrumented Systems

1. Description

1.1. Introduction

Safety instrumented systems (SIS) are a subgroup of industrial control systems (ICS). SIS are used to avert threats to technical installations, the environment, and people. There is very little difference between the basic structure of an SIS and a conventional automation system. The main difference relates to the increased reliability requirements that apply to how the security functions (SIF) to be executed by an SIS are performed. The degree of reliability is expressed by the safety integrity level (SIL), the four different levels of which are defined in IEC 61508. SIL1 is the lowest reliability requirement, and SIL4 is the highest. Depending on the SIL level, different requirements apply to the permissible failure rate of components, the hardware fault tolerance of the architecture, the independence of auditors, and other security-relevant aspects. In organisational terms, the entire lifecycle of an SIS is embedded in a functional safety management (FSM) system.

This module must be implemented regardless of the SIL level of a given SIS. Information security must be taken into account in every lifecycle phase, from the development of components to their application, operation, and decommissioning. Ensuring the integrity of the SIS in question has the highest priority in this regard.

Another essential feature of an SIS is its independence and separation from surrounding IT systems and operational technology (OT). This means that the availability and integrity of the SIS must not be influenced by such systems and technology.

1.2. Objective

The objective of this module is to formulate appropriate SIS requirements that are to be met when establishing an information security management system (ISMS).

For the purposes of this module, the term “SIS” includes sensors, actuators, safety-related programmable logic controllers (PLC, also known as the logic system), application programs,

and, in particular, the associated programming devices (such as engineering stations or hand-held devices for sensor-actuator configuration) and visualisation devices.

1.3. Scoping and Modelling

Module IND.2.7 *Safety Instrumented Systems* must be applied once to every SIS component in use.

This module supplements the generic modules IND.1 *Process Control and Automation Technology* and IND.2.1 *General ICS Components* and requires their prior implementation.

2. Threat Landscape

For module IND.2.7 *Safety Instrumented Systems*, the following specific threats and vulnerabilities are of particular importance:

2.1. Manipulation of the Logic System

The manipulation of the application program on the logic system, which can violate the integrity of an SIS, represents the greatest risk. Unlike with "simple" OT components, this can potentially have the most severe consequences for the security of people, the environment, and technical installations. On worksheet NA 163 from the international User Association of Automation Technology in Process Industries (NAMUR), the following three categories are defined in this respect:

- Category 1 includes manipulations that trigger a safety function (SIF) without a corresponding need. The consequences are not dangerous in terms of functional security because the SIS will enter its safe mode, but this will lead to an operational interruption. The causes can include malware or human error.
- Category 2 describes cases in which the security function is disabled, which means protection is no longer available. An unacceptable event then only occurs when the need for the security function arises. The consequences are classified as dangerous because the SIS cannot fulfil its primary task. The related attack scenarios are classified as complex because manipulation of the logic system alone is not sufficient to cause damage.
- The third category deals with the gravest scenario, where one or more security functions are disabled and a situation requiring action is caused intentionally. This is another case in which the effects are classified as dangerous and the attack scenarios as very complex. This is because in order to be able to cause a situation in which the security function(s) are needed, the attackers must have sound knowledge of both the physical processes at hand and ways to manipulate the SIS.

In December 2017, the first reports were published on malware that had deliberately manipulated SIS. The perpetrators had gained entry via an engineering station where special software for programming and parameterisation was located. From there, the malware installed searched specifically for connected logic systems from a certain manufacturer and loaded executable code onto them, which manipulated the application program (the logic). The validity check failed due to an error in this code. The security function was then triggered

and the attacked system was put into safe mode. Although the attack was not successful, its impact and complexity could have been classified as Category 2 or 3.

2.2. Inadequate Monitoring and Detection Procedures

An essential function of automation systems involves monitoring the operating states of the process to be automated. This usually takes into account process-related warnings (e.g. exceeded fill levels) and technical parameters (e.g. temperature or valve position). In contrast, the supporting IT infrastructure is often not monitored.

If unusual or security-relevant events are inadequately monitored (or not at all), attempted attacks, network bottlenecks, or foreseeable failures cannot be detected at an early stage.

3. Requirements

The specific requirements of module IND.2.7 *Safety Instrumented Systems* are listed below. As a matter of principle, the Head of OT is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibility	**Role**
Overall responsibility	Head of OT
Further responsibilities	Planner, ICS Information Security Officer, Maintenance Personnel

3.1. Basic Requirements

For module IND.2.7 *Safety Instrumented Systems*, the following requirements MUST be met as a matter of priority:

IND.2.7.A1 Recording and Documentation [Planner, Maintenance Personnel] (B)

All the hardware and software components, relevant information, connections, roles, and responsibilities pertaining to a given SIS MUST be recorded and documented separately.

IND.2.7.A2 Specified Use of Hardware and Software Components [Maintenance Personnel] (B)

The hardware and software components belonging to or used in connection with an SIS MUST NOT be used for any other purpose.

IND.2.7.A3 Changing the Application Program on the Logic System [Maintenance Personnel] (B)

Existing protection mechanisms on the logic system in question MUST be activated. If this is not possible, alternative measures MUST be taken. User programs on logic systems MUST ONLY be changed or released for transmission by authorised persons.

3.2. Standard Requirements

For module IND.2.7 *Safety Instrumented Systems*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

IND.2.7.A4 Making Information Security an Integral Part of Functional Safety Management [ICS Information Security Officer] (S)

All processes and responsibilities pertaining to the information security of SIS SHOULD be clearly defined. These should be described and named in the corresponding functional safety management system.

IND.2.7.A5 SIS Business Continuity Management [ICS Information Security Officer] (S)

The manner in which security incidents are to be handled SHOULD be defined in an incident response plan. This plan SHOULD define the roles and responsibilities and include the measures to be taken.

IND.2.7.A6 Secure Planning and Specification of SIS [Planner, Maintenance Personnel, ICS Information Security Officer] (S)

Accidental or unauthorised changes to specifications, implementations, and engineering data SHOULD be prevented.

IND.2.7.A7 Separation and Independence of the SIS from the Environment [Planner, Maintenance Personnel] (S)

The SIS in question SHOULD operate within its environment without adverse effects in order to guarantee its security functions. Processes that could impact the SIS SHOULD be subject to the change management process established for functional safety management.

IND.2.7.A8 Secure Transfer of Engineering Data to SIS [Planner, Maintenance Personnel, ICS Information Security Officer] (S)

The integrity of engineering data SHOULD be ensured during its transmission to SIS.

IND.2.7.A9 Protection of Data and Signal Connections [Planner, Maintenance Personnel, ICS Information Security Officer] (S)

If it cannot be proven that data and signal connections are not without adverse effects (unidirectionality), these connections SHOULD be suitably protected.

IND.2.7.A10 Displays and Alerts Pertaining to Simulated or Bridged Variables [Planner] (S)

SIS variables that are occupied (simulated) by substitute values or bridged externally SHOULD be monitored in an appropriate manner. The values SHOULD be displayed continuously to the user. Limit values SHOULD be defined. If these limit values are reached, a suitable alert SHOULD be sent to the persons in charge.

IND.2.7.A11 Dealing with Integrated Systems [Planner, Maintenance Personnel, ICS Information Security Officer] (S)

For integrated systems, a suitable strategy SHOULD be developed that regulates the handling of components that affect functional safety.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module IND.2.7 *Safety Instrumented Systems* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

IND.2.7.A12 Ensuring the Integrity and Authenticity of Application Programs and Configuration Data [Planner] (H)

Care SHOULD be taken to ensure that manufacturers develop and integrate appropriate mechanisms to ensure the integrity and authenticity of configuration data and application programs on logic systems or associated sensors and actuators. Any software that is offered for download SHOULD be protected from manipulation. Integrity violations SHOULD be detected and reported automatically.

4. Additional Information

4.1. Useful Resources

In the “ICS Security Compendium”, the Federal Office for Information Security (BSI) provides assistance for manufacturers and integrators of ICS in terms of testing components and providing IT security safeguards in ICS.

The International Organization for Standardization (ISO) provides specifications for securing energy utilities in the standard ISO/IEC 27019, “Information Technology – Security Techniques – Information Security Controls for the Energy Utility Industry”.

The German Association of Energy and Water Industries (BDEW) and Oesterreichs E-Wirtschaft offer assistance on the secure operation of control and telecommunication systems in the white paper “Requirements for Secure Control and Telecommunication Systems”.

The following international standards provide further tools for setting up IT security in safety instrumented systems:

- IEC 61508-1:2010, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Part 1: General Requirements", International Electrotechnical Commission (IEC)
- IEC 61511-1:2016, “Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements”, International Electrotechnical Commission (IEC)
- IEC 62443-2-1:2010, “Industrial Communication Networks – Network and System Security – Part 2-1: Establishing an Industrial Automation and Control System Security Program”, International Electrotechnical Commission (IEC)
- IEC 62443-2-4:2015, “Security for Industrial Automation and Control Systems – Part 2-4: Security Program Requirements for IACS Service providers”, International Electrotechnical Commission (IEC)
- IEC 62443-4-1:DRAFT: “Security for industrial automation and control systems - Technical security requirements for IACS components: Part 4-1: Secure product development life-cycle requirements”, International Electrotechnical Commission (IEC)
- IEC 62443-4-2, “Security for Industrial Automation and Control Systems – Part 4-2: Technical Security Requirements for IACS Components”, International Electrotechnical Commission (IEC)

The international User Association of Automation Technology in Process Industries (NAMUR) has published the worksheet "Security Risk Assessment of SIS”.

The NIST Special Publication 800-81, "Guide to Industrial Control Systems (ICS) Security", describes how IT security can be achieved in ICS environments.

The VDI/VDE 2180 standard covers the safeguarding of industrial process plants using process control technology (PCT).

The VDI/VDE 2182 standard provides a general model and examples for information security in industrial control systems in the following sections:

- Part 2.3, “IT Security for Industrial Automation – Example of Use of the General Model for Plant Managers in Factory Automation – Stamping Plant”
- Part 3.3, "IT Security for Industrial Automation – Example of Use of the General Model for Operators of Process Automation Systems – LDPE Machine”

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security

objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module IND.2.7 *Safety Instrumented Systems*.

G 0.5 Natural Disasters

G 0.6 Catastrophes in the Vicinity

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.46 Loss of Integrity of Sensitive Information

Federal Office
for Information Security

IND.3.2 Remote Maintenance in Industry

1. Description

1.1. Introduction

The operational technology (OT) of an organisation often has a decentralised infrastructure. Different areas of the OT can be far apart in spatial terms. In addition, industrial control systems (ICS) usually consist of a variety of products from different manufacturers (i.e. different ICS components and IT systems for OT applications). Therefore, the operational technology of an organisation usually requires numerous remote maintenance access points.

These remote maintenance access points are often customised solutions in the form of individually assembled hardware and software components. As a result, a variety of different techniques are used for OT remote maintenance. The lifecycles of OT remote maintenance solutions usually correspond to those of the products they access; in other words, such solutions may be used much longer than in IT. A wide variety of access points, services, and interfaces are available in parallel, and the interfaces communicate using very different protocols.

Some system parts in OT are also realised as closed units (known as package units) by the manufacturer. These system parts often contain several decentralised, ready-to-operate access points for remote maintenance, which the manufacturer integrates for their own access from the outset.

In addition to internal staff, external personnel from manufacturers, integrators, and service providers access OT components via remote maintenance to configure, maintain, repair, or check them. Remote maintenance access in industry is used by OT administrators and maintenance staff. OT staff only use OT remote maintenance access in exceptional cases, such as in the event of malfunctions.

In principle, remote maintenance access takes place in the security segment of an OT network in which the remote maintenance service is provided. The remote maintenance service then

communicates from this segment with the target system to be maintained (e.g. with an ICS component).

1.2. Objective

The objective of this module is to ensure information security for remote maintenance in industry.

1.3. Scoping and Modelling

IND.3.2 *Remote Maintenance in Industry* must be applied once for the entire OT of an organisation as soon as the option of remote maintenance is available. Whether further requirements must be defined for remote maintenance in industry depends on the respective area of application of the ICS in question; these requirements cannot be listed in a generally applicable way in this module. Depending on the area of application, the measures that should be implemented to meet the requirements at hand may also differ.

In order to create an IT-Grundschutz model for a specific information domain, all the modules must be considered in their entirety. As a rule, several modules must be applied to the topic or target object.

This module deals with:

- The specific aspects of OT remote maintenance that go beyond the general administration of network components and IT systems via remote maintenance
- The specific aspects of OT remote maintenance that differ from the general administration of network components and IT systems via remote maintenance

The following topics are also significant, but dealt with elsewhere:

- The general management of network components and IT systems via remote maintenance by an administrator in office and building IT (the requirements in this regard must also be fulfilled in principle in OT; see OPS.1.2.5 *Remote Maintenance*)
- The general aspects of network architecture and design, as well as segmentation (see NET.1.1 *Network Architecture and Design*)
- The individual aspects of the hardware and software components that make up the remote maintenance solution in question, such as network components, server and client systems, and OT applications (the respective modules should be modelled here)
- The general aspects of logging (see OPS.1.1.5 *Logging*)
- The general aspects of outsourcing (see OPS.2.1 *Outsourcing for Customers*)
- The general aspects of cloud-based remote maintenance solutions (see OPS.2.2 *Cloud Usage*)
- The general aspects of web-based remote maintenance solutions (see APP.3.1 *Web Applications and Web Services*)
- The general aspects of securing ICS at the operator level (see IND.1 *Process Control and Automation Technology*)

This module does **not** deal with:

- The observation and operation of ICS at the process level
- Controlling access to ICS via remote maintenance (e.g. starting or stopping systems) In principle, access like this can cause personal injury and damage to property on site.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module IND.3.2 *Remote Maintenance in Industry*, the following specific threats and vulnerabilities are of particular importance.

2.1. Incomplete Documentation of Remote Maintenance Access in OT

The remote maintenance access points in the OT of an organisation are usually numerous and diverse. In addition, a large number of internal and external persons access them. The maintenance of remote maintenance access in industry is therefore fundamentally complex and error-prone. Compared to office and building IT, there is a greater risk that the various access points will be insufficiently recorded and documented (i.e. cannot be verified).

If unknown, open access points for OT remote maintenance are not documented, the corresponding operator cannot prevent access. As a result, unauthorised users can directly influence the physical processes of an ICS, which can lead, for example, to individual components malfunctioning, an entire production plant coming to a standstill, and even to dangers to the life and limb of employees on site. If, for example, systems including decentralised components for remote maintenance are realised as a complete system (package unit) by the manufacturer, they are initially not subject to sufficient control by the operator. The operator must record each OT remote maintenance component individually and often actively reconfigure it.

If some OT remote maintenance access points are only recorded and documented in a decentralised manner, for instance, there is also a risk that necessary changes to individual access points will not made or that any changes will not be traceable.

2.2. Insufficient Availability Due to Dependencies on Office and Building IT

In contrast to office and building IT, industrial control systems are partially dependent on a completely uninterrupted flow of information. This applies in particular to all real-time data streams. Even very short interruptions in the availability of data (which can be tolerated in office and building IT) can be critical in an ICS. In addition, dependencies of networks, services, or IT systems can create vulnerabilities. This is often overlooked in planning when an organisation's OT and office and building IT communicate with each other.

If dependencies between OT and office and building IT are not taken into account and resulting vulnerabilities are not closed, security incidents can quickly spread to all the OT in place.

If central components and services of office and building IT are used for remote maintenance of OT (administration across multiple areas), there may also be coordination errors between the office and building IT and the OT. As a result, the correction of critical errors in the ICS of the OT can be delayed. One example would involve a central VPN gateway for remote access that is provided by an organisational unit outside the OT and not operated in an appropriately coordinated manner, which results in it not available quickly enough when needed. This can prolong plant downtime considerably.

2.3. Inadequate Regulations for the Use of OT Remote Maintenance Access

Unlike office and building IT, OT remote maintenance access has a very large potential user base outside the organisation operating the OT. At the same time, the uninterrupted availability of real-time data in an ICS is essential, while the availability of office and building IT data is usually somewhat less time-critical. General rules on how remote access is used for office and building IT are often inappropriate for OT or allow for too much ambiguity.

If the use of OT remote maintenance access is not adequately regulated in a contract, it can lead to a lack of clear specifications on how the users of each individual access point are to be restricted. The operator then cannot control who uses its OT remote maintenance access points. For example, access data used by integrators, manufacturers, and maintenance service providers can be passed on to users who are unknown to the operator. An ICS cannot tolerate such a risk.

If restrictive usage regulations specific to OT are insufficient, the operator cannot adequately control how remote maintenance access to the OT is used. In the event of a security incident, for example, forensic analysis is then made more difficult because causes cannot be identified quickly enough. This can prolong costly production downtime.

If OT remote maintenance access is provided and operated jointly with or by office and building IT and this joint use of the access hardware or software is not clearly regulated, it can lead to inconsistent configurations. This can result in configurations that meet the security requirements of office and building IT, but not the divergent or additional security requirements of OT.

2.4. Insufficient Human Control of OT Remote Maintenance Sessions

Data and configuration settings within an ICS may be compromised by all human access from other zones that is not controlled (or are inadequately controlled) by internal on-site personnel. In particular, personnel from external maintenance providers, integrators, and manufacturers may have the necessary specialised knowledge of the equipment being maintained, but insufficient knowledge of secure remote OT maintenance.

If the processes and contents of OT remote maintenance sessions cannot be adequately controlled by the operator, it may not be possible to detect and trace potentially high-risk configuration errors and unintentional or intentional misconduct by maintenance personnel quickly enough. This can lead to failures or manipulations of real-time data streams or the unnoticed spread of malware throughout the OT at hand. Ultimately, this can result in damage to life and limb of the operating personnel on site, high financial losses due to production

downtime, and even the destruction of entire plants. The disclosure of trade secrets is also possible. In addition, the integrity of manufactured products can be compromised (e.g. by manipulating formulas to produce defective goods that may be difficult to detect). A failure to detect defective products can damage an organisation's reputation.

One example could involve decentralised OT remote maintenance components within facilities that are implemented as a complete system by the manufacturer (package units). These remote maintenance access points are often designed to allow the manufacturer to access the system at any time. If this happens without coordination with the operator's personnel, it can lead to hazardous situations in the current production process, for example.

2.5. Direct Technical Access to ICS from Insecure Zones

Direct IP-based access from other zones and networks presents an inherent risk to the data within an ICS. This is due in part to the special patch cycles in OT, which can be much longer than in office IT, for example. At the same time, remote maintenance access to an ICS usually takes place from networks that can only be trusted to a limited extent. Such networks include private networks of third-party organisations and other zones of an organisation's own network. Zones in an organisation's own network that can only be trusted to a limited extent include those of the internal office and building IT or other zones of the OT network (such as for operations and production management with MES, ERP).

Direct access to an ICS from other zones and networks (e.g. via a local connection or VPN) can introduce malware and open the door to targeted attacks. This can lead to risks to life and limb in the OT zones to be protected, high financial losses due to downtime, or confidential information (such as company secrets) falling into the wrong hands.

2.6. Insecure Alternative OT Remote Maintenance Access in Case of Disruptions

Particularly in the event of disruptions, remote maintenance access for OT must offer greater reliability and performance than for office and building IT. In industrial settings, alternative remote maintenance access points are therefore set up specifically for fast access. These ensure the operational capability of the corresponding ICS even if the respective primary access has failed or cannot provide sufficient performance (e.g. to rectify critical error states on remote systems quickly enough). However, alternative remote maintenance access points like these can be particularly vulnerable to attackers.

If fast alternative remote maintenance access is created (e.g. via mobile communications) but does not fully meet the respective organisation's security requirements, attackers can penetrate the OT network more easily.

2.7. Insecure Technical Design of OT Remote Maintenance Access

An ICS often has a decentralised infrastructure with numerous remote OT access points from different vendors. Both the complex wide-area distribution of access and the diverse range of proprietary remote maintenance solutions make it difficult for an operator to adequately secure all points of OT remote maintenance access in a centralised way.

If OT remote maintenance access points are located in openly accessible areas, attackers can easily penetrate OT networks via these access points and carry out manipulations.

If OT remote maintenance access points are only protected by security components provided by the manufacturer and these do not meet an organisation's security requirements, attackers can also easily penetrate OT networks via these access points and carry out manipulations.

2.8. Outdated Technical Design of OT Remote Maintenance Access

The long lifecycles in industrial environments mean it is not uncommon to find OT remote maintenance solutions that have been in use for 10 years or more and no longer receive updates due to their age. In addition, special environmental conditions can develop over time due to things like the installation of remote maintenance access points in openly accessible areas.

If OT remote maintenance access points are not suitably secured due to long lifecycles, this facilitates unauthorised access to an ICS, and also to other networks and systems within and outside the corresponding OT. This can even make manipulations possible that could endanger life and limb.

In addition, integrated remote maintenance access points may have gone unnoticed in plants for many years. As a result of increasing dependencies on other networks and systems due to more recent technical changes, unauthorised access with critical consequences can then become increasingly likely.

3. Requirements

The specific requirements of module IND.3.2 *Remote Maintenance in Industry* are listed below. The Information Security Officer for the relevant division is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The Information Security Officer for the division must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	OT Operation Department
Further responsibilities	IT Operation Department, Planner, Maintenance Personnel, Data Protection Officer, Employee

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

IND.3.2.A1 Planning the Use of Remote Maintenance in OT (B) [Planner]

In industry, a uniform, central remote maintenance concept MUST be established for all remote maintenance systems for all of an organisation's OT. The following aspects MUST be considered in the OT remote maintenance concept:

- Specific requirements from system manufacturers
- Specific requirements of decentralised infrastructures
- Specific requirements for remote maintenance connections
- Specific requirements for the availability of remote maintenance
- Specific requirements due to environmental conditions
- Specific requirements due to existing plants

All these aspects MUST be coordinated with all the internal and external entities involved.

All remote maintenance access points that provide possible access to an organisation's ICS MUST be recorded in central documentation.

When purchasing new machines with remote maintenance functions, the corresponding information security requirements MUST be coordinated with the supplier.

An organisation SHOULD seek to standardise the remote maintenance solutions it uses. As soon as standardised solutions for remote maintenance are planned, the OT and the office and building IT at hand MUST be jointly coordinated.

IND.3.2.A2 Consistent Documentation of Remote Maintenance by OT and Office and Building IT (B) [IT Operation Department, Maintenance Personnel]

In industry, OT and office and building IT MUST jointly record and document all the OT remote maintenance access points in place.

Particularly for remote maintenance components that are integrated into package units, all disabled access points MUST also be documented.

IND.3.2.A3 Regular Checks and Exceptions for Existing OT Remote Maintenance Access (B) [IT Operation Department]

All facilities MUST be audited regularly to ensure that all their remote maintenance access points comply with the target status (i.e. the current remote maintenance concept for the OT).

An approval process SHOULD be established within the OT for necessary deviations from the established concept.

IND.3.2.A4 Binding Regulation of OT Remote Maintenance by Third Parties (B)

Appropriately restrictive regulations for OT remote maintenance must be contractually agreed with all external users (i.e. manufacturers, integrators and maintenance service providers). These contractual arrangements MUST ensure at all times that external users only use OT remote maintenance access in a controlled and coordinated manner.

The activities certain external users are permitted to carry out and the remote maintenance access points they are to use MUST be defined internally. The internal employees who

authorise, observe and, if necessary, support the remote maintenance access and activities of external users MUST also be defined.

Especially for safety machines, the internal OT employee in question MUST have both organisational and technical sovereignty over the times at which remote maintenance is carried out. The possibility of establishing an outward VPN tunnel MUST be forbidden by contract.

IND.3.2.A5 Internal Coordination for OT Remote Maintenance with Office and Building IT (B) [Planner]

OT, office and building IT, and all other organisational units involved MUST establish appropriately restrictive regulations for all components and interfaces that directly or indirectly enable remote OT maintenance at their organisation. These internal regulations MUST ensure controlled and coordinated use of the respective OT remote maintenance access points at all times. The following aspects MUST be regulated:

- Processes
- Responsibilities
- Authorisations

IND.3.2.A6 Securing All Remote Maintenance Access to OT (B) [IT Operation Department]

In industry, OT MUST be able to control any access to an IT system that provides a remote maintenance service to the OT. For this purpose, access MUST be secured by at least one security component under the responsibility of the OT.

All types of remote maintenance access SHOULD be standardised. All access SHOULD be controlled and explicitly allowed using central authentication components.

If OT remote maintenance access points include decentralised infrastructures or components integrated in package units, the access points MUST be secured by an additional security component that is neither integrated nor part of the decentralised infrastructure.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

IND.3.2.A7 Technical Decoupling of Access (S) [Planner]

All remote access to any components in an OT zone SHOULD be decoupled. At each remote access point to OT, an IT system SHOULD be in place that terminates the connection before the transition into the target OT zone and establishes a new, regulated connection to the remote maintenance service with a different protocol.

All tools and programs required for remote maintenance SHOULD support multi-user operation and be installed and able to function on this IT system. The IT system SHOULD be a jump server or an application layer gateway (ALG) positioned in a dedicated security segment, such as a demilitarised zone (DMZ).

The IT system for decoupling access SHOULD be the responsibility of OT (i.e. ideally located in an OT DMZ).

IND.3.2.A8 Explicit Approval of Every OT Remote Maintenance Session (S) [Employee]

Each remote maintenance session SHOULD be pre-approved by an OT employee of the operator organisation responsible for the target system of the session. This responsible OT employee SHOULD only enable the remote maintenance access following this approval. Explicit approval SHOULD be required both for unscheduled cases of need and during coordinated maintenance windows. Approval SHOULD only be valid for a limited period of time so that the responsible OT employee retains sovereignty over the time of remote maintenance (see requirement IND.3.2.A3 *Regular Checks and Exceptions for Existing OT Remote Maintenance Access*).

Furthermore, external remote maintenance access SHOULD be established exclusively from the inside out (i.e. from the OT network). In particular, open ports for remote maintenance MUST NOT be accessible from the outside (i.e. from untrusted networks).

IND.3.2.A9 Secure Exchange of Files Involved in OT Remote Maintenance (S) [Planner, IT Operation Department]

A secure procedure SHOULD be established for exchanging files involved in OT remote maintenance (e.g. configuration files, updates, or manuals). At minimum, this MUST include a check for malware.

Establishing a connection between a data exchange system and file source SHOULD not be automated; it should be initiated and authenticated by an organisation's OT prior to any file exchange. File exchanges SHOULD always be logged.

IND.3.2.A10 Observation and Control of OT Remote Maintenance Sessions (S) [Employee]

In industry, it MUST be ensured that persons working in plants or operating machines cannot be endangered directly or indirectly by active remote maintenance. Furthermore, it MUST be ensured that active remote maintenance does not interfere with the production process.

If personal injury or damage to property is possible, it MUST be ensured that an OT employee can follow the remote maintenance activities on site (dual control principle). The OT employee SHOULD be able to intervene and interrupt a remote maintenance session if necessary.

IND.3.2.A11 Central Management of All User Accounts for OT Remote Maintenance (S) [IT Operation Department]

Only user accounts managed in a central OT or organisational directory service SHOULD be used for OT remote maintenance access.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be

taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

IND.3.2.A12 Dedicated OT Remote Maintenance Solution (H) [Planner]

For remote maintenance in industry, a dedicated OT remote maintenance solution SHOULD be used that is independent from office and building IT. All other functions on the IT systems for OT remote maintenance, particularly functions for the administration of IT systems and networks outside the OT, SHOULD be deactivated or prevented.

To ensure maximum independence, dedicated Internet access SHOULD also be used for OT remote maintenance.

IND.3.2.A13 Logging of Contents of Remote Maintenance Access in OT (H) [Planner, Data Protection Officer]

For remote maintenance of OT applications or systems, logging SHOULD be extended so that all activities can be immediately traced in a seamless manner. For this purpose, in addition to logging events and session data, the subject matter involved in instances of remote maintenance access SHOULD also be logged.

IND.3.2.A14 Technical Control of Remote Maintenance Sessions (H) [Planner, Data Protection Officer]

Supplementary to IND.3.2.A10 *Observation and Control of OT Remote Maintenance Sessions*, OT remote maintenance sessions SHOULD be continuously regulated by a technical solution. In this context, command-level activities (i.e. manual and automated commands) SHOULD be technically monitored and automatically prevented where necessary.

In addition, sessions SHOULD be monitored across components. If technical monitoring is used, an alarm SHOULD be triggered for anomalies in user behaviour and for specific rule violations (e.g. as soon as a sudden increase in communication volume is detected).

4. Additional Information

4.1. Useful Resources

In its publication “Fernwartung im industriellen Umfeld” [Remote Maintenance in Industry], the Federal Office for Information Security provides an overview of how remote maintenance access can be kept secure in an industrial environment.

In its publication “ICS Security Compendium”, the Federal Office for Information Security describes how to secure industrial control systems (ICS).

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module IND.3.2 *Remote Maintenance in Industry*:

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.27 Lack of Resources

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.36 Identity Theft

G 0.39 Malware

G 0.40 Denial of Service

G 0.41 Sabotage

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

G 0.47 Harmful Side Effects of IT-Supported Attacks

NET.1.1 Network Architecture and Design

1. Description

1.1. Introduction

To carry out their business operations and processes, most of today's organisations require data networks that make it possible to exchange information and data, implement shared applications, and engage in various other activities. Along with conventional end devices, these networks are connected to the networks of partner organisations and to the wider Internet. They are also incorporating more and more mobile devices and elements associated with the Internet of Things (IoT). Moreover, cloud services and services for unified communications and collaboration (UCC) are increasingly being used via data networks. The resulting benefits are undisputed. However, all these end devices and services present greater risks, as well. It is therefore important that organisations protect their own networks with secure network architecture. Building a local area network (LAN) or a wide area network (WAN) with a secure architecture requires planning. In addition, external networks that can only be trusted to a limited extent (such as customer networks or the Internet itself) must be suitably integrated.

To ensure a high level of security, additional security-relevant aspects have to be considered. Examples include the secure separation of different clients and device groups at the network level and the control of their communications through a firewall. Another important security element, especially for clients, is network access control.

1.2. Objective

The objective of this module is to establish information security as an integral component of network architecture and design.

1.3. Scoping and Modelling

Module NET.1.1 *Network Architecture and Design* must be applied to the entire network of a given organisation, including all its sub-networks.

The module contains basic specifications which have to be considered and met when planning, designing, and operating new networks. Requirements for the secure operation of the relevant network components, including security components such as firewalls, are not covered in this module. They are addressed in the module group NET.3 *Network Components*.

This module focuses on cable-based networks and data communication. However, general requirements for architecture and design, such as the necessity to physically separate network segments with zones, must be observed and met for all network technologies.

Additional specific requirements for network areas such as wireless LAN (WLAN) or storage area networks (SAN) are addressed in the module layer NET.2 *Radio Networks* and in module SYS.1.8 *Storage Solutions*. The subjects of Voice over IP (VoIP) and the underlying security infrastructure are not discussed in this module; they are addressed in module NET.4.2 *VoIP*.

Specific security requirements for virtual private clouds and hybrid clouds are also not the focus of this module.

Network management is considered within the scope of zoning and segmentation, while all other subjects of network management are addressed in module NET.1.2 *Network Management*.

2. Threat Landscape

For module NET.1.1 *Network Architecture and Design*, the following specific threats and vulnerabilities are of particular importance.

2.1. Failure or Insufficient Performance of Communication Links

If communication links have insufficient capacity or their performance is no longer sufficient as a consequence of technical failures or denial-of-service (DoS) attacks, the communication of clients with servers will be restricted, for example. This will increase the time it takes to access internal and external services. As a result, it may only be possible to use such services to a limited extent (if at all). Business-relevant information may also no longer be available, which can bring essential business processes or entire production processes to a standstill.

2.2. Inadequately Secured Network Access

If an internal network is connected to the Internet and the transition is not sufficiently protected (e.g. due to a lack of or incorrectly configured firewalls), attackers may access sensitive information of the corresponding organisation and copy or manipulate it.

2.3. Inadequate Network Structuring

If a network is improperly structured or expanded, it may lead to insecure network topologies or network configurations. This allows attackers to easily identify vulnerabilities and penetrate the corresponding organisation's internal network, where they can steal information, manipulate data, or disrupt entire production systems. In an incorrectly structured network where monitoring by security systems is limited, attackers can also remain unnoticed for longer periods of time.

3. Requirements

The specific requirements of this module are listed below. As a matter of principle, the Planner is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Planner
Further responsibilities	IT Operation Department

3.1. Basic Requirements

For module NET.1.1 *Network Architecture and Design*, the following requirements MUST be met as a matter of priority:

NET.1.1.A1 Security Policy for the Network [IT Operation Department] (B)

Based on an organisation's general security policy, a specific policy SHOULD be drawn up for its network. It MUST comprehensibly describe requirements and specifications on how to design and construct networks securely. The policy MUST include definitions of the following:

- the cases in which zones have to be segmented and user groups or clients have to be separated logically, or even physically
- which communication relationships and which network and application protocols are permitted in each case
- how the data traffic for administration and monitoring is to be separated in the network
- what type of internal communication (WAN, wireless networks) is allowed across locations and what encryption is required on WAN, LAN, or radio links
- what type of cross-location communication is permitted

All the employees responsible for network design MUST be familiar with the policy. It MUST form the basis of their work. If the policy is changed or there are deviations from the requirements specified, this MUST be documented and agreed with the CISO in charge. The

correct implementation of the policy MUST be regularly reviewed. The results MUST be documented in an appropriate manner.

NET.1.1.A2 Documentation of the Network [IT Operation Department] (B)

Complete documentation of the network MUST be produced. It MUST include a network plan. The documentation MUST be consistently maintained. This documentation MUST contain the initial survey of the actual situation (including network performance) and all changes made to the network. The logical structure of the network MUST also be documented—in particular, the assignment of sub-networks and the zoning and segmentation of the network.

NET.1.1.A3 Specification of Network Requirements (B)

A requirements specification MUST be created based on the security policy for the network in question. The specification MUST be consistently maintained. It MUST be possible to derive all the essential elements of network architecture and design from these requirements.

NET.1.1.A4 Network Separation into Zones (B)

The overall network at hand MUST be physically separated into at least the following three zones: internal network, demilitarised zone (DMZ), and external connections (including to the Internet and other untrusted networks). The transitions between the zones MUST be protected by a firewall. This method of control MUST follow the principle of local communication so that firewalls allow only authorised communications (whitelisting).

Untrusted networks (e.g. the Internet) and trusted networks (e.g. an intranet) MUST be separated by a two-stage firewall structure consisting of stateful packet filters (firewalls). In order to separate the Internet and external DMZ in the network, a stateful packet filter must be implemented at minimum.

In the two-stage firewall architecture, all incoming and outgoing data traffic MUST be controlled and filtered by the external packet filter or the internal packet filter.

A P-A-P structure consisting of a packet filter, an application layer gateway or security proxies, and a packet filter MUST always be implemented when required by the security policy or the requirements specification at hand.

NET.1.1.A5 Client-Server Segmentation (B)

Clients and servers MUST be placed in different network segments. The communication between these network segments MUST be controlled by a stateful packet filter at minimum.

It SHOULD be noted that possible exceptions which make it possible to position clients and servers in a shared network segment are covered in the respective application-specific and system-specific modules.

For guest access and network areas where there is no internal control of end devices, dedicated network segments MUST be established.

NET.1.1.A6 End Device Segmentation in the Internal Network (B)

The end devices positioned in a given network segment MUST correspond to a similar security level.

NET.1.1.A7 Protection of Sensitive Information (B)

Sensitive information MUST be transmitted using protocols that are secure according to the state of the art in information security unless trusted dedicated network segments (e.g. within the management network) are used for communication. If it is not possible to use such protocols, appropriate encryption and authentication techniques according to the state of the art in information security MUST be implemented (see NET.3.3 *VPN*).

NET.1.1.A8 Basic Protection of Internet Access (B)

Internet traffic MUST be routed through a firewall structure (see NET.1.1.A4 *Network Separation into Zones*). Flows of data MUST be restricted to the required protocols and communication relationships by the firewall structure.

NET.1.1.A9 Basic Protection of Communication with Untrusted Networks (B)

Every network's level of trustworthiness MUST be defined. Networks that are not trusted MUST be treated like the Internet and secured accordingly.

NET.1.1.A10 DMZ Segmentation for Access from the Internet (B)

An organisation's firewall structure MUST be complemented by an external DMZ for all services and applications that can be accessed from the Internet. A concept for DMZ segmentation SHOULD be drawn up that implements the corresponding security policy and requirements specification in a transparent manner. Depending on the security level of the IT systems at hand, the DMZ segments MUST be divided further. An external DMZ MUST be connected to the external packet filter.

NET.1.1.A11 Protection of Communications Entering the Internal Network from the Internet (B)

IP-based access to an internal network MUST run through a secure communication channel. Access MUST be restricted to trusted IT systems and users (see NET.3.3 *VPN*). VPN gateways of this kind SHOULD be placed in an external DMZ. It SHOULD be ensured that adequately hardened VPN gateways can be accessed directly from the Internet. Access attempts to an internal network that are authenticated via a VPN gateway MUST at least pass through an internal firewall.

IT systems MUST NOT access an internal network via the Internet or an external DMZ. It SHOULD be ensured that any exceptions to this requirement are covered in the relevant application- and system-specific modules.

NET.1.1.A12 Protection of Outgoing Internal Communication to the Internet (B)

Outgoing communication from an internal network to the Internet MUST be decoupled through a security proxy. This decoupling MUST take place outside of the internal network. If a P-A-P structure is in use, the outgoing communication SHOULD always be decoupled by the security proxies of the P-A-P structure.

NET.1.1.A13 Network Planning (B)

Every network implementation MUST be planned in a suitable, comprehensive, and transparent manner. In this context, the security policy and the requirements specification in question MUST be observed. In addition, the following aspects MUST be considered at minimum in the planning in accordance with the needs at hand:

- the connection to the Internet and, if available, the local network and extranet
- the topology of the overall network and network areas (i.e. zones and network segments)
- the capacity and redundancy of the network and security components, transmission routes, and external connections
- the protocols to be used and their general configuration and addressing (in particular, IPv4/IPv6 sub-networks of terminal device groups)
- administration and monitoring (see NET.1.2 *Network Management*)

Network plans MUST be regularly reviewed.

NET.1.1.A14 Implementation of Network Planning (B)

Planned networks MUST be implemented properly. This MUST be verified during the approval process.

NET.1.1.A15 Regular Gap Analysis (B)

Regular checks MUST be conducted to ensure that a given network corresponds to the target condition. At minimum, the extent to which it complies with the relevant security policy and requirements specification MUST be checked. The extent to which the implemented network structure corresponds to the current network plans MUST also be checked. To this end, responsible persons and test criteria or specifications MUST be defined.

3.2. Standard Requirements

For module NET.1.1 *Network Architecture and Design*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

NET.1.1.A16 Specification of Network Architecture (S)

Based on the security policy and the requirements specification at hand, an architecture for a network's zones (including the internal network, DMZ, and external connections) SHOULD be developed and consistently maintained. In this context, all the relevant architectural elements of the respective organisation SHOULD be taken into account based on its specific situation. The following, however, are necessary at minimum:

- the architecture of the internal network, including specifications on how network virtualisation technologies, layer 2 and layer 3 communication, and redundancy procedures are to be used
- the network architecture for external connections, including firewall architectures, DMZ and extranet design, and specifications for site coupling

- specifications of the network locations where security components such as firewalls or IDS/IPS should be placed and the security functions they should provide
- specifications for the network connections of the different IT systems at hand
- the network architecture in virtualisation hosts, with a particular focus on network virtualisation overlays (NVOs) and the architecture in vertically integrated systems (ViS)
- specification of the basic architecture elements for a private cloud, as well as protection of the connections to virtual private clouds, hybrid clouds, and public clouds
- architecture for secure administration and monitoring of IT infrastructure

NET.1.1.A17 Specification of Network Design (S)

Based on the network architecture in question, the network design for the zones (including the internal network, the DMZ, and external connections) SHOULD be developed and consistently maintained. To this end, the relevant architectural elements SHOULD be considered in detail, including the following points at minimum:

- admissible forms of network components, including virtualised network components
- specifications on how WAN and wireless connections should be protected
- the connection of end devices to switching components, connections between network elements, and the use of communication protocols
- redundancy mechanisms for all network elements
- an address concept for IPv4 and IPv6, as well as associated routing and switching concepts
- virtualised networks in virtualisation hosts, including NVOs
- the structure, connection, and protection of private clouds and the secure connection of virtual private clouds, hybrid clouds, and public clouds
- specifications regarding network design for the secure administration and monitoring of IT infrastructure

NET.1.1.A18 P-A-P Structure for the Internet Connection (S)

An organisation's network SHOULD be connected to the Internet via a firewall with a P-A-P structure (see NET.1.1.A4 *Network Separation into Zones*).

A proxy-based application layer gateway (ALG) MUST be implemented between the two firewall levels. The ALG MUST be connected via its own transfer network (dual-homed) to both the external packet filter and the internal packet filter. The transfer network MUST NOT be occupied with tasks other than those performed for the ALG.

If no ALG is used, appropriate security proxies MUST be implemented. The security proxies MUST be connected via a separate transfer network (dual-homed). The transfer network MUST NOT be occupied with tasks other than those performed for the security proxies. Whether mutual attacks are possible via the security proxies MUST be checked. If this is the case, the transfer network MUST be appropriately segmented.

All data traffic MUST be decoupled via the ALG or the corresponding security proxies. A transport network that connects both firewall stages with each other MUST NOT be

configured. In addition, the internal firewall MUST reduce the exposure of the ALG or the security proxies to internal attackers or IT systems in the internal network.

Authenticated and trusted network access attempts from the VPN gateway to the internal network SHOULD NOT pass through the ALG or the security proxies of the P-A-P structure.

NET.1.1.A19 Separation of Infrastructure Services (S)

Servers providing basic services for IT infrastructure SHOULD be positioned in a dedicated network segment. The communication with these servers SHOULD be controlled by a stateful packet filter (firewall).

NET.1.1.A20 Allocation of Dedicated Sub-Networks for IPv4/IPv6 End Device Groups (S)

Different IPv4/IPv6 end devices SHOULD be allocated to dedicated sub-networks according to the protocol used (IPv4/IPv6 or IPv4/IPv6 DualStack).

NET.1.1.A21 Separation of the Management Area (S)

Out-of-band management SHOULD be used comprehensively to manage infrastructure. In this context, all the end devices required to manage IT infrastructure SHOULD be positioned in dedicated network segments. The communication with these end devices SHOULD be controlled by a stateful packet filter. The communication from and to these management network segments SHOULD be restricted to the necessary management protocols with defined communication end points.

The management area SHOULD include at least the network segments below. Depending on the security policy and the requirements specification at hand, these SHOULD be further subdivided into the following:

- network segment(s) for IT systems that are responsible for the authentication and authorisation of administrative communication
- network segment(s) for the administration of IT systems
- network segment(s) for monitoring
- network segment(s) containing the central logging system, including the syslog server and SIEM server
- network segment(s) for IT systems that are required for basic services of the management area
- network segment(s) for the management interfaces of the IT systems to be administered

The different management interfaces of the IT systems at hand MUST be separated according to their purpose and their network position via a stateful packet filter. In addition, the following IT systems (management interfaces) SHOULD be separated via dedicated firewalls:

- IT systems that can be accessed from the Internet
- IT systems in the internal network
- security components located between the IT systems accessible from the Internet and the internal network

It MUST be ensured that the segmentation cannot be circumvented by management communication. The possibility of bypassing segments MUST be prevented.

NET.1.1.A22 Specification of the Segmentation Concept (S)

Based on the specifications of the network architecture and network design at hand, a comprehensive segmentation concept SHOULD be created for the respective internal network. This segmentation concept SHOULD include any existing virtualised networks in virtualisation hosts. The segmentation concept SHOULD be planned, implemented, followed, and consistently maintained. The concept SHOULD comprise at least the following aspects, assuming they are planned in the target environment:

- network segments to be created initially, as well as specifications on how new network segments are to be created and how end devices should be positioned in the network segments
- specification for the segmentation of development and test systems (staging)
- network access control for network segments with clients
- connection of network areas which are connected to the network segments via wireless technologies or a dedicated line
- connection of the virtualisation hosts and virtual machines on the hosts to the network segments
- data centre automation
- specifications on how end devices that supply several network segments, such as load balancers and storage and backup solutions, are to be incorporated

Depending on the security policy and the requirements specification at hand, a concept SHOULD be developed that describes how each network segment is to be implemented in networking terms. In addition, the security functions that must be provided by the coupling elements between the network segments (e.g. a firewall as a stateful packet filter or IDS/IPS) SHOULD be defined.

NET.1.1.A23 Separation of Network Segments (S)

IT systems with different protection needs SHOULD be placed in different network segments. If this is not possible, IT systems SHOULD be protected according to the highest protection needs present in their network segment. In addition, network segments SHOULD be further divided depending on their size and the requirements of the segmentation concept in question. It MUST be ensured that it is not possible to bypass network segments, much less zones.

If the virtual LANs (VLANs) on a switch belong to different organisations, they SHOULD be physically separated. Alternatively, data SHOULD be encrypted to protect the transmitted information from unauthorised access.

NET.1.1.A24 Secure Logical Separation using VLAN (S)

If VLANs are used, they MUST NOT create a connection between a given internal network and a zone before the ALG or the security proxies.

In general, it MUST be ensured that VLANs cannot be overwhelmed.

NET.1.1.A25 Detailed and Implementation Planning of Network Architecture and Design (S)

Detailed and implementation planning for network architecture and design SHOULD be carried out, documented, reviewed, and consistently maintained.

NET.1.1.A26 Specification of Operating Processes for the Network (S)

Operating processes SHOULD be created, adapted as required, and documented. In particular, the impact of zoning and segmentation concepts on IT operations SHOULD be considered.

NET.1.1.A27 Integration of Network Architecture into Contingency Planning [IT Operation Department] (S)

The impact that network architecture and concepts derived from it have on contingency planning SHOULD be analysed initially and at regular intervals in a transparent way.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.1.1 *Network Architecture and Design* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

NET.1.1.A28 High-Availability Network and Security Components (H)

The central areas of an internal network and the security components in place SHOULD be designed for high availability. To this end, the components SHOULD be designed redundantly and realised with high internal availability.

NET.1.1.A29 Implementing Network Connections for High Availability (H)

The network connections (such as the Internet connection and WAN connections) SHOULD be designed with full redundancy. Depending on the availability requirements at hand, redundant connections to one or more providers SHOULD be implemented with different technology and performance. Redundant routes SHOULD also be implemented as needed both within and outside of an organisation's purview. To this end, possible single points of failure (SPoF) and disruptive environmental conditions SHOULD be considered.

NET.1.1.A30 Protection Against Distributed Denial of Service (H)

In order to fend off DDoS attacks, the available bandwidth SHOULD be purposefully distributed over different communication partners and protocols by means of bandwidth management.

In order to be able to thwart DDoS attacks with very high data rates, mitigation services SHOULD be purchased via larger Internet service providers (ISPs). Their use SHOULD be contractually regulated.

NET.1.1.A31 Physical Separation of Network Segments (H)

Depending on the security policy and requirements specification at hand, network segments SHOULD be physically separated by separate switches.

NET.1.1.A32 Physical Separation of Management Network Segments (H)

Depending on the security policy and requirements specification at hand, the network segments of a management area SHOULD be physically separated from each other.

NET.1.1.A33 Micro-Segmentation of the Network (H)

A network SHOULD be divided into small network segments with very similar requirement profiles and the same protection needs. This SHOULD be considered for DMZ segments in particular.

NET.1.1.A34 Use of Cryptographic Methods at the Network Level (H)

Network segments SHOULD already be realised at the network level in a given internal network, extranet, and DMZ by means of cryptographic techniques. To this end, VPN techniques or IEEE 802.1AE SHOULD be used.

If communication within an internal network or DMZ takes place via transmission routes which are not sufficiently secure for increased protection needs, the communication SHOULD be adequately encrypted at the network level.

NET.1.1.A35 Use of Network-Based DLP (H)

Systems for data loss prevention (DLP) SHOULD be implemented at the network level.

NET.1.1.A36 Separation by Means of VLAN for Very High Protection Requirements (H)

In cases involving very high protection needs, VLANs SHOULD NOT be used.

4. Additional Information

4.1. Useful Resources

The BSI has published the following additional documents associated with networks:

- Secure connection of local networks to the Internet (ISi-LANA)
- “Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf” [Technical Guideline for Internal Telecommunications Systems with Increased Protection Requirements] BSI-TL-02103, version 2.0

The International Organization for Standardization (ISO) provides guidelines for securing networks in the standard ISO/IEC 27033, “Information Technology – Security Techniques – Network Security – Part 1: Overview and Concepts to Part 3: Reference Networking Scenarios – Threats, Design Techniques, and Control Issues”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.1.1 *Network Architecture and Design*.

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.46 Loss of Integrity of Sensitive Information

NET.1.2 Network Management

1. Description

1.1. Introduction

Reliable network management is a basic requirement for operating state-of-the-art networks in a secure and efficient manner. To that end, network management must fully integrate all the network components at hand. Appropriate safeguards must also be implemented to protect network management communication and infrastructure.

Network management includes many important functions, such as network monitoring, component configuration, event handling, and logging. Another important function is reporting, which may be designed as a common platform for network and IT systems. Alternatively, it may be implemented in a dedicated manner as a uniform platform or as part of individual network management components.

Network management infrastructure consists of central management systems (such as an SNMP server), administration devices with software for management access, and decentralised management agents. It also includes dedicated management tools such as probes or specific measurement devices, and management protocols such as SNMP or SSH. Management interfaces such as dedicated Ethernet ports or console ports are also part of a network management infrastructure.

1.2. Objective

The objective of this module is to establish information security as an integral part of network management.

1.3. Scoping and Modelling

Module NET.1.2 *Network Management* must be applied to each network management system (a management system and the IT system to be managed) that is used in the information domain under consideration. The IT systems to be managed are usually individual clients, servers, or active network components (network coupling elements).

This module considers the necessary components and conceptual tasks involved in network management. System management requirements for networked clients and servers are not described here.

This module describes how network management can be structured and secured and how the related communication can be protected. However, details regarding the protection of network components, particularly their management interfaces, are covered by the module groups NET.2 and NET.3.

The logging addressed in this module should be integrated into a comprehensive logging and archiving concept (see OPS.1.1.5 *Logging* and OPS.1.2.2 *Archiving*).

Network management data must be considered in backup concepts. The requirements for this are included in module CON.3 *Backup Concept*.

2. Threat Landscape

For module NET.1.2 *Network Management*, the following specific threats and vulnerabilities are of particular importance.

2.1. Unauthorised Access to Central Network Management Components

If attackers manage to access network management solutions due to unpatched vulnerabilities or insufficient network separation, for example, they can control and reconfigure all the connected network components. They may thus access sensitive information, divert network traffic, or even significantly disrupt the entire network.

2.2. Unauthorised Access to Individual Network Components

If attackers manage to gain access to individual network components, they can control and manipulate the respective components. All data traffic that passes through a compromised network component may thus also be compromised. Furthermore, additional attacks may be prepared in order to penetrate further into the corresponding organisation’s network.

2.3. Unauthorised Interference in Network Management Communication

If network management communication is intercepted and manipulated, this may be used as a means of misconfiguring and controlling active network components. This in turn may violate the network's integrity and limit the availability of network infrastructure. Furthermore, the transmitted data may be intercepted and viewed.

2.4. Insufficient Time Synchronisation of Network Management Components

If the system time of network management components is insufficiently synchronised, the related log data may not be correlated. Attempts to correlate this data could possibly also lead to erroneous conclusions because different time stamps of events do not provide for a common basis. This makes it impossible to respond to events appropriately, and problems cannot be eliminated. Security incidents and data leaks may thus remain undetected.

3. Requirements

The specific requirements of module NET.1.2 *Network Management* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Planner, Supervisor

3.1. Basic Requirements

For module NET.1.2 *Network Management*, the following requirements MUST be met as a matter of priority:

NET.1.2.A1 Network Management Planning (B)

Network management infrastructure MUST be planned appropriately. This SHOULD address all the items listed in the respective security policy and requirements specification for network management. The following aspects MUST be considered at minimum:

- the network management areas to be separated
- possible ways to access the management servers at hand
- communication for management access
- the protocols used (e.g. IPv4 and IPv6)
- requirements that management tools must fulfil
- interfaces for forwarding collected event or alarm messages
- logging (including the required interfaces to a centralised logging solution)
- reporting and interfaces to overarching solutions
- corresponding requirements to be fulfilled by the network components to be integrated

NET.1.2.A2 Specification of Network Management Requirements (B)

Based on NET.1.2.A1 *Network Management Planning*, requirements for the network management infrastructure and processes in question MUST be specified. In so doing, all the essential elements of network management MUST be taken into account. The network management policy at hand SHOULD also be considered.

NET.1.2.A3 ELIMINATED (B)

This requirement has been eliminated.

NET.1.2.A4 ELIMINATED (B)

This requirement has been eliminated.

NET.1.2.A5 ELIMINATED (B)

This requirement has been eliminated.

NET.1.2.A6 Regular Backups (B)

In terms of network management backups, the system data for integrating the components or objects to be managed, event messages, statistical data, and stored data for configuration management MUST be backed up at minimum.

NET.1.2.A7 Basic Logging of Events (B)

The following events MUST be logged at minimum:

- unauthorised access or access attempts
- performance or availability fluctuations of the network in question
- errors in automatic processes (e.g. during configuration distribution)
- restricted accessibility of network components

NET.1.2.A8 Time Synchronisation (B)

All network management components, including the integrated network components, MUST be synchronised. The time SHOULD be synchronised by means of the NTP service at every location within the local network in question. If a separate management network has been established, an NTP instance SHOULD be positioned within it.

NET.1.2.A9 Protection of Network Management Communication and Access to Network Management Tools (B)

Whenever network management communication takes place via production infrastructure, secure protocols MUST be used. If this is not possible, a dedicated administration network (out-of-band management) MUST be used (see NET.1.1 *Network Architecture and Design*).

If network management tools are accessed from a network outside the management networks in question, authentication and encryption methods that are considered secure MUST be implemented.

NET.1.2.A10 Limitation of SNMP Communication (B)

In principle, insecure versions of the Simple Network Management Protocol (SNMP) MUST NOT be used in network management. If insecure protocols are nevertheless used and not secured via other secure network protocols (e.g. VPN or TLS), a separate management network MUST be used. As a matter of principle, SNMP SHOULD ONLY be used for access with the minimum access rights required. The access authorisations SHOULD be limited to dedicated management servers.

3.2. Standard Requirements

For module NET.1.2 *Network Management*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

NET.1.2.A11 Definition of a Security Policy for Network Management (S)

For network management, a security policy SHOULD be drawn up and continuously maintained. All persons involved in network management SHOULD be familiar with the security policy. The security policy SHOULD form the basis of their work. Regular and transparent reviews SHOULD be conducted to ensure that the policy's requirements are being implemented. The results SHOULD be appropriately documented.

The security policy SHOULD define which areas of network management are to be implemented using central management tools and services. It SHOULD also define the extent to which tasks in the network management of the organisation in question are to be implemented automatically.

In addition, framework conditions and specifications SHOULD be specified for network separation, access control, logging, and communication protection. Framework conditions and specifications SHOULD also be specified for the network management tools used and for the basic operational rules of network management.

NET.1.2.A12 Current Inventory and Documentation of Network Management (S)

Documentation SHOULD be drawn up that describes the management infrastructure of the network in question. It SHOULD include an initial inventory and all changes made in network management. In particular, it SHOULD document which network components are administered using which management tools. Furthermore, all IT workstations and end devices used for network management, as well as all information and management data available on network management operations, SHOULD be included. Ultimately, all interfaces to applications and services outside of network management SHOULD be documented.

The resulting documentation of the actual status of the management infrastructure SHOULD be compared against the network infrastructure documentation (see module NET.1.1 *Network Architecture and Design*).

The documentation SHOULD be complete and up to date at all times.

NET.1.2.A13 Drawing Up a Network Management Concept (S)

Based on the security policy drawn up for network management, a network management concept SHOULD be established and consistently maintained. In doing so, the following minimum aspects SHOULD be taken into account as required:

- methods, techniques, and tools for network management
- protection of access and communication
- network separation, in particular the assignment of network management components to zones
- the scope of monitoring and alerts for each network component
- logging
- automation (particularly of the central distribution of configuration files to switches)
- reporting chains in the event of malfunctions and security incidents
- provisioning of network management information for other areas of the organisation in question
- integration of network management into contingency planning

NET.1.2.A14 Detailed and Implementation Planning (S)

Detailed and implementation planning SHOULD be drawn up for network management infrastructure. It SHOULD consider all the items addressed in the respective security policy and network management concept.

NET.1.2.A15 Concept for Secure Operation of Network Management Infrastructure (S)

A concept for secure operation of network management infrastructure SHOULD be drawn up based on the relevant security policy for network management and the network management concept. This concept SHOULD take into account the application and system operations for the network management tools in use. The manner in which the performance of other operative units can be integrated and controlled SHOULD also be checked.

NET.1.2.A16 Setup and Configuration of Network Management Solutions (S)

Network management solutions SHOULD be established, configured securely, and put into operation based on the security policy, the specified requirements (see NET1.2.A2 *Specification of Network Management Requirements*), and the detailed and implementation plan in the case at hand. Afterwards, the specific processes for network management SHOULD be set up.

NET.1.2.A17 Regular Gap Analysis within the Framework of Network Management (S)

The extent to which the network management solution in use corresponds to the target state SHOULD be checked regularly and transparently. In so doing, whether the existing solution still complies with the relevant security policy and requirements specification SHOULD be checked. The extent to which the management structure implemented and the processes used

comply with the current status SHOULD also be checked. A comparison SHOULD also be made to determine whether the management infrastructure is up to date.

NET.1.2.A18 Training Measures for Management Solutions [Supervisor] (S)

Training measures SHOULD be developed and carried out for the network management solutions used. The measures SHOULD cover the individual circumstances at hand in terms of configuration, availability, and capacity management, as well as typical situations in the field of error management. The training SHOULD be repeated at regular intervals, but at least when there are major technical or organisational changes within the network management solutions.

NET.1.2.A19 ELIMINATED (S)

This requirement has been eliminated.

NET.1.2.A20 ELIMINATED (S)

This requirement has been eliminated.

NET.1.2.A21 Decoupling of Network Management Communication (S)

Administrators SHOULD avoid using direct management access to interface with network components from IT systems outside of their organisation's management networks. If such access is necessary without a central management tool, the communication SHOULD be decoupled. Jump servers of this kind SHOULD be integrated into the management network in question and located in a separate access segment.

NET.1.2.A22 Restriction of Management Functions (S)

The management functions enabled SHOULD be limited to those that are actually required.

NET.1.2.A23 ELIMINATED (S)

This requirement has been eliminated.

NET.1.2.A24 Central Configuration Management for Network Components (S)

It SHOULD be possible to automatically distribute, install, and activate software, firmware, configuration data, and network components over a given network without interrupting operations. The information required for this SHOULD be securely available from a central point and integrated into version management and data backup processes. The central configuration management used for this purpose SHOULD be maintained continuously and audited regularly.

NET.1.2.A25 Status Monitoring for Network Components (S)

The basic performance and availability parameters of central network components SHOULD be monitored continuously. For this purpose, the respective threshold values SHOULD be determined in advance (baselining).

NET.1.2.A26 Alarming and Logging (S)

Important events on network components and network management tools SHOULD be automatically transmitted to a central management system and logged there (see OPS.1.1.5

Logging). In addition, the persons in charge SHOULD be informed automatically. Alerts and logging SHOULD include the following items at minimum:

- failure and non-availability of network or management components
- hardware malfunctions
- failed login attempts
- critical conditions or overloading of IT systems

Event messages and log data SHOULD be transmitted to a central management system either continuously or in a bundled manner. Alarm messages SHOULD be transmitted as soon as they occur.

NET.1.2.A27 Integration of Network Management into Contingency Planning (S)

An organisation's network management solutions SHOULD be integrated into its contingency planning. To this end, network management tools and the configurations of network components SHOULD be backed up and integrated into the organisation's recovery schemes.

NET.1.2.A28 Location of Management Clients for In-Band Management (S)

Dedicated management clients SHOULD be used for administering both internal and external IT systems. To this end, one management client MUST be located on the external network area (for administering IT systems connected to the Internet) and another in the internal area (for administering internal IT systems).

NET.1.2.A29 Using VLANS in the Management Network (S)

If management networks are separated by VLANs, it SHOULD be ensured that the external packet filter and the devices connected to this filter are located in their own sub-network. It MUST also be ensured that the ALG is not bypassed in this process.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.1.2 *Network Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

NET.1.2.A30 Implementing Management Solutions for High Availability (H)

Central management solutions SHOULD be operated in manner that ensures high availability. To this end, the servers and tools involved (including their network connections) SHOULD be designed redundantly. The individual components SHOULD also be provided in a highly available manner.

NET.1.2.A31 Basic Use of Secure Protocols (H)

Only secure protocols SHOULD be used for network management. All the security features of these protocols SHOULD be used.

NET.1.2.A32 Physical Separation of the Management Network [Planner] (H)

An organisation's management network SHOULD be separated physically from its productive networks.

NET.1.2.A33 Physical Separation of Management Segments [Planner] (H)

At minimum, physically separated zones SHOULD be established for managing LAN components, security components, and components for external connections.

NET.1.2.A34 ELIMINATED (H)

This requirement has been eliminated.

NET.1.2.A35 Specifications for Securing Evidence (H)

Collected log data SHOULD be archived for forensic analysis in a legally compliant and audit-compliant manner (see also DER.2.2 *Provisions for IT Forensics*).

NET.1.2.A36 Integration of Network Management Logging into an SIEM Solution (H)

Network management logging SHOULD be integrated into a security information and event management (SIEM) solution. For this purpose, the requirements catalogues used to select network management solutions SHOULD be adapted to reflect the support required for interfaces and transmission formats (see NET.1.2.A2 *Specification of Network Management Requirements*).

NET.1.2.A37 Time Synchronisation Across Locations (H)

Time synchronisation SHOULD be ensured across all of an organisation's sites. A common reference time SHOULD be used for this purpose.

NET.1.2.A38 Specification of Forms of Emergency Operations for Network Management Infrastructure (H)

In order to quickly recover the target software or firmware status and configure the components of network management infrastructure, replacement solutions of a sufficient quality SHOULD be specified.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for securing networks in the standard ISO/IEC 27033, “Information Technology – Security Techniques – Network Security – Part 1: Overview and Concepts to Part 3: Reference Networking Scenarios – Threats, Design Techniques, and Control Issues”.

The BSI has published the document “Secure Connection of Local Networks to the Internet (ISi-LANA)” on the topic of network management.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.1.2 *Network Management*.

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.35 Coercion, Blackmail or Corruption

G 0.37 Repudiation of Actions

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

NET.2.1 WLAN Operation

1. Description

1.1. Introduction

Wireless LANs (WLANs) can be used to create wireless local networks or extend existing wired networks. To this day, almost all the WLAN components available on the market have been based on the IEEE 802.11 standard and its additions. The manufacturer consortium Wi-Fi Alliance plays an important role in this regard as the creator of the industry-agreed “Wi-Fi” standard based on IEEE 802.11. The Wi-Fi Alliance uses the Wi-Fi quality label to confirm that a device has passed certain interoperability and conformity tests.

Within organisations, WLANs can be used to work flexibly with mobile devices and enable them to access internal networks. For this purpose, network access is established within a given organisation via access points. Because they can usually be installed quickly and easily, WLANs are also used to establish temporary networks—for example, at trade fairs or smaller events. Furthermore, network access may be offered in public spaces such as airports or train stations through hotspots. This enables mobile users to connect to the Internet or to their organisation's network. Communication then generally takes place between a central access point and the WLAN component of the end device used.

1.2. Objective

This module systematically demonstrates how WLANs can be established and operated securely in an organisation.

1.3. Scoping and Modelling

Module NET.2.1 *WLAN Operation* must be applied to all communication networks that are established and operated according to the standard series IEEE 802.11 and its extensions.

The module includes basic specifications that must be considered and met when establishing and operating WLANs in organisations. Requirements for the secure use of WLANs are not part of this module. The secure use of WLANs is addressed in module NET.2.2 *WLAN Usage*.

WLANs may be operated in two different modes depending on the needs of the operator in question and the hardware equipment available. In ad-hoc mode, two or more WLAN clients communicate directly with each other. WLANs in ad-hoc mode can set up and configure themselves independently (i.e. without a fixed infrastructure), allowing them to establish a fully meshed parallel network infrastructure. This makes ad-hoc mode unsuitable in an environment that needs to be protected; it is therefore not considered further in this module. In the majority of cases, WLANs are operated in infrastructure mode—that is, the communication of WLAN clients and the connection to wire-bound LAN segments take place via access points.

If corresponding services (e.g. RADIUS) are used for WLAN authentication, the corresponding IT systems on which the services are operated must be secured separately. The modules of the SYS.1 layer, such as SYS.1.1 *General Server*, can be used for this purpose.

In principle, any WLAN operations that have been established should be taken into account when implementing the modules NET.1.1 *Network Architecture and Design*, NET.1.2 *Network Management,* and DER.2.1 *Security Incident Handling*.

2. Threat Landscape

For module NET.2.1 *WLAN Operation*, the following specific threats and vulnerabilities are of particular importance.

2.1. Failure or Disruption of a Radio Network

In radio networks, information is transmitted using electromagnetic radio waves. If there are other electromagnetic sources radiating energy in the same frequency spectrum, these emissions could disrupt wireless communication and, in extreme cases, prevent the operation of a WLAN. This may be caused by other radio systems and devices, such as Bluetooth, microwave ovens, or other WLAN networks. Denial-of-service attacks are also possible. For example, if certain control and management signals are sent repeatedly, this may hinder the availability of a radio network.

2.2. Inadequate Planning of WLAN Usage

Planning errors often turn out to be particularly serious because they can easily create extensive vulnerabilities. If the use of WLANs is planned insufficiently (or not at all), this may result in a number of issues. For example:

- Confidential data might be intercepted—for example, when using WLAN standards that no longer correspond to the state of the art (e.g. WEP for encryption).
- The available transmission capacity could be insufficient. As a consequence, it will not be possible to use bandwidth-intensive applications with the required service quality.
- WLAN coverage may be insufficient to provide network availability in certain places.

2.3. Insufficient Rules on WLAN Usage

If a WLAN infrastructure is not administered centrally, access points left in their default settings will mostly be pre-configured with insufficient security mechanisms (or none at all). For example, if a lack of regulations leads an employee to connect an unauthorised or unsecured access point to an organisation's internal network, this can lead to serious problems. Doing so will undermine practically all the security safeguards taken within the LAN in question, such as the firewall that is meant to protect the LAN against unauthorised external access.

2.4. Inappropriate Selection of Authentication Methods

If authentication methods or mechanisms are missing or inadequate, this may result in vulnerabilities. For example, the IEEE 802.1X (Port-Based Network Access Control) standard defines the EAP (Extensible Authentication Protocol). However, some of the EAP methods described contain vulnerabilities. For example, EAP-MD5 is vulnerable to man-in-the-middle and dictionary attacks. Passwords can be guessed if EAP-MD5 is used and communication can also be intercepted.

2.5. Incorrect Configuration of WLAN Infrastructure

Access points and other WLAN components (e.g. WLAN controllers) provide numerous configuration settings that relate in particular to security features. If the settings configured here are incorrect, communication via an access point will be impossible or insufficiently protected (if at all).

2.6. Insufficient WLAN Security Mechanisms

In their delivered state, WLAN components are often configured with only a few security mechanisms activated (or none at all). Some of these mechanisms are also insufficient and therefore fail to offer adequate protection. Even today, various WLAN components are still used that only support inadequate security mechanisms such as WEP. In some cases, these devices cannot even be updated with stronger security mechanisms. If such devices are used, an attacker might easily eavesdrop on all communications and thereby obtain confidential information.

2.7. Eavesdropping on WLAN Communication

Since radio is a medium that can be shared by several users, the data transmitted via WLANs can easily be intercepted and recorded. Insufficient or non-existent encryption of data can make it easy to eavesdrop on transmissions. In addition, radio networks or the radio waves emitted often exceed the boundaries of users' own premises. Data may thus be broadcast into areas that cannot be controlled and secured by users or their organisations.

2.8. Simulating a Valid Access Point (Rogue access Points)

An attacker can masquerade as part of a given WLAN infrastructure by installing their own access point with a suitable SSID in the vicinity of a WLAN client. A simulated access point of

this kind is referred to as a “rogue access point”. If this access point provides the WLAN client with stronger transmission performance than the real access point, the client will use it as its base station if they do not authenticate each other. Furthermore, the real access point may be disabled by a denial-of-service attack. Users will then log into a network that only pretends to be the target network. This makes it possible for an attacker to eavesdrop on communications. Poisoning or spoofing methods can also simulate a false identity for an attacker or redirect network traffic to the attacker's IT systems. This means that the attacker can listen in on and control communications. Particularly in public radio networks (hotspots), rogue access points are a frequently used means of attack.

2.9. Unprotected LAN Access at Access Points

If access points are mounted visibly and without any physical protection, an attacker may position themselves between the access points and the corresponding switch infrastructure in order to eavesdrop on all the network traffic. Even if wireless communications are encrypted using WPA2, this presents a risk because these methods only protect the air interface and do not take Ethernet connections into account.

2.10. Hardware Damage

Hardware damage may cause disruptions in radio traffic. In the worst-case scenario, the WLAN might even fail completely. This is particularly applicable to WLAN devices that are mounted outside of protected rooms (e.g. in order to cover open spaces). They are exposed to additional threats, such as deliberate damage caused by attackers or environmental damage caused by lightning or other weather.

2.11. Theft of an Access Point

WLAN access points that are installed insecurely in public areas can be stolen. As a consequence, it may be possible to obtain a shared secret key used for authentication with a RADIUS server or another type of key (such as for WPA2 Personal). This information may be used to access a WLAN without authorisation.

3. Requirements

The specific requirements of module NET.2.1 *WLAN Operation* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Planner, Building Services

3.1. Basic Requirements

For module NET.2.1 *WLAN Operation*, the following requirements MUST be met as a matter of priority:

NET.2.1.A1 Definition of a Strategy for WLAN Usage (B)

Before WLANs are used in an organisation, the organisation's general strategy for communication through WLANs MUST be specified. In particular, the organisational units in which WLANs will be used, the applications and purposes they will be used for, and the information that may be transmitted MUST be clarified and defined. The WLAN coverage area MUST also be determined.

Furthermore, it MUST be defined right from the planning phase who will be responsible for the administration of the various WLAN components, which interfaces will be in place between the persons in charge who are involved in WLAN operations, and when specific information must be exchanged among the persons in charge.

NET.2.1.A2 Selection of a Suitable WLAN Standard [Planner] (B)

Within the framework of WLAN planning, there MUST be an initial determination of which of the devices operated by the organisation in question (e.g. microwave ovens, Bluetooth devices) radiate into the ISM band at 2.4 GHz and into the 5 GHz band.

In addition, the security mechanisms available in the individual WLAN standards MUST be compared. In general, it MUST be ensured that only authentication and encryption methods that are generally considered secure will be used. The organisation MUST document its reasons for choosing a particular WLAN standard.

Devices that need to fall back on insecure methods from recognised secure methods MUST NOT be considered during planning.

NET.2.1.A3 Selection of Suitable Crypto Methods for WLAN [Planner] (B)

Communication via the air interface MUST be completely secure in cryptographic terms. Cryptographic methods that are less secure than WPA2 MUST NOT be used.

If WPA2 is used with pre-shared keys (WPA2-PSK), a complex key with a minimum length of 20 characters MUST be used.

NET.2.1.A4 Suitable Location of Access Points [Building Services] (B)

Access points MUST be mounted such that they cannot be accessed or stolen. If they are set up, the required areas MUST be adequately covered. Furthermore, it MUST be ensured to the greatest extent possible that the radio waves are not emitted into areas not designated for WLAN coverage. Outside installations MUST be protected appropriately against weather and electrical discharges.

NET.2.1.A5 Secure Basic Configuration of Access Points (B)

Access points MUST NOT be used in their default configuration. Pre-set SSIDs (service set identifiers), passwords, and cryptographic keys MUST be changed prior to productive use. In

addition, insecure administration access MUST be disabled. Access points MUST ONLY be administered via a suitably encrypted connection.

NET.2.1.A6 Secure Configuration of WLAN Infrastructure (B)

It MUST be ensured that WLAN communication is not used to couple security zones or bypass established protection safeguards.

NET.2.1.A7 Setting Up a Distribution System [Planner] (B)

Before a wired distribution system is established, a basic decision MUST be made as to whether separation will be performed physically or logically through VLANs on the access switches of the wired LAN in question.

NET.2.1.A8 Codes of Conduct in the Event of WLAN Security Incidents (B)

If a security incident occurs, the IT Operation Department MUST initiate appropriate countermeasures:

- At the point where WLAN communication enters the internal LAN in question, communication SHOULD be blocked selectively for every SSID and access point—or even for the entire WLAN infrastructure—in the event of an attack.
- If access points have been stolen, defined security safeguards MUST be implemented to prevent any misuse of the access points or the information stored on them.
- If WLAN clients have been stolen and central certificate-based authentication is being used, the client certificates MUST be blocked.

The possibility of using stolen devices without authorisation in order to access the network of a given organisation MUST be ruled out.

3.2. Standard Requirements

For module NET.2.1 *WLAN Operation*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

NET.2.1.A9 Secure Connection of WLANs to a LAN [Planner] (S)

If WLANs are connected to a LAN, the transition between the WLANs and the LAN SHOULD be protected—for example, with the help of a packet filter. The access point SHOULD be integrated in line with the requirements of NET.2.1.A7 *Setting Up a Distribution System*.

NET.2.1.A10 Drawing Up a Security Policy for WLAN Operation (S)

Based on the general security policy of the organisation in question, essential core aspects SHOULD be specified for the secure use of WLANs. The policy SHOULD be known to all persons in charge who are involved in establishing and operating WLANs. It SHOULD form the basis of their work. The implementation of the policy's requirements SHOULD be checked at regular intervals. If the contents of the policy are not implemented, there MUST be a suitable response. The results SHOULD be documented appropriately.

NET.2.1.A11 Selection of Suitable WLAN Components (S)

Based on the results of the planning phase, a requirements list SHOULD be drawn up that can be used to help evaluate the products available on the market. When procuring WLAN components, data protection and the intercompatibility of the components SHOULD be taken into account along with security.

NET.2.1.A12 Use of a Suitable WLAN Management Solution (S)

A central management solution SHOULD be used. The functional range of the solution used SHOULD be in accordance with the requirements of the WLAN strategy at hand.

NET.2.1.A13 Regular Security Checks of WLANs (S)

WLANs SHOULD be checked regularly for security vulnerabilities. In addition, the WLANs provided SHOULD be searched regularly for access points that have been installed without authorisation. Their performance and coverage SHOULD also be measured. The results of security checks SHOULD be documented transparently and compared against the target condition. Deviations SHOULD be investigated.

NET.2.1.A14 Regular Audits of WLAN Components (S)

All components of WLAN infrastructure SHOULD be checked regularly to ensure that all the specified security safeguards have been implemented and all the components have been configured correctly. Access points mounted in public areas SHOULD be checked randomly at regular intervals to determine whether there have been attempts to open or manipulate them by force. The audit results SHOULD be documented transparently and compared against the target condition. Deviations SHOULD be investigated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.2.1 *WLAN Operation* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

NET.2.1.A15 Using a VPN to Secure WLANs (H)

A VPN SHOULD be used to achieve additional protection of WLAN communications.

NET.2.1.A16 Additional Protection When Connecting WLANs to a LAN (H)

If a WLAN infrastructure is connected to a LAN, the transition between WLANs and the LAN SHOULD be secured in line with the applicable increased protection needs.

NET.2.1.A17 Protecting Communication Between Access Points (H)

Communication between access points via the wireless interface and the LAN SHOULD be encrypted.

NET.2.1.A18 Use of Wireless Intrusion Detection / Wireless Intrusion Prevention Systems (H)

Wireless intrusion detection or prevention systems SHOULD be used.

4. Additional Information

4.1. Useful Resources

The BSI has published the following additional documents related to WLAN:

- BSI Standard for Internet Security (ISi series): Secure Connection of Local Networks to the Internet (ISi-LANA)

The National Institute of Standards and Technology (NIST) has published the following additional documents on WLAN:

- NIST Special Publication 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.2.1 *WLAN Operation*.

G 0.9 Failure or Disruption of Communication Networks

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.44 Unauthorised Entry to Premises

NET.2.2 WLAN Usage

1. Description

1.1. Introduction

Wireless LANs (WLANs) can be used to create wireless local networks or extend existing wired networks. To this day, almost all the WLAN components available on the market have been based on the IEEE 802.11 standard and its additions. The manufacturer consortium Wi-Fi Alliance plays an important role in this regard as the creator of the industry-agreed "Wi-Fi" standard based on IEEE 802.11. The Wi-Fi Alliance uses the Wi-Fi quality label to confirm that a device has passed certain interoperability and conformity tests.

WLANs provide extra convenience and mobility. However, wireless communication also poses an additional risk to the security of information. That is why it is important that both IT operation departments and users be aware of possible risks that may occur if WLANs are used improperly. Users must have the knowledge required to correctly understand and apply security safeguards. In particular, they must know what is expected of them in terms of information security and how they should respond in certain situations when using WLANs.

1.2. Objective

This module is designed to show how WLANs can be used in a secure manner.

1.3. Scoping and Modelling

Module NET.2.2 *WLAN Usage* must be applied to all IT systems (WLAN clients) that use WLANs.

The module includes basic specifications to be considered and fulfilled when using WLANs in order to be able to counteract the specific threats. Requirements for the secure operation of WLANs are not included in this module; they are described in module NET.2.1 *WLAN Operation*. Moreover, the present module does not deal with general aspects of clients. These aspects are covered in module SYS2.1 *General Client* and in the operating-system-specific modules of the SYS layer *IT Systems*. Module NET.2.2 *WLAN Usage* should always be taken into

account when implementing the modules ORP.3 *Awareness and Training in Information Security* and DER.2.1 *Security Incident Handling*.

2. Threat Landscape

For module NET.2.2 *WLAN Usage*, the following specific threats and vulnerabilities are of particular importance.

2.1. Insufficient Knowledge of Rules and Procedures

If users do not know the rules on proper handling of WLANs well enough, they will not be able to adhere to them. They may then connect clients to unfamiliar wireless networks without realising that information transmitted through them without encryption can be intercepted. In addition, information about users (such as the websites they visit) can be collected by the operators of such wireless networks.

2.2. Non-Compliance with Security Safeguards

Due to negligence and insufficient checks, it is relatively common for people to fail to implement some or all of the security safeguards that have been recommended or assigned to them. For example, if a WLAN client is used in ad-hoc mode despite this being explicitly prohibited in the relevant user policy, another client may communicate directly with it. This can allow the second client to access confidential documents that may be shared on the first client without authorisation.

2.3. Eavesdropping on WLAN Communication

Since radio is a medium that can be shared by several users, the data transmitted via WLANs can easily be intercepted and recorded. Insufficient or non-existent data encryption can make it easy to eavesdrop on such transmissions. In addition, radio networks or the radio waves emitted often exceed the boundaries of the premises in use. Data can thus be broadcast into areas that cannot be controlled or secured by the users in question or their organisation.

2.4. Analysis of Connection Data Related to Wireless Communication

In WLANs based on IEEE 802.11, the MAC address of a WLAN card is sent every time data is transmitted. Since it is transmitted in an unencrypted manner, movement profiles can be created for mobile users—for example, when and where users log in to public hotspots.

2.5. Simulating a Valid Access Point (Rogue Access Points)

An attacker can masquerade as part of WLAN infrastructure by installing their own access point with a suitable WLAN name (SSID) in the vicinity of a WLAN client. A simulated access point of this kind is referred to as a “rogue access point”. If this access point provides the WLAN client with stronger transmission performance than the real access point, the client will use it as its base station if they do not authenticate each other. Furthermore, the real access point may be disabled by a denial-of-service attack. Users will then log into a network that

only pretends to be the target network. This makes it possible for an attacker to eavesdrop on communications. Poisoning or spoofing methods can also simulate a false identity for an attacker or redirect network traffic to the attacker's IT systems. This means that the attacker can listen in on and control communications. Particularly in public radio networks (hotspots), rogue access points are a frequently used means of attack.

3. Requirements

The specific requirements of module NET.2.2 *WLAN Usage* are listed below. As a matter of principle, the User is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	User
Further responsibilities	IT Operation Department, Supervisor

3.1. Basic Requirements

For module NET.2.2 *WLAN Usage*, the following requirements MUST be implemented as a matter of priority:

NET.2.2.A1 Creating a User Policy for WLAN [IT Operation Department] (B)

The essential core aspects of secure WLAN usage MUST be specified in a WLAN user policy based on the general security policy of the organisation in question. This user policy MUST describe the particularities of WLAN usage, such as whether, how, and with what devices hotspots may be used.

The policy MUST contain information on which data may be used and transmitted over a WLAN and which may not.

It MUST describe how to handle client-side security solutions. The user policy MUST contain a clearly stated ban on connecting unauthorised access points to the network of the respective organisation. Moreover, the policy MUST state that WLAN interfaces must be disabled if they are not used for a longer period.

There MUST be regular checks to ensure that the policy's requirements have been implemented correctly. If this is not the case, there MUST be an appropriate response. The results SHOULD be appropriately documented.

NET.2.2.A2 Awareness and Training of WLAN Users [Supervisor, IT Operation Department] (B)

The users of WLAN components (mainly WLAN clients) MUST be made aware of and trained on the safeguards stated in the corresponding user policy. Suitable training MUST be

identified and established for this purpose. What WLAN-specific security settings mean and why they are important MUST be explained in detail to users. In addition, users MUST be informed of the threats that result from bypassing or disabling these security settings.

The training content in question MUST always be adapted to the respective operational scenarios. In addition to training on WLAN security mechanisms, users MUST be given a copy of their organisation's WLAN security policy and made aware of the measures it contains. Users MUST also be made aware of the possible dangers posed by unfamiliar WLANs.

NET.2.2.A3 Safeguarding WLAN Usage in Hotspots [IT Operation Department] (B)

If the use of external hotspots is permitted, the following MUST be implemented:

- Every user of a hotspot MUST know the security requirements and then decide if and under which conditions hotspot usage is allowed.
- If hotspots are used, it SHOULD be ensured that the connection between the hotspot access point and the user's IT system is cryptographically secured according to the state of the art.
- WLANs that are only used sporadically SHOULD be deleted from users' histories.
- The option to log into WLANs automatically SHOULD be disabled.
- If possible, separate user accounts with a secure basic configuration and restrictive authorisations SHOULD be used.
- It SHOULD be ensured that users with administrator authorisations can never log into external WLANs from their clients.
- In order to transmit sensitive data, all the necessary security safeguards (especially appropriate encryption) MUST be activated on the clients involved.
- If a WLAN interface is not used over an extended period of time, it MUST be disabled.
- When using publicly available WLANs, users MUST use a virtual private network (VPN) to access internal resources of their organisation.

3.2. Standard Requirements

For module NET.2.2 *WLAN Usage*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be MET as a matter of principle.

NET.2.2.A4 Codes of Conduct in the Event of WLAN Security Incidents (S)

In case of WLAN security incidents, users SHOULD act as follows:

- Users SHOULD save their work.
- They should terminate their WLAN connection and disable the WLAN interface on their client.
- Users SHOULD document any error messages and deviations as precisely as possible. Users SHOULD also document what they were doing before and during the security incident.

- Users SHOULD notify the IT Operation Department via a suitable escalation level (e.g. the user help desk). If the WLAN interface in question is not used for a longer period of time, it MUST be disabled.
- When using publicly available WLANs, users MUST use a virtual private network (VPN) to access internal resources of their organisation.

3.3. Requirements in Case of Increased Protection Needs

No requirements with increased protection needs are defined for module NET.2.2 *WLAN Usage*.

4. Additional Information

4.1. Useful Resources

The BSI has published the following additional documents related to WLAN:

- BSI Standard for Internet Security (ISi series): Secure Connection of Local Networks to the Internet (ISi-LANA)
- The National Institute of Standards and Technology (NIST) has published the following additional documents on WLAN:
    - NIST Special Publication 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs)
    - NIST Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.2.2 *WLAN Usage*.

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.23 Unauthorised Access to IT Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.43 Attack with Specially Crafted Messages

NET.3.1 Routers and Switches

1. Description

1.1. Introduction

Routers and switches form the backbone of today's data networks. The failure of one or more of these devices can bring an entire IT infrastructure to a halt, which is why they require special protection.

Routers work on OSI layer 3 (the network layer) and transport data packets based on the destination IP addresses in IP headers. Routers are able to connect networks with different topologies. They are used to segment local networks or connect local networks via wide area networks. A router identifies a suitable connection between the source system or network and the destination system or network. In most cases, this is performed by forwarding data packets to the next router.

The first switches worked on OSI layer 2, but switches with different functions are now available. Manufacturers usually give their devices designations that indicate the OSI layer they support. This has resulted in the terms "layer 2", "layer 3", and "layer 4 switch", whereby layer 3 and layer 4 switches are actually already routers in functional terms. While the functions of switches and routers were originally different, they are now frequently combined in one device.

1.2. Objective

This module describes how routers and switches can be used securely.

1.3. Scoping and Modelling

Module NET.3.1 *Routers and Switches* must be applied to each router and switch used in the information domain under consideration.

A wide selection of different routers and switches from different manufacturers are available on the market. This module does not describe any specific requirements for certain products. It is designed to be as manufacturer-agnostic as possible.

Due to the amalgamation of the functions of routers and switches, the majority of its requirements are applicable to both routers and switches. In most instances, this module does not differentiate between these device types.

Today, nearly all the operating systems of servers and clients also offer a routing feature. This module does not mention any requirements for enabled routing features in server and client operating systems.

In addition, aspects of infrastructural security such as suitable installation, power supplies, or cabling are not covered in this module. Security requirements on these topics can be found in the respective modules of the INF *Infrastructure* layer.

This module does not describe any requirements for securing virtual routers and switches. The firewall features that routers and switches may offer are not addressed either. Module NET.3.2 *Firewall* must be implemented in this regard. Some aspects of network design and management are also important for using routers and switches and will be mentioned within the framework of the corresponding requirements. Additional information for establishing, designing, and managing a network can be found in the modules NET.1.1 *Network Architecture and Design* and NET.1.2 *Network Management*.

In principle, routers and switches should also be considered when implementing the modules ORP.4 *Identity and Access Management*, OPS.1.1.3 *Patch and Change Management*, CON.3 *Backup Concept*, and OPS.1.1.2 *Proper IT Administration*.

2. Threat Landscape

For module NET.3.1 *Routers and Switches*, the following specific threats and vulnerabilities are of particular importance.

2.1. Distributed Denial of Service (DDoS)

Within the framework of a DDoS attack on a protected network (for example, via TCP-SYN flooding or a UDP packet storm), the large number of network connections that must be processed may result in the router failing. This may render certain services unavailable in the local area network (LAN) or cause the entire LAN to fail.

2.2. Manipulation

If an attacker manages to access a router or switch without authorisation, they might re-configure the devices or even start additional services. For example, the configuration may be changed in a way that blocks services, clients, or entire network segments. At the same time, an attacker can intercept, read, or manipulate network traffic at a switch.

2.3. Incorrect Configuration of a Router or Switch

Routers and switches are delivered with a default configuration in which many services are activated. Login banners also give away the model and version numbers of devices, for example. When routers and switches with insecure factory settings are used in production

environments, it is easier to access them without authorisation. In the worst-case scenario, this might make internal services accessible to attackers.

2.4. Improper Planning and Design

Many organisations plan and design the use of routers and switches improperly. Among other things, this results in devices being procured that do not have sufficient capacity (in terms of performance or the number of ports, for example). As a consequence, a router or switch can be overloaded the first time it is used. This means that services or entire networks might not be available and considerable resources may be required to correct the situation.

2.5. Incompatible Active Network Components

Compatibility issues may occur, particularly if active network components from other manufacturers are added to existing networks or networks are operated with components from different manufacturers. If active network components with different implementations of the same communication method are operated together in one and the same network, individual sub-areas of the network, of certain services, or even the entire network may fail.

2.6. MAC Flooding

During MAC flooding, an attacker sends a large number of requests with different source MAC addresses to a switch. Once the switch has reached the maximum number of MAC addresses it can store, it starts sending all requests to all the IT systems in the network. As a consequence, the attacker may view the network traffic.

2.7. Spanning Tree Attacks

During spanning tree attacks, an attacker sends Bridge Protocol Data Units (BPDUs) in order to induce switches to consider the attacker's own (malicious) switch as the root bridge. Network traffic is thereby routed through the switch of the attacker, enabling them to record all information sent via the switch. As a consequence, the attacker might initiate DDoS attacks and force the network to re-establish the spanning tree topology with the help of incorrect BPDUs, which might cause the network to fail.

2.8. GARP Attacks

During gratuitous ARP (GARP) attacks, an attacker sends unrequested ARP replies to certain targets or to all the IT systems in the same sub-network. In these forged ARP replies, the attacker enters their MAC address as an assignment to a third-party IP address and induces the target to change their ARP table in such a way that the network traffic will then be sent to the attacker instead of its valid destination. As a consequence, the attacker may record or manipulate the communication between the targets.

3. Requirements

The specific requirements of module NET.3.1 *Routers and Switches* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module NET.3.1 *Routers and Switches*, the following requirements MUST be met as a matter of priority:

NET.3.1.A1 Secure Basic Configuration of a Router or Switch (B)

Prior to using a router or switch, it MUST be configured securely. All configuration changes SHOULD be documented in a transparent manner. The integrity of the configuration files MUST be protected appropriately. Before access passwords are stored, they MUST be secured using an up-to-date cryptographic method (see CON.1 *Crypto Concept*).

Routers and switches MUST be configured in such a way that only absolutely necessary services, protocols, and functional extensions are used. Services, protocols, and functional extensions that are not required MUST be disabled or uninstalled completely. Unused interfaces on routers and switches MUST also be disabled. If possible, unused network ports MUST be disabled or at least assigned to an unassigned VLAN set up for this purpose.

If functional extensions are used, the security policies of the organisation in question MUST continue to be met. The use of such extensions SHOULD also be justified and documented.

Information on internal configurations and operating statuses MUST be hidden from third parties. Unnecessary information services MUST be disabled.

NET.3.1.A2 ELIMINATED (B)

This requirement has been eliminated.

NET.3.1.A3 ELIMINATED (B)

This requirement has been eliminated.

NET.3.1.A4 Protection of Administration Interfaces (B)

All administration and management access to routers and switches MUST be restricted to individual source IP addresses or address ranges. It MUST be ensured that it is not possible to access the administration interfaces directly from untrusted networks.

Suitably encrypted protocols SHOULD be used to administer and monitor routers and switches. If unencrypted protocols are nevertheless used, a separate administration network (out-of-band management) MUST be used for administration. The management interfaces and administration connections MUST be protected by means of a separate firewall. Appropriate time limits MUST be specified for the interfaces (e.g. for timeouts).

All services not required for management interfaces MUST be disabled. If a network component has a dedicated hardware interface, any unauthorised access to this interface MUST be prevented appropriately.

NET.3.1.A5 Protection Against Fragmentation Attacks (B)

Protection mechanisms MUST be enabled on routers and layer 3 switches in order to fend off IPv4 and IPv6 fragmentation attacks.

NET.3.1.A6 Emergency Access to Routers and Switches (B)

Administrators MUST always be capable of directly accessing routers and switches to ensure continuous administration even if an entire network fails.

NET.3.1.A7 Logging on Routers and Switches (B)

A router or switch MUST be configured in such a way that it logs the following events, among others:

- configuration changes (automatically whenever possible)
- reboots
- system errors
- Status changes for each interface, system, and network segment
- Login errors

NET.3.1.A8 Regular Backups (B)

The configuration files of routers and switches MUST be backed up at regular intervals. The backup copies MUST be created in such a way that they can be accessed in an emergency.

NET.3.1.A9 Operational Documentation (B)

The most important operational tasks of a router or switch MUST be documented appropriately. All configuration changes and security-relevant tasks SHOULD be documented. The documentation SHOULD be protected against unauthorised access.

3.2. Standard Requirements

For module NET.3.1 *Routers and Switches*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

NET.3.1.A10 Creating a Security Policy(S)

A specific security policy MUST be drawn up for routers and switches based on the general security policy of the organisation in question. This security policy SHOULD transparently

describe the requirements and specifications for the secure operation of routers and switches. The policy SHOULD be known to all administrators and be integral to their work. If the policy is changed or deviations from the agreed requirements are allowed, this SHOULD be coordinated with the CISO and documented. It SHOULD be checked regularly whether the policy is still being properly implemented. The results SHOULD be documented appropriately.

NET.3.1.A11 Procurement of a Router or Switch (S)

Prior to procuring routers and switches, a requirements list SHOULD be drawn up based on the relevant security policy that can be used to evaluate the products available on the market. It SHOULD be ensured that the desired security level of the organisation in question can be achieved with the devices to be procured. The procurement process SHOULD thus be based on the requirements of the aforementioned security policy.

NET.3.1.A12 Drawing Up a Configuration Checklist for Routers and Switches (S)

A configuration checklist SHOULD be created that can be used to check the most important security-relevant settings on routers and switches. Since secure configurations strongly depend on the purpose at hand, the different requirements of these devices SHOULD be taken into consideration within the framework of the configuration checklist.

NET.3.1.A13 Administration Using a Separate Management Network (S)

Routers and switches SHOULD only be administered via a separate management network (out-of-band management). Any administration interface available via the actual data network at hand (in-band) SHOULD be disabled. The available security mechanisms of the management protocols used for authentication, integrity assurance, and encryption SHOULD be activated. All insecure management protocols SHOULD be disabled.

NET.3.1.A14 Protection Against Misuse of ICMP Messages (S)

The protocols ICMP and ICMPv6 SHOULD be filtered restrictively.

NET.3.1.A15 Bogon and Spoofing Filtering (S)

Attackers SHOULD be prevented from entering routers and switches with the help of forged, reserved, or unassigned IP addresses.

NET.3.1.A16 Protection Against “IPv6 Routing Header Type-0” attacks (S)

When using IPv6, mechanisms SHOULD be used to detect and prevent attacks on the type-0 routing header.

NET.3.1.A17 Protection Against DoS and DDoS Attacks (S)

Mechanisms SHOULD be used that detect and fend off high-volume attacks and TCP state exhaustion attacks.

NET.3.1.A18 Configuration of Access Control Lists (S)

Access to routers and switches SHOULD be defined with the help of access control lists (ACLs). Based on the security policy of the organisation in question, the ACL SHOULD define which IT systems or networks (and corresponding methods) may be used to access a router or switch. If

there are no specific rules, a restrictive whitelist approach SHOULD be preferred as a matter of principle.

NET.3.1.A19 Protection of Switch Ports (S)

The ports of a switch SHOULD be protected against unauthorised access.

NET.3.1.A20 Security Aspects of Routing Protocols (S)

Routers SHOULD authenticate themselves when exchanging routing information or transmitting updates for routing tables. Only routing protocols that support this SHOULD be used.

Dynamic routing protocols SHOULD only be used in secure networks. They MUST NOT be used in demilitarised zones (DMZs). In DMZs, static routes SHOULD be entered instead.

NET.3.1.A21 Identity and Authorisation Management in Network Infrastructure (S)

Routers and switches SHOULD be connected to a central identity and authorisation management system (see ORP.4 *Identity and Access Management)*.

NET.3.1.A22 Contingency Planning for Routers and Switches (S)

There SHOULD be planning and preparation for the errors in routers or switches that can be diagnosed in an emergency. There SHOULD also be planning and preparation regarding how to remedy the errors identified. Appropriate actions SHOULD be defined for typical failure scenarios and updated at regular intervals.

The contingency planning for routers and switches SHOULD be coordinated with overarching fault and contingency planning. The contingency planning SHOULD be based on the general contingency planning concept at hand (see DER.4 *Business Continuity Management*). It SHOULD be ensured that contingency planning documentation and the instructions it contains are available in paper form. The procedure described in the contingency planning concept SHOULD be tested regularly.

NET.3.1.A23 Audits and Penetration Tests (S)

Routers and switches SHOULD be checked for known security issues at regular intervals. Audits SHOULD also be performed regularly. This SHOULD include checking whether the actual situation corresponds to the basic configuration defined as secure. The results SHOULD be clearly documented and compared against the target situation. Deviations SHOULD be investigated.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.3.1 *Routers and Switches* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

NET.3.1.A24 Use of Network Access Controls (H)

Port-based access control according to IEEE 802.1x SHOULD be implemented on the basis of EAP-TLS. Implementations according to the standards IEEE 802.1x-2001 and IEEE 802.1x-2004 SHOULD NOT be performed.

NET.3.1.A25 Advanced Integrity Protection for Configuration Files (H)

If a router or switch crashes, it SHOULD be ensured that no legacy or incorrect configurations (including ACLs) are used when recovering and restarting the device.

NET.3.1.A26 High Availability (H)

The implementation of a high-availability solution SHOULD NOT impair the operation of routers and switches or their security features, or reduce the level of security. Routers and switches SHOULD be designed redundantly. In so doing, it SHOULD be ensured that the security policy of the organisation in question is observed.

NET.3.1.A27 Bandwidth Management for Critical Applications and Services (H)

Routers and switches SHOULD include and use features that can detect applications and prioritise bandwidths.

NET.3.1.A28 Use of Certified Products (H)

Routers and switches with a Common Criteria security evaluation of at least EAL4 SHOULD be used.

4. Additional Information

4.1. Useful Resources

The BSI has published further information on the security of routers and switches in the BSI Standards for Internet Security (ISi series).

The Institute of Electrical and Electronics Engineers (IEEE) has published the standards IEEE 802.1Q, “IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks”, and IEEE 802.1AE, “IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security”.

RFC 6165, “Extensions to IS-IS for Layer-2 Systems”, and RFC 7348, “Virtual Extensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer-2 Networks over Layer-3 Networks”, provide further information on routers and switches.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.3.1 *Routers and Switches*.

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

NET.3.2 Firewall

1. Description

1.1. Introduction

A firewall is a system consisting of hardware and software components that is used to securely connect IP-based data networks. It uses a firewall structure to restrict the information flow that is technically feasible to communications that are previously defined as secure in a corresponding policy. In this context, "secure" means that only the access or data streams desired between different networks are allowed.

In many cases, securing network gateways no longer involves an individual component; a whole range of IT systems takes on different tasks (e.g. filtering packets exclusively or strictly disconnecting network connections with the help of proxy features). The term "application level gateway" (ALG), which is used in this module, refers to a firewall component that controls data streams on the basis of security proxies.

A firewall is installed at the gateway between networks with differing levels of trustworthiness. Internet and intranet connections are not the only example of networks with different levels of trustworthiness. Two internal networks in the same organisation can also have different protection requirements. For example, an office communication network usually requires less protection than the network of a human resources department, where particularly sensitive personal data is transferred.

1.2. Objective

The objective of this module is to facilitate the secure use of a firewall or a firewall structure with the help of the requirements described in order to ensure secure connections between networks with different protection needs.

1.3. Not in scope and modelling

Module NET.3.2 *Firewall* must be applied to each firewall in the information domain under consideration.

A typical application case involves the protection of an external connection, such as at the interface between an internal network and the Internet or in situations involving links to networks of business partners. However, this module must also be applied when two internal networks with different protection needs within an organisation are linked (for example, when separating an office communication network from the network of a development department if particularly confidential data is processed there).

The present module builds upon module NET.1.1 *Network Architecture and Design* and includes specific requirements to be observed and complied with when procuring, establishing, configuring and operating network-based firewalls.

In order to secure networks, additional network components are typically required, such as routers and switches. The related requirements are not covered in this module, but can be found in NET.3.1 *Routers and Switches*. If a firewall assumes the tasks of a router or switch, the requirements included in module NET.3.1 *Routers and Switches* also apply to the firewall.

Furthermore, products such as next-generation firewalls (NGFW) or unified threat management (UTM) firewalls that also include functional extensions (e.g. VPN, intrusion detection and intrusion prevention systems (IDS/IPS), virus scanners, or spam filters) are not addressed. Security aspects of these functional extensions are not part of this module; they are addressed in the modules NET.3.3 *VPN* and OPS1.1.4 *Protection Against Malware*, for example.

Application detection and filtering are not addressed either. These are common features of next-generation firewalls and IDS/IPS. Since these products involve different implementations, it is advisable to consider them individually depending on the use scenario at hand. This module does not address the individual protection options for server services that are offered externally, such as through a reverse proxy or for web services with the help of a web application firewall (WAF). Furthermore, aspects of infrastructural security (e.g. appropriate installation or power supplies) are not discussed in this module; they can be found in the respective modules of the INF *Infrastructure* layer.

Directory services should always be included as part of the modules ORP.4 *Identity and Access Management*, OPS.1.1.3 *Patch and Change Management*, and OPS.1.1.2 *Proper IT Administration*.

2. Threat Landscape

For module NET.3.2 *Firewall*, the following specific threats and vulnerabilities are of particular importance.

2.1. Distributed denial of service (DDoS)

Within the framework of a DDoS attack on a protected network (e.g. via TCP-SYN flooding or a UDP packet storm), the large number of network connections that must be processed may result in the firewall failing. This may render certain services unavailable in the local area network (LAN) or cause the entire LAN to fail.

2.2. Manipulation

If an attacker manages to access a firewall or a corresponding administration interface, they may manipulate data in any number of ways. For example, they may change the configuration, start additional services, or install malware. They may also eavesdrop on communication links in the manipulated IT system. The firewall's rules may also be changed in a way that makes it possible to access the firewall and the respective organisation’s intranet from the Internet. Furthermore, an attacker may start a denial-of-service attack (DoS) by using the firewall's rule set to prevent access to individual server services.

2.3. Bypassing firewall rules

Attackers may use basic mechanisms in network protocols to bypass a firewall's rules (e.g. through fragmentation attacks) and enter a protected area. In the protected area, they may then cause additional damage (e.g. by accessing, manipulating, or deleting sensitive data).

2.4. Incorrect configuration and errors in operating a firewall

An improperly configured or operated firewall may have dramatic effects on the availability of services. If, for example, firewall rules are set improperly, network access may be blocked. Furthermore, incorrect configurations may result in insufficient protection of IT systems. In the worst-case scenario, this might make internal services accessible to attackers.

3. Requirements

The specific requirements of module NET.3.2 *Firewall* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module NET.3.2 *Firewall*, the following requirements MUST be implemented as a matter of priority:

NET.3.2.A1 Creating a Security Policy (B)

A specific security policy for firewalls MUST be drawn up based on the general security policy of the organisation in question. The specific policy MUST transparently describe the requirements and specifications for securely operating firewalls. The policy MUST be known

to all employees in charge in firewalls and be integral to their work. If the policy is changed or deviations from the requirements are allowed, this MUST be coordinated with the CISO and documented. The correct implementation of the policy MUST be regularly reviewed. The results MUST be documented in an appropriate manner.

NET.3.2.A2 Definition of Firewall Rules (B)

All communications between two given networks MUST pass through a firewall. It MUST be ensured that no unauthorised connections from the outside can be established with a protected network. In addition, unauthorised connections MUST NOT be established from a protected network.

Unambiguous rules MUST be defined for a firewall that specify which communication links and data streams are allowed. Any other connections MUST be prevented by the firewall (whitelist approach). The communication relationships with connected service servers that are routed through the firewall MUST be taken into consideration in its rules.

Persons in charge MUST be appointed to develop, implement, and test filter rules. In addition, it MUST be clear who is allowed to change filter rules. The decisions taken and the relevant information and reasons for them MUST be documented.

NET.3.2.A3 Configuring Appropriate Filter Rules on the Packet Filter (B)

Based on the firewall rules from NET.3.2.A2 *Definition of Firewall Rules*, appropriate filter rules must be defined and configured for the packet filter.

A packet filter MUST be configured to discard any invalid TCP flag combinations. As a matter of principle, filtering MUST always be performed in a stateful manner. Stateful filter rules MUST also be configured for the connectionless protocols UDP and ICMP. A firewall MUST filter the ICMP and ICMPv6 protocols restrictively.

NET.3.2.A4 Secure Firewall Configuration (B)

Before a firewall is used, it MUST be configured securely. All configuration changes MUST be documented transparently. The integrity of the configuration files MUST be protected appropriately. Before access passwords are stored, they MUST be secured using an up-to-date cryptographic method (see CON.1 *Crypto Concept*). A firewall MUST be configured in such a way that only the services absolutely required are available. If functional extensions are used, the security policies of the organisation in question MUST continue to be met. The use of such extensions MUST also be justified and documented. Any unnecessary (information) services and functional extensions MUST be disabled or uninstalled completely. Information on internal configurations and operating statuses MUST be hidden from third parties whenever possible.

NET.3.2.A5 ELIMINATED (B)

This requirement has been eliminated.

NET.3.2.A6 Protection of Administration Interfaces (B)

All administration and management access to firewalls MUST be restricted to individual source IP addresses or address ranges. It MUST be ensured that it is not possible to access administration interfaces from untrustworthy networks.

Only secure protocols MUST be used to manage or monitor firewalls. Alternatively, a dedicated administration network (out-of-band management) MUST be used. Appropriate time limits MUST be specified for the user interfaces.

NET.3.2.A7 Emergency Access to the Firewall (B)

It MUST always be possible to access a firewall directly in order to manage it locally, even if the entire network has failed.

NET.3.2.A8 Prevention of Dynamic Routing (B)

Dynamic routing MUST be disabled in the settings of a firewall unless the packet filter is being used as a perimeter router in accordance with module NET.3.1 *Routers and Switches*.

NET.3.2.A9 Logging (B)

Firewalls MUST be configured to log the following events at minimum:

- rejected network connections (source and destination IP addresses, source and destination ports or ICMP/ICMPv6 type, dates, times)
- failed attempts to access system resources due to improper authentication, lack of authorisation, lack of resources
- error messages from firewall services
- general system error messages
- configuration changes (automatically whenever possible)

If security proxies are used, security breaches and violations of access control lists (ACLs or access lists) MUST be logged in a suitable manner. The types of protocol violations or ACL violations, source and destination IP addresses, source and destination ports, services, dates and times and, if necessary, the duration of connections MUST be logged at minimum.

When a user provides authentication to a security proxy, either the authentication data or solely the information on a failed authentication attempt MUST also be logged.

NET.3.2.A1 Protection Against Fragmentation Attacks on the Packet Filter (B)

Protection mechanisms MUST be enabled on packet filters in order to fend off IPv4 and IPv6 fragmentation attacks.

NET.3.2.A11 ELIMINATED (B)

This requirement has been eliminated.

NET.3.2.A12 ELIMINATED (B)

This requirement has been eliminated.

NET.3.2.A13 ELIMINATED (B)

This requirement has been eliminated.

NET.3.2.A14 Operational Documentation (B)

The operational tasks of a firewall MUST be documented in a transparent manner. All configuration changes and security-relevant tasks MUST be documented—in particular,

changes made to the system services and the rule set of the firewall. This documentation MUST be protected against unauthorised access.

NET.3.2.A15 Procuring a Firewall (B)

Prior to procuring a firewall, a requirements list MUST be drawn up that can be used to evaluate the products available on the market. It SHOULD be ensured that the desired security level of the organisation in question can be achieved with the firewall it selects. Hence, the procurement process MUST be based on the requirements of the organisation's security policy.

If IPv6 is used, the packet filter MUST check IPv6 extension headers. Furthermore, it MUST be possible to configure IPv6 adequately for IPv4.

3.2. Standard Requirements

For module NET.3.2 *Firewall*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

NET.3.2.A16 Creation of a “P-A-P” structure (S)

A "packet filter – application level gateway – packet filter" (P-A-P) structure SHOULD be used. It MUST consist of several components, each with appropriate hardware and software. Application layer security proxies SHOULD be available for the main protocols used. For other services, at least generic security proxies for TCP and UDP SHOULD be used. The security proxies SHOULD also be executed in a secured runtime environment of the operating system in use.

NET.3.2.A17 Disabling IPv4 or IPv6 (S)

If IPv4 or IPv6 protocol is not required in a given network segment, it SHOULD be disabled at the respective firewall network access point (e.g. at the corresponding firewall interface). If IPv4 or IPv6 protocol is not required or used, it SHOULD be disabled completely on the firewall.

NET.3.2.A18 Administration Using a Separate Management Network (S)

Firewalls SHOULD only be administered using a separate management network (out-of-band management). Any administration interface available via the actual data network at hand (in-band) SHOULD be disabled. Communication in a management network SHOULD be limited to a few management protocols with well-defined origins and destinations via management firewalls (see NET.1.1 *Network Architecture and Design*). The available security mechanisms of the management protocols used for authentication, integrity assurance, and encryption SHOULD be activated. All insecure management protocols SHOULD be disabled (see NET.1.2 *Network Management*).

NET.3.2.A19 Protection Against TCP SYN Flooding, UDP Packet Storms, and Sequence Number Guessing on the Packet Filter (S)

On packet filters protecting server services that are available from untrustworthy networks, a suitable limit SHOULD be configured for semi-open and open connections.

On packet filters protecting server services that are available from untrustworthy (or less trustworthy) networks, rate limits SHOULD be set for UDP data streams.

On outer packet filters, the random generation of initial sequence numbers (ISN) SHOULD be enabled for outgoing TCP connections unless this is already implemented by security proxies.

NET.3.2.A20 Protection of Fundamental Internet Protocols (S)

The protocols HTTP, SMTP, and DNS (including their encrypted versions) SHOULD be routed via protocol-specific security proxies.

NET.3.2.A21 Temporary Decryption of Data Traffic (S)

Encrypted connections to untrusted networks SHOULD be decrypted temporarily in order to verify the protocol and check the data for malware. In so doing, the relevant legal framework conditions SHOULD be taken into consideration.

The component that temporarily decrypts data traffic SHOULD prevent the use of outdated encryption options and cryptographic algorithms.

The TLS proxy SHOULD also be able to check whether certificates are trustworthy. If a certificate is not trustworthy, it SHOULD be possible to reject the respective connection. It SHOULD be possible to subsequently integrate proprietary certificates in order to be able to configure and check “internal” root certificates, as well. Pre-configured certificates SHOULD be checked and removed if they are not required.

NET.3.2.A22 Secure Time Synchronisation (S)

A firewall's system time SHOULD be synchronised with a Network Time Protocol (NTP) server. Firewalls SHOULD not permit external time synchronisation.

NET.3.2.A23 System Monitoring and Evaluation (S)

Firewalls SHOULD be integrated into an appropriate system monitoring concept. Whether a firewall itself and the services operated on it are working properly SHOULD be constantly monitored. Should errors occur or thresholds be exceeded, the appropriate operational personnel SHOULD be alerted. Furthermore, alarm messages SHOULD be generated automatically for defined events. Log data or status messages SHOULD ONLY be transmitted using secure communication paths.

NET.3.2.A24 Audits and Penetration Tests (S)

Firewall structures SHOULD be checked for known security issues at regular intervals. Regular penetration tests and audits SHOULD be performed.

NET.3.2.A32 Firewall Contingency Planning (S)

Diagnosis and troubleshooting SHOULD be planned and prepared in advance. Appropriate actions SHOULD be defined for typical failure scenarios and updated at regular intervals.

Contingency planning for firewalls SHOULD be coordinated with an organisation's overall incident and emergency preparedness. It SHOULD be based on the general contingency planning concept at hand (see DER.4 *Business Continuity Management*). It SHOULD be ensured that contingency planning documentation and the instructions it contains are available in

paper form. The procedure described in the contingency planning concept SHOULD be tested regularly.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.3.2 Firewall are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

NET.3.2.A25 Advanced Integrity Protection for Configuration Files (H)

When restoring a firewall that has crashed, it SHOULD be ensured that no legacy or incorrect configurations (among other things, access lists) are used. This SHOULD also apply if an attacker manages to restart a firewall.

NET.3.2.A26 Outsourcing of Functional Extensions to Dedicated Hardware (H)

Functional extensions of firewalls SHOULD be outsourced to dedicated hardware and software.

NET.3.2.A27 Use of Different Firewall Operating Systems and Products in Multi-Layer Firewall Architecture (H)

In a multi-tier firewall architecture, different operating systems and products SHOULD be used for the outer and inner firewalls.

NET.3.2.A28 Central Filtering of Active Content (H)

Active content SHOULD be filtered in a centralised manner according to the security objectives of the organisation in question. To this end, the encrypted data traffic SHOULD also be decrypted. The required security proxies SHOULD support the filtering of active content.

NET.3.2.A29 Use of High-Availability Solutions (H)

Packet filters and application level gateways SHOULD be designed to ensure high availability. Furthermore, there SHOULD be two independent options for accessing external networks (e.g. Internet access through two different providers). Internal and external routers and any other active components involved (e.g. switches) SHOULD also be designed to ensure high availability.

Even after an automatic failover, firewall structures SHOULD comply with the requirements of the security policy at hand (e.g. "fail safe" or "fail secure").

This function SHOULD be monitored on the basis of multiple parameters. Function monitoring SHOULD not be based on a single criterion. The log files and warnings of high-availability solutions SHOULD be checked at regular intervals.

NET.3.2.A30 Bandwidth Management for Critical Applications and Services (H)

In order to ensure bandwidth management for critical applications and services, packet filters with a corresponding bandwidth management function SHOULD be used at network gateways and at the gateways between different security zones.

NET.3.2.A31 Use of Certified Products (H)

Firewalls with a Common Criteria security evaluation of at least level EAL4 SHOULD be used.

4. Additional Information

4.1. Useful Resources

The BSI has published the following additional documents related to firewalls:

- "Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf" [Technical Guideline for Internal Telecommunications Systems with Increased Protection Requirements] BSI-TL-02103, version 2.0
- "Cryptographic Mechanisms: Recommendations and Key Lengths: Use of Transport Layer Security (TLS)", version: 2020-1, BSI TR-02102-2
- Secure connection of local networks to the Internet (ISi-LANA)

The National Institute of Standards and Technology (NIST) provides recommendations for using firewalls in NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy".

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.3.2 *Firewall*.

G 0.8 Failure or Disruption of the Power Supply

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.39 Malware

G 0.40 Denial of Service

G 0.41 Sabotage

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

NET.3.3 VPN

1. Description

1.1. Introduction

With the help of virtual private networks (VPNs), sensitive data can be transmitted through untrustworthy networks like the Internet. A VPN is a virtual network that is operated within another network, but logically separated from this network. A VPN only uses the network as a transport medium; it is independent of the structure and design of the network used. VPNs can use cryptographic procedures to protect the integrity and confidentiality of data. VPNs also enable the secure authentication of communication partners when several networks or IT systems are connected to each other via leased lines or public networks.

1.2. Objective

This module defines requirements for the secure and systematic planning, implementation, and operation of a VPN.

1.3. Scoping and Modelling

This module must be applied to every option that is available to access a given organisation's network via a VPN endpoint.

The module does not deal with the basics of secure networks and how to assemble them (see NET.1.1 *Network Architecture and Design*). Moreover, this module does not cover all the processes involved in operating a VPN. VPNs should always be included as part of the modules ORP.4 *Identity and Access Management*, OPS.1.1.3 *Patch and Change Management*, OPS.1.2.5 *Remote Maintenance*, OPS.1.1.2 *Proper IT Administration*, and CON.1 *Crypto Concept*.

Recommendations on how to configure the operating systems of VPN end points are not part of this module either. Corresponding requirements are included in the modules SYS.1.1 *General Server* and SYS.2.1 *General Client*, as well as in the relevant operating-system-specific modules of the IT-Grundschutz Compendium.

2. Threat Landscape

For module NET.3.3 *VPN*, the following specific threats and vulnerabilities are of particular importance:

2.1. Inadequate Planning of VPN Usage

If a VPN is not carefully planned, designed, and configured, vulnerabilities may occur that impair all the IT systems connected to it. Attackers will thus be able to access confidential information of the corresponding organisation.

For example, inadequate VPN planning can mean that users have not been properly trained. They could thus use a VPN in an insecure environment or connect to one from insecure clients. This in turn may enable attackers to access the respective organisation's entire network.

Attacks may also be detected too late if regular checks of VPN access have not been inadequately planned. It will thus not be possible to respond in time, and an attacker may steal data or sabotage entire processes without being detected.

2.2. Insecure VPN Service Providers

If an organisation uses a VPN service provider that was not selected carefully, it could threaten the security of the organisation's entire network. The service provider's VPN access may not be secure, for example, and could thus be used by attackers to steal specific information.

2.3. Insecure Configuration of VPN Clients for Remote Access

If a VPN client is configured insecurely, users may utilise its security mechanisms incorrectly (or not at all). They could also change the configuration of the VPN client. Due to insecure configuration, software installed by users may also threaten the security of the VPN client.

2.4. Insecure Default Settings on VPN Components

In their default setting, VPN components are usually preconfigured with insufficient security mechanisms (or none at all). In many cases, the manufacturers pay more attention to user-friendliness and problem-free integration into existing systems than they do to security. If VPN components are insufficiently adapted to the actual security requirements of a given organisation, this will create vulnerabilities and corresponding points of attack. If, for example, passwords preset by a manufacturer are not changed, an entire VPN (and thus the internal network of the corresponding organisation) could be attacked.

3. Requirements

The specific requirements of module NET.3.3 *VPN* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief

Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	IT Operation Department
Further responsibilities	

3.1. Basic Requirements

For module NET.3.3 *VPN*, the following requirements MUST be met as a matter of priority:

NET.3.3.A1 Planning the Use of VPNs (B)

The introduction of a VPN MUST be planned carefully. The responsibilities for operating the VPN MUST be defined. User groups and their authorisations MUST also be planned for the VPN. Moreover, it MUST be defined how access authorisations that are granted, changed, or withdrawn are to be documented.

NET.3.3.A2 Selection of an Appropriate VPN Service Provider (B)

If a VPN service provider is to be used, service level agreements (SLAs) MUST be negotiated and documented in writing. The VPN service provider's compliance with the agreed SLAs MUST be checked regularly.

NET.3.3.A3 Secure Installation of VPN End Devices (B)

If an appliance that requires maintenance is used, this MUST be subject to a valid maintenance contract. It MUST be ensured that VPN components are only installed by qualified personnel. The installation of VPN components and any deviations from the planning specifications at hand SHOULD be documented. The functions and the selected security mechanisms of a VPN MUST be checked before it is put into operation.

NET.3.3.A4 Secure Configuration of a VPN (B)

Secure configurations MUST be established for all VPN components. This SHOULD be documented in a suitable manner. The administrator in charge MUST check regularly that these configurations are still secure and adapt them to all the IT systems at hand (if applicable).

NET.3.3.A5 Blocking Unneeded VPN Accounts (B)

It MUST be checked regularly that only authorised IT systems and users can access a given VPN. VPN access that is no longer required MUST be disabled promptly. VPN access MUST be limited to the usage time required.

3.2. Standard Requirements

For module NET.3.3 *VPN*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

NET.3.3.A6 Analysis of VPN Requirements (S)

A requirements analysis SHOULD be performed to determine the usage scenarios for a given VPN and use them as a basis for deriving the specifications that the corresponding hardware and software components will need to fulfil. The requirements analysis SHOULD take into consideration the following:

- business processes and specialised tasks
- access routes
- identification and authentication procedures
- users and user authorisations
- responsibilities
- reporting channels

NET.3.3.A7 Planning the Technical VPN Implementation (S)

In addition to the general planning required (see NET.3.3.A1 *Planning the Use of VPNs*), the technical aspects of a VPN SHOULD be planned carefully. Encryption methods, VPN end points, permitted access protocols, services, and resources SHOULD be specified for the VPN. Furthermore, the sub-networks that can be accessed via VPN SHOULD be defined. (See NET.1.1 *Network Architecture and Design*.)

NET.3.3.A8 Drawing Up a Security Policy for VPN Usage (S)

A security policy SHOULD be created for VPN usage. All the relevant employees SHOULD be made aware of this policy. The security safeguards described in the security policy SHOULD be explained through related training. If VPN access is set up for an employee, they SHOULD be issued an information sheet detailing the most important VPN security mechanisms. All VPN users SHOULD be obligated to comply with the security policy.

NET.3.3.A9 Selection of Suitable VPN Products (S)

When selecting VPN products, an organisation SHOULD consider its requirements regarding the networking of different locations and the connections of mobile employees and teleworkers.

NET.3.3.A10 Secure Operation of a VPN (S)

An operational concept SHOULD be created for VPNs. This SHOULD include the aspects of quality management, monitoring, maintenance, training, and authorisation.

NET.3.3.A11 Secure Integration of an External Network (S)

It SHOULD be ensured that VPN connections are ONLY created between the intended IT systems and services. The tunnel protocols used for this SHOULD be suitable for such use.

NET.3.3.A12 User and Access Management for Remote Access VPNs (S)

In cases involving remote access VPNs, central and consistent user and access management SHOULD be ensured.

NET.3.3.A13 Integration of VPN Components into a Firewall (S)

VPN components SHOULD be integrated into a firewall. This SHOULD be documented.

3.3. Requirements in Case of Increased Protection Needs

No requirements with increased protection needs are defined for module NET.3.3 *VPN*.

4. Additional Information

4.1. Useful Resources

The BSI has published the advanced document “Virtuelles Privates Netz (ISi-VPN): BSI-Leitlinie zur Internet Sicherheit (ISi-L)” [Virtual Private Network (ISi-VPN): BSI Guideline on Internet Security (ISi-L)” on the topic of VPNs.

The International Organization for Standardization (ISO) provides guidelines for the use of VPNs in the standard ISO/IEC 27033-5:2013, “Information Technology – Security Techniques – Network Security – Part 5: Securing Communications Across Networks Using Virtual Private Networks (VPNs)”.

The National Institute of Standards and Technology (NIST) provides general guidelines for the use of VPNs in Special Publication 800-77, “Guide to IPsec VPNs”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.3.3 *VPN*.

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.32 Misuse of Authorisation

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.46 Loss of Integrity of Sensitive Information

NET.4.1 Telecommunications Systems

1. Description

1.1. Introduction

Using a telecommunication system (also known as a PBX system), an organisation's telephones can be connected internally and to an external public telephone network. Due to the increasing integration of IT and telecommunications, PBX systems can be both analogue and IP-based. Hybrid systems, meanwhile, combine a classic telecommunications solution with a VoIP system. With a hybrid system, conventional digital or analogue telephony and VoIP can be used simultaneously.

Along with voice telephony, additional services may be used depending on the end devices connected. For example, PBX systems can be used to transmit data, texts, graphics, and moving images. The information can be forwarded in an analogue or digital manner using wired or wireless transmission media. Depending on the connection and the data networks used, a wide variety of PBX systems can be used in an organisation.

1.2. Objective

This module examines the threats and requirements that apply specifically to PBX systems and the corresponding parts of hybrid systems. The aim of the module is to protect the information that is transmitted via PBX systems, as well as the systems themselves from external intervention and manipulation.

1.3. Scoping and Modelling

Module NET.4.1 *Telecommunications Systems* must be applied to every telecommunication system.

This module deals with the hazards and requirements that are specific to PBX systems and the corresponding parts of a hybrid system. Topics that go beyond the scope of PBX systems—such as hazards and requirements for individual VoIP implementations, as well as externally

provided services—are covered in the specific corresponding modules of the IT-Grundschutz Compendium.

The security aspects of VoIP components and voice transmission via VoIP are described in more detail in module NET.4.2 *VoIP*.

PBX systems should also be considered as a matter of principle when implementing the modules ORP.4 *Identity and Access Management*, OPS.1.2.5 *Remote Maintenance*, CON.3 *Backup Concept,* and OPS.1.1.5 *Logging*.

2. Threat Landscape

For module NET.4.1 *Telecommunications Systems*, the following specific threats and vulnerabilities are of particular importance.

2.1. Eavesdropping on Telecommunications Systems

If telephone calls or data are transmitted in an unencrypted form via a PBX system, there is a general risk of attackers eavesdropping on or reading the information. For example, they could tap directly into the telephone cables or eavesdrop on a PBX system when it connects callers.

In many PBX systems, callers can leave a message for a recipient who is not available for a call. Some answering machines, especially those in VoIP systems, send this information in the form of an audio file attached to an e-mail. The contents of such e-mails could be directly intercepted and heard by an attacker.

In addition, it is possible for third parties to listen in on calls by activating disabled features, some of which are not allowed in Germany. Silent monitoring is one example of this. Activation of such features does require more detailed knowledge of the target system, but this is not a serious obstacle due to the large amount of information freely available on the Internet.

2.2. Eavesdropping on Rooms using Telecommunications Systems

As a matter of principle, it is possible to eavesdrop on rooms using microphones in end devices. A distinction is made between two variants here:

The first involves end devices that can be prompted to activate their built-in microphones from the public network or via LAN if corresponding functions are implemented. A well-known example of this is the “baby monitor” function available in some phones or answering machines.

The second variant involves misuse of the “voice calling” feature in combination with the “handsfree” option. This combination can cause the target system to operate like an intercom system under certain circumstances, which makes it possible to eavesdrop on a room.

2.3. Call Charge Fraud

Call charge fraud in connection with data or telecommunication services involves transferring the cost of telephone calls or data transfers to a third party. A PBX system can be manipulated in various ways from the outside. On the one hand, attackers can try to abuse existing features for call charge fraud. These features include, for example, remotely reprogrammable call forwarding or dial-in options. On the other hand, rights can be granted in such a way that incoming outside lines occupy outgoing outside lines. In this way, the caller can be automatically reconnected to the exchange from the outside when dialling a specific number—but at the expense of the PBX operator.

Along with external attackers, employees within an organisation can also be involved in call charge fraud. For example, they can try to make calls at the expense of their employer or other employees, such as by making calls from other people's devices, obtaining other people's authorisation codes (passwords), or changing personal authorisations.

2.4. Abuse of Freely Accessible Telephone Extensions

Telephones are often used without being assigned to a specific user. Some of these telephones, such as those found in printer rooms, can only be accessed by a limited group of people. However, telephones are often found in areas accessible to visitors. These include parking garages or areas near the entrances to access control systems. If these telephones have an electronic telephone book containing internal telephone numbers, these numbers could be exposed to outsiders.

3. Requirements

The specific requirements of module NET.4.1 *Telecommunications Systems* are listed below. As a matter of principle, the Process Owner is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Process Owner
Further responsibilities	IT Operation Department, Supervisor

3.1. Basic Requirements

For module NET.4.1 *Telecommunications Systems*, the following requirements MUST be met as a matter of priority:

NET.4.1.A1 Requirements Analysis and Planning for Telecommunications Systems [IT Operation Department] (B)

Prior to the procurement or expansion of a PBX system, a requirements analysis MUST be carried out. This analysis MUST determine the functions the PBX system should offer. In addition to the features of the PBX system, the number of required connections and ports MUST also be determined. Possible expandability and basic security functions MUST also be considered during planning. In addition, support and maintenance contracts for the PBX system MUST be taken into account as required. Based on the requirements determined, the use of the PBX system MUST then be planned and documented. The requirements identified and the plans devised MUST be coordinated with the corresponding persons responsible for IT.

NET.4.1.A2 Selection of Telecommunications Service Providers [IT Operation Department] (B)

In order to be able to make calls to persons who are not connected to a given organisation's own PBX system, a PBX service provider MUST be contracted. The requirements for the PBX system, the relevant security policy, and contractual and financial aspects MUST be taken into account. All services agreed MUST be specified clearly and concisely in writing.

NET.4.1.A3 ELIMINATED (B)

This requirement has been eliminated.

NET.4.1.A4 ELIMINATED (B)

This requirement has been eliminated.

NET.4.1.A5 Logging for Telecommunications Systems (B)

Suitable data MUST be recorded for PBX systems and evaluated as required. Additionally, all evaluation procedures, data transmissions, data access, and system-related interventions that involve program modifications MUST be logged. All administration work on PBX systems MUST also be logged. The logged information SHOULD be checked regularly.

3.2. Standard Requirements

For module NET.4.1 *Telecommunications Systems*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

NET.4.1.A6 Creating a Security Policy for Telecommunications Systems [IT Operation Department] (S)

Organisations SHOULD create a specific security policy for their PBX systems based on their general security policies. PBX security policies SHOULD include basic statements about confidentiality, availability, and integrity. All persons and groups involved in the procurement, design, implementation, and operation of PBX systems SHOULD be familiar with the security policy for PBX systems and use it as the basis for their work. The central security requirements for a given PBX system and the security level to be achieved SHOULD be included in the respective organisation's general security policy.

NET.4.1.A7 Suitable Installation of the Telecommunications System (S)

A PBX system SHOULD be located in a suitable room. The interfaces on the PBX, especially those that are unused, SHOULD be suitably protected.

NET.4.1.A8 Limitation and Blocking of Unnecessary or Security-Critical Features (S)

The scope of available features SHOULD be limited to the necessary minimum. Only the features needed SHOULD be activated. The features not required or deemed critical due to their potential for misuse SHOULD be disabled on the central system to the greatest extent possible. Additional protective safeguards SHOULD be implemented for the confidential data stored on or retrievable from the end devices in use.

NET.4.1.A9 Training on the Secure Use of Telecommunications Systems [Supervisor] (S)

Users of PBX systems SHOULD be instructed in the correct use of related services and devices. Users of PBX systems SHOULD be provided with all the required documents regarding the operation of corresponding end devices. Any anomalies and abnormal behaviour of PBX systems SHOULD be reported to the relevant person in charge.

NET.4.1.A10 Documentation and Revision of the Telecommunications System Configuration [IT Operation Department] (S)

The configurations of PBX systems SHOULD be suitably documented and updated. Such configurations MUST be evaluated at regular intervals. The results of the evaluation SHOULD at least be presented to the Chief Information Security Officer, the Process Owner, and other specifically appointed persons.

NET.4.1.A11 Decommissioning Telecommunications Systems and Devices [IT Operation Department] (S)

The disposal of PBX systems and connected PBX devices SHOULD be considered in an organisation's general security policy. All the data stored on PBX systems or devices SHOULD be securely erased before disposal.

NET.4.1.A12 Backup of Configuration Files (S)

The configuration and application data of PBX systems SHOULD be backed up during their initial setup and then on a regular basis, particularly after modifications. Whether the backups of PBX systems can actually be used as a basis for system recovery SHOULD be regularly checked and documented.

A backup concept SHOULD be drawn up for PBX systems and coordinated with an organisation's general data protection concepts for servers and network components.

NET.4.1.A13 Acquisition of Telecommunications Systems (S)

The results of requirements analysis and planning SHOULD be factored into the procurement of PBX systems. When procuring a PBX system, the need for both digital and analogue subscriber connections SHOULD be considered. Furthermore, existing communication systems and components SHOULD be taken into account in the procurement process.

NET.4.1.A14 Contingency Planning for Telecommunication Systems (S)

A contingency plan SHOULD be drawn up for PBX systems. This SHOULD be integrated in an organisation's contingency concept. Regular emergency drills SHOULD be carried out for PBX systems.

NET.4.1.A15 Emergency Calls in the Event of a Telecommunications System Failure (S)

It SHOULD be ensured that emergency calls can be made from a given organisation even in the event of a PBX system failure. The emergency call facilities SHOULD be accessible and sufficiently close to all rooms.

NET.4.1.A16 Securing End Devices in Openly Accessible Rooms (S)

The range of functions of end devices set up in openly accessible rooms SHOULD be restricted. If this is not possible, end devices SHOULD be protected against unauthorised access in a suitable manner.

NET.4.1.A17 Maintenance of Telecommunications Systems (S)

Devices for maintaining and configuring PBX systems SHOULD be secured with passwords or PINs.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.4.1 *Telecommunications Systems* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

NET.4.1.A18 Increased Access Protection (H)

A PBX system SHOULD be located in a separate and suitably secured room. Site and system access to PBX systems SHOULD be restricted to a specific group of people. External staff SHOULD ONLY be able to access PBX systems with supervision.

NET.4.1.A19 Redundant Connections (H)

PBX system connections SHOULD be redundant. An additional PSTN connection SHOULD be available for IP-based PBX systems.

4. Additional Information

4.1. Useful resources

As part of its technical guideline series, the BSI has published “BSI-TL-02013 für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf” [BSI-TL-02013, Technical Guideline for Internal Telecommunications Systems with Increased Protection Requirements].

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.4.1 *Telecommunications Systems*.

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.42 Social Engineering

NET.4.2 VoIP

1. Description

1.1. Introduction

Voice over IP (VoIP) refers to telephony over data networks, in particular over the Internet. Special signalling protocols are used to transmit signalling information, such as when making a call. The actual payload, such as voice or video data, is transmitted with the aid of a media transport protocol. Both protocols are required to establish and maintain a multimedia connection. Some procedures use only one protocol for signalling and transporting media.

1.2. Objective

This module examines the security aspects of VoIP end devices and switching units (middleware). The functionality of the components described here is the same as for the telecommunication components described in module NET 4.1 *Telecommunication Systems*.

1.3. Scoping and Modelling

Module NET.4.2 *VoIP* must be applied to all communication networks that use VoIP. Since VoIP operates over a data network, the requirements of the modules NET.1.1 *Network Architecture and Design* or NET.3.2 *Firewall* must be taken into account in addition to this module.

This module examines the security aspects of VoIP components and voice transmission via VoIP. It also applies to situations in which circuit-switching telecommunications systems exchange information using a data network.

The specific threats and requirements of classic PBX systems and hybrid systems are considered in module NET 4.1 *Telecommunications Systems*.

VoIP software is often operated on standard IT systems rather than dedicated hardware. If softphones are installed on clients, the requirements of module SYS.2.1 *General Client* and the operating-system-specific modules should be taken into account. If software for VoIP is operated on servers, the requirements of module SYS.1.1 General Server should be met in addition to the requirements of the operating-system-specific modules.

VoIP should always be included as part of the modules ORP.4 *Identity and Access Management*, OPS.1.1.3 *Patch and Change Management*, OPS.1.1.5 *Logging*, and OPS.1.1.2 *Proper IT Administration*.

2. Threat Landscape

For module NET.4.2 *VoIP*, the following specific threats and vulnerabilities are of particular importance.

2.1. Incorrect Configuration of VoIP Middleware

A VoIP-based telephone system can be affected by faulty configurations in the same manner as a circuit-switching telephone solution. Telephone users could be assigned incorrect telephone numbers, for example, or the entire telephone infrastructure could fail. Even minor errors, such as a name spelled incorrectly in the telephone book, cannot be ruled out.

When VoIP is used for communication, several IT systems are usually involved. If SIP is used as the initialisation protocol, systems such as *registrars*, *SIP proxy servers*, and *location servers* are usually required for communication. If the VoIP infrastructure at hand changes, all the related IT systems must be adapted. This can easily lead to configuration errors. Even when all services are located on one server, they often need to be configured individually. An incorrect change made to just one system could render the entire telephone infrastructure unusable.

2.2. Incorrect Configuration of VoIP Components

Regardless of whether its components come in the form of dedicated hardware (appliances) or software-based systems, configuration is crucial for the error-free functioning of a VoIP system. In addition to the signalling settings specified during the planning phase, the transmission method plays an important role in media streams. Applying a compression method can reduce the size of the data packets that contain voice information.

Errors in the configuration of the transmission method can lead to transmission problems. If an unsuitable method is used and voice information is compressed too much, the voice quality often deteriorates. If, however, a method that does not compress the data enough is selected, the stream of information will not be adequately reduced and the data network can become overloaded.

2.3. Eavesdropping on Telephone Calls

If telephone calls or data are transmitted in an unencrypted form, there is a general risk of attackers eavesdropping on or reading the information. For example, they could tap directly into the telephone cables or eavesdrop on a PBX system when it connects callers. With VoIP, it is even easier to eavesdrop on telephone calls and data transmissions than with classic PBX systems. All the voice data is transmitted in a media stream—using the Real-time Transport Protocol (RTP), for example. In the case of VoIP, techniques such as spoofing and sniffing enable attackers to use all types of incursions that pertain to data networks, as well.

In many PBX systems, callers can leave a message for recipients who are not available at the time of the call. Some answering machines, especially those in VoIP systems, send this information in the form of an audio file attached to an e-mail. The contents of such e-mails could be directly intercepted and heard by an attacker.

2.4. Abuse of Freely Accessible Telephone Extensions

Telephones are often used without being assigned to a specific user. Some of these telephones, such as those found in printer rooms, can only be accessed by a limited group of people. However, telephones are often found in areas accessible to visitors. These include parking garages or areas near the entrances to access control systems. If these telephones have an electronic telephone book containing internal telephone numbers, these numbers could be exposed to outsiders.

When VoIP telephones are used in freely accessible areas, additional aspects can be relevant. These telephones consist primarily of software and are often operated in data networks that are also used for other IT applications. An attacker could therefore attempt to exploit vulnerabilities in the VoIP software or install malware through direct access to device information.

VoIP telephones need to be connected to a data network. An attacker could connect a mobile IT system to this network and access it under some circumstances, even if it is protected from the outside by a firewall. They could then exploit this access to initiate attacks on confidentiality, integrity, and availability.

3. Requirements

The specific requirements of module NET.4.2 *VoIP* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	User

3.1. Basic Requirements

For module NET.4.2 *VoIP*, the following requirements MUST be met as a matter of priority:

NET.4.2.A1 Planning the Use of VoIP (B)

The conditions required for the use of VoIP MUST be specified. Among other things, it MUST be decided whether to switch completely or partially to VoIP. Special requirements for the availability of VoIP or the confidentiality and integrity of telephone calls or signalling

information SHOULD be determined in advance. Suitable signalling and media transport protocols MUST be selected prior to use.

It SHOULD be decided whether and how VoIP infrastructure should be connected to public (data) networks. The capacities and design of existing data networks SHOULD be taken into account during planning.

NET.4.2.A2 ELIMINATED (B)

This requirement has been eliminated.

NET.4.2.A3 Secure Administration and Configuration of VoIP End Devices (B)

End device functions that are not required MUST be disabled. The corresponding configuration settings MUST NOT be changed without authorisation. All end-device security functions SHOULD be tested prior to productive use. The security mechanisms and parameters used SHOULD be documented.

NET.4.2.A4 Restricting Accessibility via VoIP (B)

A decision MUST be taken as to how external callers will be able to access VoIP architecture. IT systems from insecure networks MUST be prevented from establishing direct data connections to an organisation's VoIP components. If all incoming and outgoing connections are to be handled via a central IT system, it SHOULD be ensured that all signalling and voice information between the public and private data networks in question is only exchanged via this authorised IT system.

NET.4.2.A5 Secure Configuration of VoIP Middleware (B)

VoIP components MUST be configured to satisfy the protection needs at hand in a suitable manner. The default configurations of VoIP middleware MUST be adapted before it is put into productive operation. All installation and configuration steps SHOULD be documented such that the installation and configuration can be understood and repeated by a qualified third party based on the documentation. All the services of VoIP middleware that are not required MUST be disabled.

NET.4.2.A6 ELIMINATED (B)

This requirement has been eliminated.

3.2. Standard Requirements

For module NET.4.2 *VoIP*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

NET.4.2.A7 Drawing up a Security Policy for VoIP (S)

The central security requirements for VoIP and the security level to be achieved SHOULD be included in an organisation-wide security policy. This security policy SHOULD detail all the general security-related requirements of the organisation in question. In addition, the policy SHOULD regulate the requirements for the operation and use of VoIP components. The

different VoIP functions, such as voicemail, SHOULD be considered in this regard. The VoIP security policy SHOULD be available and known by all the persons and groups involved.

NET.4.2.A8 Encryption of VoIP (S)

A decision SHOULD be taken as to whether and which voice and signalling information should be encrypted. In general, all VoIP data packets leaving a secure LAN SHOULD be protected by suitable security mechanisms. Users SHOULD be informed about the use of VoIP encryption.

NET.4.2.A9 Selection of Suitable VoIP Components (S)

Before VoIP components are purchased, a requirements list SHOULD be created. The list of requirements SHOULD be used to evaluate the products available on the market. The requirements list SHOULD include all the characteristics necessary to achieve the desired security level. The manner in which the products available on the market can be evaluated according to the requirements list SHOULD be regulated.

NET.4.2.A10 ELIMINATED (S)

This requirement has been eliminated.

NET.4.2.A11 Secure Handling of VoIP End Devices [User] (S)

Users of VoIP end devices SHOULD be aware of the basic VoIP threats and security safeguards. In addition, they SHOULD select suitable passwords to secure voicemails.

NET.4.2.A12 Secure Decommissioning of VoIP Components (S)

When VoIP components are decommissioned or replaced, all security-related information SHOULD be deleted from the devices. After data is deleted, it SHOULD be verified that the data was deleted successfully. Confidential information SHOULD also be deleted from backup media. All labels, especially on end devices, SHOULD be removed before disposal. Safeguards for deleting security-related information which are compatible with the applicable conditions of contracts and guarantees SHOULD be clarified in advance with manufacturers, retailers, or service providers.

NET.4.2.A13 Firewall Requirements When Using VoIP (S)

Organisations SHOULD check whether their firewalls can be adapted for the use of VoIP. If this is not the case, an additional firewall SHOULD be purchased and installed.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.4.2 *VoIP* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

NET.4.2.A14 Encryption of Signalling (H)

The integrity and confidentiality of signalling information SHOULD be ensured by appropriate cryptographic procedures. Along with the actual payloads, authentication data SHOULD also be continuously encrypted. Access to VoIP gateways SHOULD be restricted to the greatest possible extent with the help of VoIP addresses and H.323 identities. Additional

end-to-end security mechanisms SHOULD be used for media transport and signalling. The way in which signalling is protected SHOULD be documented.

NET.4.2.A15 Secure Media Transport Using SRTP (H)

For transmissions using the Real-Time Transport Protocol (RTP), media data and information for controlling such data SHOULD be appropriately protected. The user data SHOULD be protected by the use of Secure Real-Time Transport Protocol (SRTP) and Secure Real-Time Control Protocol (SRTCP). The security-relevant options for implementing the protocols SHOULD be documented.

NET.4.2.A16 Network Separation for Data and VoIP (H)

VoIP networks SHOULD be separated from data networks in a suitable manner. The way in which devices that need to access VoIP and data networks are to be dealt with SHOULD be regulated. VoIP end devices in a VoIP network SHOULD ONLY be able to establish the intended VoIP connections to other IT systems.

4. Additional Information

4.1. Useful Resources

As part of its technical guideline series, the BSI has published "BSI-TL-02013 für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf" [BSI-TL-02013, Technical Guideline for Internal Telecommunications Systems with Increased Protection Requirements].

As part of its series of special publications, the National Institute of Standards and Technology (NIST) has published NIST Special Publication 800-5, “Security Considerations for Voice Over IP Systems”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.4.2 *VoIP*.

G 0.9 Failure or Disruption of Communication Networks

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.40 Denial of Service

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

NET.4.3 Fax Machines and Fax Servers

1. Description

1.1. Introduction

This module examines the security aspects of information transmission via standard fax machines and fax servers. The information transmitted is referred to as a fax (short for telefax) or, more rarely, as a telecopy or facsimile. With a conventional fax machine, the contents of a document are scanned point by point by the transmitting machine and then sent to a recipient. The receiver device reconstructs the contents point by point and usually outputs it directly on paper.

A fax server, on the other hand, is a service that is installed on a server to enable other IT systems in its data network to send and receive faxes. Fax servers are often integrated into existing e-mail or groupware systems. It is therefore possible for incoming fax documents to be delivered to users by e-mail. Outgoing documents are relayed to the fax server either via a printer queue system or by e-mail. A document is usually sent and received as an image file between the fax server and clients in a data network. The transmitted image file cannot be processed directly in text processing systems. Optical character recognition (OCR) is usually required for this first. Documents received and processed by a fax server can usually be easily archived—for example, by the fax server service itself, by document management systems, or by groupware directly connected to the fax server service.

1.2. Objective

One aim of this module is to protect information transmitted and processed by fax. Another objective is to protect fax machines and fax servers against manipulation by unauthorised persons. Since the transmission medium used is irrelevant to the application of this module, the requirements of this module should also be implemented for fax over IP (FoIP).

1.3. Scoping and Modelling

Module NET.4.3 *Fax Machines and Fax Servers* must be applied to every fax machine and fax server in the information domain under consideration.

This module considers standard stand-alone fax machines and fax servers as the technical basis for sending faxes. Additional aspects of fax machines that can be found in a multifunction (or all-in-one) device are dealt with separately in module SYS.4.1 *Printers, Copiers, and All-in-One Devices*. To protect the information that is processed, offered, stored and transmitted on fax servers, module SYS.1.1 General Server and the respective operating-system-specific modules should be considered. Information on correct archiving can be found in module OPS.1.2.2 *Archiving*.

2. Threat Landscape

For module NET.4.3 *Fax Machines and Fax Servers*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inadequate or Incorrect Supply of Consumables

Fax machines receive documents and usually print them directly on paper. The smooth and uninterrupted operation of a fax machine requires the availability of consumer goods such as paper and toner in sufficient quantities. If these are not available, fax documents often cannot be received. In addition, transmission confirmations (which may be mandatory) cannot be printed out.

2.2. Fax Transmission Errors

Many different forms of interference can occur between the sender and recipient of a fax during transmission. This can result in the fax documents to be transmitted being incomplete or illegible or not arriving at the recipient at all. Decisions based on this information may be inappropriate, which can result in significant losses or damage.

Delays that occur because problems have to be identified and documents need to be resent can lead to further complications. The transmitter or receiver usually has no way of influencing the transmission path and thus has to wait until the interference has been rectified by a third party. In many cases, the sender even believes that a faxed document has been properly transmitted to the desired addressee and the resulting problems are only detected some time later.

In addition, it cannot be ruled out that a fax document may have been transmitted to the wrong recipient machine due to a faulty connection in the public telecommunications network, for example. Wrong numbers may also be dialled on fax machines, or the direct dial keys may have been incorrectly programmed. If a fax server is used, fax numbers may also have been entered or stored incorrectly in the address book. As a result, confidential information may be sent to unauthorised persons.

2.3. Manipulation of Address Books and Distribution Lists

Fax machines often have address books and distribution lists. If a fax server is used, the corresponding groupware usually makes it possible to keep similar address books and distribution lists in a central location where they can be accessed by several users. Recipient numbers can be stored in address books so they do not have to be re-entered each time a fax is sent. It is also possible to create a group of recipients using distribution lists and thus send faxes to several people at the same time.

Once programmed, recipient numbers or distribution lists are often no longer checked when a fax document is to be sent. If an unauthorised person changes the address books or distribution lists on a fax machine or in its groupware, confidential information may be sent to the wrong recipients. It is also possible that the intended recipients may not receive urgently needed information. For example, a fax number could be exchanged in the address book, or another recipient could be added to the distribution list without this ever being detected by the person in charge at the organisation in question.

2.4. Unauthorised Reading of Incoming Fax Transmissions

In almost all cases, it is most economical for several users to share a fax machine. Such machines are therefore usually set up in rooms that can be accessed by all the employees of an organisation, such as printer rooms. As the fax machines are freely accessible, all employees can read the received faxes and thus access potentially confidential information.

2.5. Evaluation of Residual Information in Fax Machines

Depending on the technical procedure that fax machines use to store, further process, or print information, they may contain varying amounts of residual information after sending or receiving a fax. Unauthorised persons who come into possession of a fax machine or corresponding components may be able to recover this information.

Fax transmissions are stored on the hard drive of a fax server at least until they can be delivered to a recipient. Moreover, state-of-the-art operating systems use swap files that may also contain residual information. This information could be used without permission if a fax server is accessed.

2.6. Impersonation of a False Sender on Fax Machines

Fax transmissions are a popular medium for transmitting documents that are only valid with a signature. In the same way that a false sender can be faked with a misleading name and letterhead, a fax transmission can also be manipulated. For example, signatures from other documents can be scanned and copied onto a fax document. Generally speaking, it is almost impossible to recognise the difference between a real signature and a reproduced graphic file. A recipient who considers the information contained therein to be authentic or even legally binding can suffer related losses as a result.

3. Requirements

The specific requirements of module NET.4.3 *Fax Machines and Fax Servers* are listed below. As a matter of principle, the Process Owner is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Responsible as a matter of principle	Process Owner
Further responsibilities	User, Procurement Department, IT Operation Department, Building Services

3.1. Basic Requirements

For module NET.4.3 *Fax Machines and Fax Servers*, the following requirements MUST be met as a matter of priority:

NET.4.3.A1 Suitable Siting of a Fax Machine [Building Services] (B)

Fax machines MUST be installed in such a way that received faxes cannot be viewed or removed by unauthorised persons. The installation site SHOULD also be selected to ensure that an adequate number of telephone communication lines or channels are available. An installation site MUST have a suitable network connection for the fax machine in question. Fax machines MUST NOT be used with network connections that were not intended for this purpose.

NET.4.3.A2 Information for Employees on Using Fax Machines (B)

All employees MUST be made aware of the specifics of transmitting information by fax. They MUST also be informed that fax transmissions are only legally binding to a very limited extent. An instruction manual that is easy to understand MUST be available at every fax machine. Users SHOULD receive at least a brief tutorial on the fax client software used by a fax server. In addition, instructions on correct fax usage MUST be displayed.

NET.4.3.A3 Secure Operation of a Fax Server [IT Operation Department] (B)

Before a fax server is put into operation, a test phase SHOULD be carried out. The configuration parameters and all the changes made to the fax server's configuration SHOULD be documented. The archiving and deletion of fax data SHOULD be regulated. In addition, the functionality of the connection from the fax server to the corresponding PBX system or the public telephone network MUST be checked regularly. It MUST also be ensured that the fax server only offers fax services and is not used for any other purposes. All features and communication interface access points that are not required MUST be disabled.

3.2. Standard Requirements

For module NET.4.3 *Fax Machines and Fax Servers*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

NET.4.3.A4 Drawing Up a Security Policy for Fax Use (S)

A security policy for fax use SHOULD be created before a corresponding device is used. It SHOULD detail the intended type of use. In addition, the way in which incoming and outgoing faxes are to be dealt with SHOULD be regulated. A regulation on the handling of undeliverable faxes SHOULD also be drawn up. The security policy for fax use SHOULD also contain information and instructions regarding contingency planning and fallback options for fax operations.

NET.4.3.A5 ELIMINATED (S)

This requirement has been eliminated.

NET.4.3.A6 Procurement of Suitable Fax Machines and Servers [Procurement Department] (S)

A requirements list SHOULD be created before fax machines and fax servers are purchased. The systems or components under consideration SHOULD be assessed using this list. The requirements list for fax machines SHOULD also include security-relevant aspects such as the exchange of subscriber IDs, the output of transmission reports, error logging, and journal management. In addition, appropriate additional security functions SHOULD be considered based on the protection needs at hand.

When selecting a fax server, the requirements to be met by the respective IT system—including the operating system, communications components, and application software—SHOULD be specified and taken into consideration. The option of integrating a fax server into an existing data network and groupware system SHOULD be considered if necessary.

NET.4.3.A7 Suitable Labelling of Outgoing Fax Transmissions [User] (S)

The sender and the desired recipient SHOULD be visible on all outgoing faxes. If this information cannot be obtained from the document sent, a standardised fax cover sheet SHOULD be used. In general, a fax cover sheet SHOULD include at least the name of the organisation of the sender, the name of the contact person, the date, the number of pages, and an indication of how urgent the fax is. It SHOULD also include the name and organisation of the recipient. If necessary, the fax cover page SHOULD be customised for each outgoing fax.

NET.4.3.A8 Appropriate Disposal of Consumable Fax Accessories and Spare Parts (S)

All fax consumables from which information on sent and received fax messages might be retrieved SHOULD be made unreadable before disposal or disposed of by a reliable specialised company. The same procedure SHOULD also be followed for replaced parts that contain information. Maintenance companies that check or repair fax machines SHOULD be required to handle them appropriately in this regard. Regular checks SHOULD be carried out to determine whether these guidelines are being followed.

NET.4.3.A9 Using Transmission and Reception Logs (S)

The transmission processes of incoming and outgoing faxes SHOULD be logged. The communication journals available on standard fax machines SHOULD be used for this purpose. If fax machines have logging functions, they SHOULD be activated. Logging SHOULD also be activated for fax servers. A decision SHOULD be taken regarding the information that should be logged.

The communication journals and log files of fax machines SHOULD be regularly evaluated and archived. They SHOULD undergo random inspections for irregularities. Unauthorised persons SHOULD not be able to access these communication journals or logged information.

NET.4.3.A10 Control of Programmable Destination Addresses, Logs, and Distribution Lists (S)

Programmable speed-dial keys and saved destination addresses SHOULD be checked regularly to see if the desired numbers match the respective programmed numbers. Fax numbers that are no longer required SHOULD be deleted. Appropriate documentation SHOULD be created when a new entry is added or a recipient number is changed.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.4.3 *Fax Machines and Fax Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

NET.4.3.A11 Preventing Fax Machine Overload [IT Operation Department] (H)

Sufficient communication lines or channels SHOULD be available. The expected fax volume SHOULD be estimated for a fax server. Components which are capable of handling this volume SHOULD be selected. Logs of fax servers SHOULD be checked regularly in order to prevent bottlenecks caused by overloads in good time. Fax data that is no longer required SHOULD be promptly deleted from fax servers.

NET.4.3.A12 Blocking Specific Recipient and Sender Fax Numbers (H)

Undesired fax addresses SHOULD be blocked. Alternatively, only specified numbers SHOULD be allowed. The appropriate approach SHOULD be determined for each individual situation.

NET.4.3.A13 Designating Authorised Fax Operators [User] (H)

Access to a fax machine SHOULD be restricted to a small number of employees. These employees SHOULD distribute incoming faxes to the recipients. The employees SHOULD be taught how to use the fax machine and how to implement the necessary security safeguards. Every authorised user SHOULD be informed about who may operate the fax machine and who is in charge of it.

NET.4.3.A14 Producing Copies of Incoming Fax Messages [User] (H)

Faxes printed on thermal paper that are needed for a longer period SHOULD be copied or scanned onto plain paper. It SHOULD be taken into account that the ink on thermal paper

fades faster and becomes unreadable. Copies or scanned faxes SHOULD be archived appropriately.

NET.4.3.A15 Announcing and Acknowledging Fax Messages [User] (H)

Important faxes SHOULD be announced to the recipient before they are sent. The documents to be announced in advance SHOULD be specified. Employees who wish to send confidential fax documents SHOULD be instructed to have the recipient confirm full receipt. For important or unusual faxes, the recipient SHOULD have the sender confirm that the fax document came from them and has not been falsified. A suitable form of communication (telephone, for example) SHOULD be selected to announce or confirm fax documents.

4. Additional Information

4.1. Useful Resources

No further information is available for module NET.4.3 *Fax Machines and Fax Servers*.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module NET.4.3 *Fax Machines and Fax Servers*.

G 0.2 Unfavourable Climatic Conditions

G 0.4 Pollution, Dust, Corrosion

G 0.8 Failure or Disruption of the Power Supply

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.27 Lack of Resources

G 0.31 Incorrect Use or Administration of Devices and Systems

INF.1 Generic Building

1. Description

1.1. Introduction

A building encompasses all the stationary workstations and installed information technology on the premises, as well as the information processed there. It thus ensures protection against external influences. This is why both the building itself (i.e. walls, ceilings, floors, roof, windows, and doors) and all the infrastructure facilities and utilities it contains (such as electricity, water, gas, heating, and cooling) should be considered.

This module is based on an example in which a building is used by one or more units of an organisation. These units may have differing security requirements. Furthermore, all related considerations must include the fact that almost every building is also entered by persons not belonging to the respective organisation, such as citizens, customers, or suppliers. If a building is used by various parties, its design and equipment must match the building's usage concept. An optimal environment should be ensured for the persons working there. Unauthorised persons should not be allowed access to areas where they could compromise security. It should also be possible to operate the technology installed in the building safely and efficiently.

1.2. Objective

This module describes the requirements to be met in order to ensure optimal protection of a building in terms of information security. The safeguards resulting from the requirements depend on the type and size of both the organisation and the building in question. Requirements from this module may also be applied to large properties including several buildings, or to the use of individual sections of buildings used by multiple entities.

1.3. Scoping and Modelling

Module INF.1 *Generic Building* must be applied once to each building.

This module considers technical and non-technical security aspects of the planning and use of typical buildings designed for companies and public authorities. This includes consideration of

the entire lifecycle of buildings from the perspective of information security—from the creation of a requirements catalogue to conceptual design, furnishings, building usage, alterations, and eventual departure.

The cabling in a building is examined separately in module INF.12 *Cabling*, and special rooms such as server rooms or archive rooms are examined in the corresponding modules of the INF *Infrastructure* layer.

The topic of working with third-party personnel is covered in module ORP.1 *Organisation*.

2. Threat Landscape

For module INF.1 *Generic Building*, the following specific threats and vulnerabilities are of particular importance:

2.1. Fire

Buildings and facilities can be severely damaged by fire and people can be injured or killed. Along with damage caused directly by a fire, subsequent damage must also be considered. It usually takes weeks or even months to put areas damaged by fire back into operation. Toxic smoke from a fire also poses a very great danger: most personal injuries due to a fire are caused by smoke inhalation. Smoke can cause serious damage to facilities and IT systems, as well.

Burning PVC generates chlorine gases that form hydrochloric acid when they come into contact with moist air and extinguishing water. If the resulting hydrochloric acid vapours are spread through the air conditioning system, sensitive electronic devices located in a part of the building far from the site of the fire may also be damaged.

2.2. Lightning

If there is a storm, lightning is the greatest danger to buildings and IT. A lightning strike can release current strengths of up to 200,000 amperes at voltages up to several hundred thousand volts. This enormous amount of electrical energy is released and dissipated within 50 to 100 microseconds. A lightning strike of this magnitude at a distance of approximately two kilometres will still cause voltage spikes in the electrical cables of a building that could destroy sensitive electronic devices. The risk of this indirect damage increases the closer a building is to the lightning.

If a building is struck directly by lightning, major damage can be caused by the dynamic energy released. This may affect the roof and façade, for example, and subsequent fires or surges can also damage electrical devices.

2.3. Water

Water can damage a building and its facilities from the outside as a result of rain, high water, or flooding, for example, or from the inside due to things like defects in water pipes.

2.4. Natural Hazards and Disasters

Depending on their location, buildings are exposed to different degrees of risks with regard to natural hazards and disasters. The causes of natural disasters may include seismic, climatic, or volcanic phenomena such as earthquakes, flooding, landslides, tsunamis, avalanches, and volcanic eruptions. Examples of extreme meteorological phenomena include thunderstorms, hurricanes, or torrential rain.

2.5. Threats in the Vicinity

Buildings can also be damaged by events in the immediate vicinity, such as leaks of toxic substances. Rescue efforts, road closures, or evacuations may also restrict the use of a building.

2.6. Unauthorised Site Access

If unauthorised persons are able to access a building or individual rooms therein, this poses a variety of further threats. Unauthorised persons may cause damage through deliberate acts such as theft or manipulation of information or IT systems or components, but also through unintentional misconduct (e.g. due to a lack of expertise).

In this context, less obvious manipulations can cause far greater damage than direct acts of destruction. Property damage can also result from the very act of unauthorised intrusion, such as when windows and doors are forced open and damaged in the process. Repairing or replacing them usually takes financial resources and time, during which their protective function is limited or non-existent.

2.7. Violation of Laws or Regulations

When a building is constructed, there are many laws and regulations that must be observed, such as those relating to fire protection or other aspects of structural safety. If these laws are violated, this may not be noticed for a long time, but it can have catastrophic consequences—for example, if firestop seals are not installed as intended.

2.8. Insufficient Fire Protection

Every building in which IT is operated is criss-crossed by a multitude of cables and pipes, such as fresh water and waste water pipes, heating pipes, or lines for supplying energy or transmitting data. It is impossible to prevent these pipe and cable trays from crossing ceilings and firewalls. If suitable firestop seals are not installed at such locations, fire and smoke may spread uncontrollably through them.

The highly dynamic nature of IT makes the continued re-routing of cables necessary, even across firestop seals. How this can be done correctly depends directly on a building's existing fire protection, which means the possible solutions can vary a great deal. If modifications to a firestop seal are not carried out according to the specifications of the respective manufacturer, it can fail in the event of a fire. The fire could then spread to areas that should actually be protected by the seal.

2.9. Failure of the Power Supply

In the event of a power failure, entire buildings or parts of them may be rendered useless. Not only obvious, direct power consumers such as IT or lighting depend on the power supply; all the infrastructural equipment used today depends directly or indirectly on electrical power. That includes lifts, air conditioning systems, alarm systems, security gates, automatic door locking units, sprinkler systems, and private branch exchanges for telephones. Even the water supply on floors above or below ground is dependent on electricity due to the necessary pumps.

3. Requirements

The specific requirements of module INF.1 *Generic Building* are listed below. As a matter of principle, Building Services is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Building Services
Further responsibilities	Employee, Planner, Construction Company, Central Administration, Construction Manager, Building Services, Top Management

3.1. Basic Requirements

For module INF.1 Generic Building, the following requirements MUST be met as a matter of priority:

INF.1.A1 Planning the Building Protection [Planner] (B)

The protection for a building MUST be defined based on the (planned) use of a building and the protection needs of the business processes operated within it. In particular, security aspects regarding the protection of persons, commodities, and IT in the building MUST be taken into consideration, from fire prevention and electrical aspects to site access control. The security requirements from different areas MUST be coordinated.

INF.1.A2 Appropriate Segmentation of Circuits (B)

Regular checks MUST be carried out to ensure that the protection and design of a building's circuits still meet the actual requirements at hand.

INF.1.A3 Compliance with Fire Prevention Regulations (B)

The current fire prevention regulations and the requirements imposed by the building inspectors MUST be met. The escape routes MUST be marked in accordance with the respective regulations and kept unobstructed. Regular checks MUST be carried out to determine whether the escape routes are usable and not blocked by any obstacles so that the

building in question can be evacuated quickly in the event of a dangerous situation. The local fire department SHOULD be consulted when fire prevention plans are being developed. An IT-related fire prevention concept MUST be drawn up and implemented.

Unnecessary fire loads MUST be avoided.

Organisations MUST have a Fire Safety Officer or another person who is assigned the tasks involved. This person MUST be suitably trained.

INF.1.A4 Fire Detection in Buildings [Planner] (B)

Buildings MUST be equipped with a sufficient number of smoke detectors in accordance with the requirements in their construction permits and fire protection concepts. If a local alert at the location of each detector is not sufficient, all detectors MUST be connected to a fire alarm control panel (FACP). If smoke is detected a building, an alarm MUST be triggered. Everyone in the building MUST be able to hear it. The functioning of all smoke detectors and all other components of a fire alarm system MUST be checked regularly.

INF.1.A5 Hand-Held Fire Extinguishers (B)

A sufficient number of suitably dimensioned hand-held fire extinguishers with the fire class required for the situation at hand (based on DIN EN 3, "Portable Fire Extinguishers") MUST be available for immediate firefighting measures. These hand-held fire extinguishers MUST be inspected and serviced regularly. Employees SHOULD be instructed in the use of the hand-held fire extinguishers. This instruction SHOULD be repeated at appropriate intervals.

INF.1.A6 Closed Windows and Doors [Employee] (B)

Windows and doors accessible from the outside, such as from balconies or terraces, MUST be closed when a room is not occupied. Rooms MUST be locked if confidential information is left there. Corresponding instructions MUST be issued in this regard. All employees SHOULD be required to comply with the instructions. Regular checks MUST be carried out to ensure that windows and internal and external doors are locked after leaving a building. Fire and smoke doors MUST NOT be kept open for extended periods of time unless approved hold-open systems are used.

INF.1.A7 Site Access Regulations and Control [Central Administration] (B)

Access to areas of sensitive buildings and rooms MUST be governed by a policy and controlled. There SHOULD be a concept for site access control. The number of persons with site access authorisation SHOULD be reduced to the bare minimum for every area. Additional persons MUST not gain access until a corresponding need is confirmed. The site access authorisations granted SHOULD be documented. The site access control safeguards MUST be checked regularly for effectiveness.

Site access controls SHOULD also remain in place as far as possible during relocations.

INF.1.A8 Smoking Ban (B)

Smoking MUST be prohibited in rooms where fires or contamination could cause considerable damage, such as server rooms or storage media and document archives. Regular checks MUST be carried out to ensure that site access protection is not circumvented when smoking areas are designated or tolerated.

INF.1.A10 Compliance with Relevant Standards and Regulations [Construction Company, Construction Manager] (B)

When planning, erecting, and converting buildings and installing technical equipment, all the relevant standards and regulations MUST be taken into consideration.

3.2. Standard Requirements

For module INF.1 *Generic Building*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

INF.1.A9 Security Concept for Building Use [Planner] (S)

There SHOULD be a security concept for a building's use. The security concept for the building SHOULD be adapted to the overall security concept of the respective organisation. It SHOULD be documented and updated at regular intervals.

Sensitive rooms or building areas SHOULD NOT be located in highly exposed or particularly hazardous areas.

INF.1.A11 ELIMINATED (S)

This requirement has been eliminated.

INF.1.A12 Key Management (S)

There SHOULD be a lock-up plan for all keys to a given building. The manufacture, storage, management, and issue of keys SHOULD be organised in a centralised manner. Backup keys SHOULD be available and secured, but kept on hand for emergencies. Keys that have not been issued SHOULD be stored securely. Every key issued SHOULD be documented.

INF.1.A13 Regulations Governing Access to Distributors (S)

Rapid access to the distributors of all supply facilities within a building SHOULD be possible if and when required. Access to distributors SHOULD be restricted to a small group of authorised persons.

INF.1.A14 Lightning Protection Devices (S)

A lightning protection system SHOULD be installed according to the applicable standard. A comprehensive lightning and surge protection concept SHOULD be in place. At minimum, buildings with comprehensive IT equipment SHOULD be equipped with lightning protection devices of protection class II according to DIN EN 62305, “Lightning Protection”. The lightning protection system SHOULD be inspected and serviced regularly.

INF.1.A15 Plans Detailing the Location of Supply Lines (S)

Up-to-date layout plans of all supply lines SHOULD be available for a given building. It SHOULD be specified who is responsible for maintaining and updating the layout plans of all supply lines. The plans SHOULD be stored in such a way that only authorised persons may access them, but they must be quickly accessible in case of need.

INF.1.A16 Avoiding References to the Locations of Sensitive Building Areas (S)

References to the locations of sensitive areas SHOULD be avoided. Sensitive areas of buildings SHOULD not be easily visible from the outside.

INF.1.A17 Structural Smoke Protection [Planner] (S)

A building's structural smoke protection SHOULD be checked after installation and conversion work. Regular checks SHOULD be carried out to ensure that smoke protection components are still functioning.

INF.1.A18 On-Site Fire Safety Inspections (S)

On-site fire safety inspections SHOULD take place regularly, i.e. at least once or twice a year. Deficiencies identified during on-site fire safety inspections SHOULD be rectified immediately.

INF.1.A19 Notification of the Fire Safety Officer (S)

The Fire Safety Officer SHOULD be informed of work being performed on cable trays, hallways, and escape and rescue routes. They SHOULD check that fire safety measures are being implemented properly.

INF.1.A20 Alert Plan and Fire Drills (S)

An alert plan for the measures to be taken in case of a fire SHOULD be drawn up. The alert plan SHOULD be reviewed and updated at regular intervals. Fire drills SHOULD be performed at regular intervals.

INF.1.A27 Burglary Protection (S)

Adequate safeguards for burglary protection SHOULD be implemented and adapted to the local conditions at hand. Care SHOULD be taken during the planning, implementation, and operation of burglary protection to ensure that it is consistent, including in terms of its quality. It SHOULD be regularly inspected by a person with corresponding expertise. Employees SHOULD be aware of the regulations for burglary protection.

INF.1.A36 Regular Documentation Updates (S)

The documentation on a building (e.g. construction plans, route plans, wiring diagrams, escape route plans, fire department route maps) SHOULD always be kept up to date. It SHOULD be checked that all the relevant plans are still up to date and correct at least once every three years. Employees SHOULD be informed of any changes.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.1 *Generic Building* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

INF.1.A21 ELIMINATED (H)

This requirement has been eliminated.

INF.1.A22 Secure Doors and Windows (H)

Doors and windows SHOULD be selected on the basis of the protection objectives of the area to be secured, the protection needs of the organisation in question, and the appropriate classification in line with the relevant standards. All the safeguarding measures meant to secure the windows, doors, and walls enclosing a given space SHOULD be appropriate and of equal quality with regard to burglary, fire and smoke. The proper functioning of safety doors and windows SHOULD be checked regularly.

INF.1.A23 Formation of Security Zones [Planner] (H)

Rooms with similar protection needs SHOULD be consolidated into zones in order to treat comparable risks in a uniform way and reduce the costs of required security safeguards.

INF.1.A24 Automatic Drainage (H)

All areas at risk of water damage SHOULD be equipped with an automatic drainage system. Regular checks SHOULD be performed to ensure that active and passive drainage systems still function.

INF.1.A25 Selection of Appropriate Locations [Top Management] (A)

When selecting or planning a building location, the environmental conditions that could influence information security SHOULD be checked. There SHOULD be an overview of the location-related threats at hand. These threats SHOULD be addressed by means of additional compensating safeguards.

INF.1.A26 Gatekeeper or Security Service (H)

The tasks of a gatekeeper or security service SHOULD be clearly documented. The gatekeeper SHOULD observe and monitor all movements of persons at the gate and at all other entrances in line with the respective organisation's security concept. All employees and visitors SHOULD be able to identify themselves to the gatekeepers. Visitors SHOULD be escorted to the person to be visited or collected from the entrance. The gatekeepers SHOULD be promptly informed of any changes in site access authorisations.

INF.1.A28 ELIMINATED (H)

This requirement has been eliminated.

INF.1.A29 ELIMINATED (H)

This requirement has been eliminated.

INF.1.A30 Selection of an Appropriate Building (H)

When selecting an appropriate building, it SHOULD be checked whether all the security requirements relevant for later use can be implemented. For every building, the existing threats and the safeguards required to prevent or reduce damage SHOULD be documented in advance.

INF.1.A31 Moving Out of Buildings [Central Administration] (H)

Before moving out of a building, an organisation SHOULD draw up an inventory of all items relevant to information security for the move, such as hardware, software, storage media, files,

or documents. Once the move is complete, all rooms SHOULD be checked for items left behind.

INF.1.A32 Firestop Seal Register (H)

A firestop seal register SHOULD be maintained. This SHOULD record all the individual types of such partitions. After work is performed on firestop seals, the changes SHOULD be entered into the register within four weeks.

INF.1.A33 ELIMINATED (H)

This requirement has been eliminated.

INF.1.A34 Intruder and Fire Detection System (H)

There SHOULD be an intruder and fire detection system appropriate for the rooms and risks at hand. The intruder and fire detection system SHOULD be inspected and serviced regularly. It MUST be ensured that the recipients of intrusion and fire detection alerts are capable of responding appropriately from both a technical and personnel-related perspective.

INF.1.A35 Perimeter Protection [Planner, Building Services] (H)

Depending on the protection needs and terrain at hand, a building SHOULD have perimeter protection. At minimum, the following components SHOULD be considered in terms of their usefulness and feasibility:

- a wall or fence around the property
- security safeguards against accidental trespassing (crossing the property line)
- security safeguards against deliberate trespassing without the use of force
- safeguards to impede the deliberate crossing of the property line through force
- open-air security safeguards
- person and vehicle detection
- safeguards for preserving evidence (e.g. video recording)
- automatic alerts

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for the physical and environmental security of buildings in annex A.11 of ISO/IEC 27001:2013.

In "The Standard of Good Practice for Information Security", the Information Security Forum (ISF) provides guidelines for the physical and environmental security of buildings in section CF19.

The National Institute of Standards and Technology (NIST) has published NIST Special Publication 800-53, “Assessing Security and Privacy Controls for Federal Information Systems

and Organizations", which provides specifications on the physical and environmental security of buildings in appendix F-PS.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module INF.1 *Generic Building*.

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.3 Water

G 0.4 Pollution, Dust, Corrosion

G 0.5 Natural Disasters

G 0.6 Catastrophes in the Vicinity

G 0.7 Major Events in the Vicinity

G 0.8 Failure or Disruption of the Power Supply

G 0.10 Failure or Disruption of Supply Networks

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.29 Violation of Laws or Regulations

G 0.34 Assault

G 0.44 Unauthorised Entry to Premises

INF.2 Data Centre and Server Room

1. Description

1.1. Introduction

Today, almost all strategic and operative functions and tasks are substantially supported by (if not entirely dependent on) information technology. As a consequence, the requirements for the performance and availability of IT systems and their network connections are constantly increasing. To meet these performance requirements, ensure that adequate reserve capacity is available, and operate IT in economical ways, organisations of all sizes concentrate their IT landscapes in data centres.

A data centre is defined as follows:

- If an organisation that uses IT has only one central area of IT operations, this, together with the required support areas, must generally always be treated as a data centre in terms of its protection needs. The term “area of IT operations” refers to rooms in which hardware is installed and operated to provide services and data. In addition to its area of IT operations, a data centre comprises all other technical support areas (e.g. power supply, cold air supply, extinguishing technology, security technology) that facilitate the correct operation and security of the area of IT operations.
- If an organisation’s IT operations are distributed over several areas within a building or a given premises and these areas are connected both to one another and to IT users by internal LAN connections, the most functionally significant of these areas (at minimum) must be treated as a data centre. In addition, areas in which proper operations are crucial for 50% or more of the users at hand or from which 50% or more of the services and data (proportionate to all areas) are provided must be treated as a data centre.
- If an organisation that uses IT is located at several physically separate sites and these are connected to each other by means other than internal LAN connections, each of the sites must be considered and treated separately according to (1) above.
- An area of IT operations that houses IT required for critical business processes (i.e. processes whose disruption or failure would significantly impair the fulfilment of an organisation’s primary tasks) must always be treated as a data centre, independent of the size or the proportion specified in (2) above.

- Areas of IT operations from which services for third parties are performed must always be treated as part of a data centre. Here, it is irrelevant whether these services are subject to fees.
- If there is a justifiable interest in treating an area of IT operations (together with its support areas) as a server room contrary to the above regulations, reasons must be provided for the resulting reduction of security requirements.

An area does not need to fulfil all six of the points listed here to be considered a data centre. The list merely describes different scenarios in which an area is to be considered a data centre. If an area of IT operations deviates from these definitions, it is referred to as a server room. This designation is solely based on how significant the IT structure in question is to the respective organisation's ability to fulfil its tasks, and thus corresponds to the methodology specified in DIN EN 50600.

If a server room is to be protected, the requirements in this module can be reduced accordingly. However, substantial and comprehensible reasons must be given for this in accordance with (6) above and the Basic Requirements must be implemented at minimum.

1.2. Objective

On the one hand, this module is directed towards organisations that operate a data centre and want to check if suitable security safeguards have been implemented in the framework of an audit. On the other, the module can also be used to estimate the security safeguards that will need to be implemented if IT is to be centralised in a data centre. The primary goal of the requirements described in this module is to ensure the secure operation of data centres.

1.3. Scoping and Modelling

INF.2 *Data Centre and Server Room* must be applied to every data centre and every server room.

It is not suitable for small information domains with, for example, only one or a very small number of servers or IT systems. This might involve a small organisation with a few IT workstations and a server that is located in a separate room, for example. In such cases, it is often sufficient to implement module INF.5 *Room or Cabinet for Technical Infrastructure*.

General requirements for buildings and cabling are also not part of this module. These can be found in the modules INF.1 *Generic Building* and INF.12 *Cabling*.

To make this module easier to understand, technical details and planning variables have deliberately been avoided. The relevant standards and other BSI publications provide more detailed information.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module INF.2 *Data Centre and Server Room*, the following specific threats and vulnerabilities are of particular importance.

2.1. Incorrect Planning

If protection against Elementary Threats is not taken into account when designing a data centre, there is a very high risk of failure. For example, site risks such as air traffic, earthquakes, or flooding may threaten operational security and availability. Massive impacts on the operation of a data centre are also possible if the available bandwidth or the energy supply at the selected site is insufficient due to incorrect conceptional design.

2.2. Insufficient Site Access Controls

If the corresponding site access controls are insufficient, there is an increased risk that unauthorised persons may enter a data centre and cause unintentional (e.g. due to a lack of technical knowledge) or intentional damage. Attackers may thus extract sensitive data, steal devices, or manipulate servers, for example. Insufficient site access controls can therefore impact the availability, confidentiality, and integrity of data and IT components.

2.3. Insufficient Monitoring

If the IT and infrastructure operated at data centre is insufficiently monitored and supported, components may fail without anyone noticing. This may seriously impair the data centre's availability and proper functionality. In many cases, failures also occur gradually over a longer period of time. Without active monitoring, they may be noticed too late. At that point, it is often no longer possible to react in time.

2.4. Insufficient Air Conditioning in a Data Centre

IT components require specific operating conditions in order to function reliably. They also convert the electrical power they absorb into additional heat. If the temperature, humidity, or dust content of the air in an IT operating area is not kept within the limits specified by the equipment manufacturers, this can cause technical components to function improperly or fail entirely.

2.5. Fire

Fire is not a common threat. When a fire does occur, however, it usually has serious consequences. This is because fire and smoke can cause major damage. While electrical fires are the most common cause of fire within IT operations areas, a fire outside of an IT operations area— especially in support areas involving the power supply (including EPS and UPS) or the air conditioning system—can have numerous other causes. If an IT operations area, its support areas, or other neighbouring areas have inadequate fire protection, a fire can spread quickly. In addition, fires that start outside could spread to a data centre.

2.6. Water

Water can enter a data centre due to leaking or burst water pipes, floods, or defective sprinkler or air conditioning systems. This can damage equipment and cause it to stop working. A short circuit can also be triggered, which could cause individual areas of a data centre to fail or catch fire.

2.7. Insufficient Burglary Protection

Even if a well-functioning access control system is in place, unauthorised persons can enter a data centre if it is not adequately protected against intrusion. Offenders could then steal or manipulate IT components or obtain confidential information. They could also destroy devices or cause general damage to the data centre.

2.8. Failure of the Power Supply

If a power failure occurs, the operations of a data centre (and thus the entire surrounding organisation) can be significantly disrupted. In the event of a power failure, the IT services provided by a data centre will suddenly no longer be available. Data can also be lost. In addition, it is possible that IT systems, telecommunication systems, or monitoring technology may be damaged by a sudden power failure.

2.9. Contamination

Dust and other contamination in a data centre can cause technical components (e.g. fans) to stop working. Contamination also causes equipment to wear out earlier and fail more often.

3. Requirements

The specific requirements of module INF.2 *Data Centre and Server Room* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	IT Operation Department
Further responsibilities	Employee, Planner, Data Protection Officer, Building Services, Maintenance Personnel

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

INF.2.A1 Defining Requirements [Building Services, Planner] (B)

Adequate technical and organisational requirements MUST be defined and implemented for a data centre.

When planning a data centre or choosing suitable rooms, appropriate security safeguards MUST also be planned that take the protection needs of the IT components (especially regarding their availability) into account.

A data centre as a whole MUST be designed as a closed security area. In addition, it MUST have different security zones. For example, administration, logistics, and IT operations and support areas MUST be clearly separated from each other. In the case of a server room, it SHOULD be checked whether it is possible to implement different security zones.

INF.2.A2 Formation of Fire Zones [Planner] (B)

Suitable fire and smoke zones MUST be defined for the rooms of a data centre. The fire and smoke zones MUST also provide protection that goes beyond the scope prescribed by building law for the technical equipment located therein and its availability. Fire and smoke MUST be prevented from spreading. In the case of a server room, it SHOULD be checked whether adequate fire and zones can be implemented.

INF.2.A3 Use of an Uninterruptible Power Supply [Building Services] (B)

An uninterruptible power supply (UPS) MUST be installed for all the operationally relevant components of a data centre. As the power consumption of air conditioning is often too high for a UPS, the control of these systems MUST at least be connected to the UPS. In the case of a server room, the necessity of operating a UPS SHOULD be checked based on the availability requirements of the IT systems at hand.

The UPS MUST have sufficient capacity. If there are relevant changes in loads, checks MUST be carried out to establish whether the capacity of the existing UPS systems is still sufficient.

In UPS systems that use a battery for energy storage, the battery MUST be kept within the required temperature range. For this purpose, it SHOULD be kept away from the power electronics of the UPS if possible. The UPS MUST be serviced and checked for functionality at regular intervals. The maintenance schedule specified by the manufacturer MUST be followed for this purpose.

INF.2.A4 Emergency Shutdown of the Power Supply [Building Services] (B)

There MUST be suitable options for switching off the electrical consumers in a data centre. Attention MUST be paid to whether and how an existing UPS is spatially and functionally integrated into the power supply. If conventional emergency stop switches are used, it MUST be ensured that the entire data centre will not be switched off. The emergency shutdown system MUST be subdivided in a systematic and sensible manner. All emergency off switches MUST be protected such that they cannot be activated unintentionally or without authorisation.

INF.2.A5 Maintenance of Air Temperature and Humidity [Building Services] (B)

It MUST be ensured that the air temperature and humidity in an IT operating area will remain within the prescribed limits. The actual thermal load in cooled areas MUST be checked at regular intervals and after major conversions.

Any air conditioning systems in use MUST be maintained regularly. At minimum, temperature and humidity parameters MUST be recorded in a way that makes it possible to retrospectively identify whether thresholds have been exceeded as a means of both pinpointing and eliminating the cause of any deviation.

INF.2.A6 Site Access Control [Building Services] (B)

Access to a data centre MUST be controlled. Site access rights MUST be assigned in accordance with the specifications of module ORP.4 *Identity and Access Management*. It MUST be ensured that those who work at a data centre do not have access to IT systems outside their scope of work.

All the possible ways to access a data centre MUST be equipped with site access control devices. Each instance in which a person accesses a data centre MUST be individually recorded by a site access control system. In the case of a server room, it SHOULD be checked whether it is appropriate to monitor all the possible ways to access the site in question.

Regular checks MUST be carried out to determine whether the regulations regarding the use of site access controls are being observed.

An organisation's requirements regarding its site access control system MUST be documented in a concept with a sufficient level of detail.

INF.2.A7 Locking and Securing Facilities [Employee, Building Services] (B)

All the doors of a data centre MUST always be kept locked. Windows MUST be avoided in the planning stage whenever possible. If there are windows, they MUST always be kept locked. Doors and windows MUST provide protection adequate for the security level at hand against attacks and external influences. They MUST have privacy screens. Consideration MUST be given to the structural design of all room-forming elements and their ability to provide a uniform level of protection.

INF.2.A8 Use of a Fire Alarm System [Planner] (B)

A fire alarm system MUST be installed in a data centre. It MUST monitor all areas. All the alarms of the fire alarm system MUST be forwarded appropriately (see also INF.2.A13 *Planning and Installation of Alarm Systems*). The fire alarm system MUST be serviced at regular intervals. It MUST be ensured that no particular fire loads are present in the rooms of a data centre.

INF.2.A9 Use of an Extinguishing or Fire Prevention System [Building Services] (B)

An extinguishing or fire prevention system in line with the current state of the art MUST be installed in a data centre. If this is not possible, technical (especially a wide-area early detection system; see INF.2.A17 *Early Fire Detection*) and organisational measures (trained personnel and response plans for early fire detection alarms) MUST ensure that early fire detection alarms are responded to immediately and within no more than three minutes.

In server rooms without an extinguishing or fire prevention system, hand-held fire extinguishers with suitable extinguishing agents MUST be available in sufficient number and size. Attention MUST be paid to the fact that these provisions do not affect any additional building code requirements regarding the provision of hand-held fire extinguishers. The fire

extinguishers MUST be mounted so that they are easy to access in case of a fire. Each fire extinguisher must be inspected and serviced regularly. All staff who are allowed to enter a data centre or server room MUST be instructed in the use of hand-held fire extinguishers.

INF.2.A10 Inspection and Maintenance of Infrastructure [Maintenance Personnel, Building Services] (B)

For all components of building services infrastructure, the intervals and requirements for inspection and maintenance recommended by the respective manufacturers or specified by corresponding standards MUST be observed at minimum. Inspections and maintenance work MUST be documented. Firestop seals MUST be checked to ensure that they are intact. The results MUST be documented.

INF.2.A11 Automatic Monitoring of Infrastructure [Building Services] (B)

All infrastructure facilities, including leakage monitoring, air conditioning, and power and UPS systems, MUST be automatically monitored. Detected disruptions MUST be reported and dealt with in an appropriate manner as quickly as possible.

In the case of a server room, IT and support devices that do not or only occasionally need to be operated by a person SHOULD be equipped with a remote means of indicating malfunctions. The responsible employees MUST be alerted promptly.

INF.2.A17 Use of Early Fire Detection [Planner, Building Services] (B)

A data centre MUST be equipped with an early fire detection system. A server room SHOULD be equipped with an early fire detection system. Early fire detection alarms MUST be routed to a continuously staffed department that can initiate a corresponding check and a protective response within three minutes. Alternatively, an automatic protective response MUST be initiated. In order to achieve a balance between fire protection and availability, it MUST be ensured that equipment providing redundancy is not located together within the effective range of the same voltage isolation circuit.

INF.2.A29 Avoidance and Monitoring of Unnecessary Wiring [Building Services, Planner] (B)

The cables laid in a data centre MUST be restricted to those that directly supply the technology installed there (usually IT and, if applicable, cooling technology). If structural reasons make it unavoidable to run lines through a data centre in order to supply areas other than those within the data centre, this MUST be documented along with suitable justification. The risks posed by such lines MUST be minimised by appropriate safeguards (e.g. enclosures and monitoring).

The aforementioned lines may be routed through server rooms without justifying why this is unavoidable, but they MUST be treated in the same way as described for data centres.

Messages from systems that monitor such lines MUST be checked and evaluated immediately to determine whether a threat is present. Countermeasures MUST be implemented in a timely manner according to the threat level identified (see also INF.2.A13 *Planning and Installation of Alarm Systems*).

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

INF.2.A12 Data Centre Perimeter Protection [Planner, Building Services] (S)

Perimeter protection SHOULD be in place for data centres. Depending on the protection needs defined for a given data centre and its premises, perimeter protection SHOULD consist of the following components:

- A wall or fence around the property
- Security safeguards against accidental trespassing (crossing the property line)
- Security safeguards against deliberate trespassing without the use of force
- Security safeguards against deliberate trespassing through the use of force
- Outdoor security safeguards
- Visual detection of people and vehicles
- Safeguards for preserving evidence (e.g. video recording)
- Automatic alerts

INF.2.A13 Planning and Installation of Alarm Systems [Building Services] (S)

The corresponding building's security concept SHOULD be used to plan which alarm systems are needed and should be installed for specific areas of a data centre. In addition, a procedure for dealing with alarm messages SHOULD be defined. The security concept SHOULD always be adapted if and when the use of the building's areas changes.

An alarm system that is fit for purpose SHOULD be installed. The notifications from the alarm system SHOULD be transmitted to an alarm receiving centre in compliance with the applicable technical connection requirements. The selected alarm receiving centre MUST be reachable at all times. It MUST be able to react appropriately to alarms in terms of its technology and personnel. The transmission path between the alarm system and the alarm receiving centre SHOULD be designed according to the technical connection requirements at hand and, if possible, with redundancy. All established transmission routes MUST be tested at regular intervals.

INF.2.A14 Use of an Emergency Power System [Planner, Building Services] (S)

The power supplied to a data centre from the grid of an energy utility company SHOULD be supplemented by an emergency power system (EPS). If an EPS is in place, it MUST be regularly maintained. Load and functional tests, as well as test runs under load, MUST be conducted when performing maintenance.

The operating supplies for an EPS MUST be checked regularly to see if they are sufficient. Regular checks MUST also be performed to ensure that these supplies are still usable, and especially to avoid "diesel bug". If possible, low-sulphur heating oil SHOULD be used instead of diesel fuel. Refuelling operations MUST be logged. The log MUST include the type of fuel, the additives used, the date of refuelling, and the quantity refuelled.

If an EPS is not used for a server room, a UPS with a run time appropriate for the protection needs at hand SHOULD be implemented as an alternative.

INF.2.A15 Overvoltage Protection Devices [Planner, Building Services] (S)

A lightning and overvoltage protection concept SHOULD be drawn up on the basis of the currently valid standard (DIN EN 62305 parts 1 to 4). The lightning protection zones (LPZ) required for the proper operation of a data centre must be defined. For all the facilities required for the proper operation of a data centre and its ability to provide services, this SHOULD be at least LPZ 2. All overvoltage protection equipment SHOULD be subject to a comprehensive test once a year in accordance with DIN EN 62305-3 (table E.2).

INF.2.A16 Air Conditioning in Data Centres [Planner] (S)

It SHOULD be ensured that suitable climatic conditions are established and maintained in a data centre. A data centre's air-conditioning system SHOULD have sufficient capacity. All the relevant values SHOULD be constantly monitored. If a value deviates from the norm, an automatic alarm SHOULD be triggered.

Air-conditioning systems SHOULD be as fail-safe as possible in areas of IT operations.

INF.2.A18 ELIMINATED (S)

This requirement has been eliminated.

INF.2.A19 Functional Testing of Technical Infrastructure [Building Services] (S)

The technical infrastructure of a data centre SHOULD be tested regularly (at least once or twice a year) and following system modifications and extensive repairs. The results SHOULD be documented. In particular, entire reaction chains SHOULD be subjected to a real function test.

INF.2.A20 ELIMINATED (S)

This requirement has been eliminated.

INF.2.A30 Systems for Extinguishing or Preventing Fires [Building Services, Planner] (S)

A data centre SHOULD be equipped with an automatic extinguishing or fire prevention system.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

INF.2.A21 Alternate Data Centre (H)

A geographically separate alternate data centre SHOULD be established. The alternate data centre SHOULD have sufficient capacity to maintain all of the corresponding organisation’s

processes. It SHOULD always be ready for operation, as well. All of the organisation's data SHOULD be mirrored to the alternate data centre on a regular basis. The procedure for switching to the emergency data centre SHOULD be tested and drilled regularly. The transmission routes to the alternate data centre SHOULD be suitably secured and designed with appropriate redundancy.

INF.2.A22 Implementation of Dust-Protection Measures [Building Services] (H)

During construction work in a data centre, suitable dust-protection measures SHOULD be defined, planned, and implemented. Persons who are not involved in the construction work themselves SHOULD check the dust-protection measures frequently to make sure they are working properly and the regulations on dust protection are being followed.

INF.2.A23 Appropriate Design of Data Centre Cabling [Building Services] (H)

Cable routes in data centres SHOULD be carefully planned and implemented. Cable trays in data centres SHOULD be carefully designed in terms of their arrangement and dimensioning so that separation of voltage levels and a sensible distribution of cables on the trays is possible, and that sufficient space is also available for future increases in demand. To ensure the optimal supply of IT hardware that has two power supply units, a two-line A-B supply SHOULD be set up from the low-voltage main distributor for the IT operating areas in question. Pairs of redundant lines SHOULD be laid in separate trays.

INF.2.A24 Use of Video Monitoring Systems [Data Protection Officer, Building Services, Planner] (H)

Site access control and intrusion detection systems SHOULD be supplemented by video monitoring systems. A video monitoring system SHOULD be integrated into the overall security concept at hand. The Data Protection Officer MUST always be involved in the planning, design, and potential evaluation of video recordings.

The central technical components required for a video monitoring system SHOULD be installed in a suitable environment and protected. The video monitoring system SHOULD be tested regularly to ensure its proper function and its compliance with the angles of view agreed with the Data Protection Officer.

INF.2.A25 Redundant Design of Uninterruptible Power Supplies [Planner] (H)

UPS systems SHOULD be modular and designed to have a redundant module compensate for any failure without interruption. If a two-line A-B supply is set up for IT operating areas, each of the two current paths SHOULD be equipped with an independent UPS system.

INF.2.A26 Redundant Design of Emergency Power Systems [Planner] (H)

Emergency power systems SHOULD be redundant. With regard to maintenance, a redundant EPS MUST also be treated according to INF.2.A14 *Use of an Emergency Power System*.

INF.2.A27 ELIMINATED (H)

This requirement has been eliminated.

INF.2.A28 Use of Higher-Level Alarm Systems [Planner] (H)

For areas of data centres with increased protection needs, VdS class-C alarm systems SHOULD be used exclusively (in line with VdS Guideline 2311).

4. Additional Information

4.1. Useful Resources

The BSI makes the documents “Redundanz Modularität Skalierbarkeit” [Redundancy, Modularity, Scalability] and “Kriterien für die Standortwahl von Rechenzentren” [Criteria for the Siting of Data Centres] available on its website.

The German Institute for Standardisation (DIN) describes general principles for the design of data centres in the standard DIN EN 50600-1:2019-08, "Information Technology – Data Centre Facilities and Infrastructures – Part 1: General Concepts”.

The German Institute for Standardisation (DIN) deals with the topic of lightning protection in the standard DIN EN 62305-4:2011-10, "Protection Against Lightning – Part 4: Electrical and Electronic Systems Within Structures”.

Germany's digital association, Bitkom, provides assistance in planning and setting up a data centre in its guide "Betriebssicheres Rechenzentrum” [Reliable Data Centre].

The German Insurance Association (GDV) describes perimeter security safeguards in the publication “Sicherungsleitfaden Perimeter” [Perimeter Security Guide], which can be used as an aid in securing properties.

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module INF.2 *Data Centre and Server Room*:

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.3 Water

G 0.4 Pollution, Dust, Corrosion

G 0.6 Catastrophes in the Vicinity

G 0.7 Major Events in the Vicinity

G 0.8 Failure or Disruption of the Power Supply

G 0.10 Failure or Disruption of Supply Networks

G 0.11 Failure or Disruption of Service Providers

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.34 Assault

G 0.41 Sabotage

G 0.44 Unauthorised Entry to Premises

INF.5 Room or Cabinet for Technical Infrastructure

1. Description

1.1. Introduction

A technical infrastructure room contains technical components that only rarely need to be operated directly on site. However, they are indispensable to building infrastructure, and thus also to IT infrastructure. This can include, for example, power supply distributors, fuse boxes, ventilation systems, telecommunications components, patch panels, switches, or routers. A technical infrastructure room is not a continuous workplace and is usually only entered or opened for maintenance.

If the technical infrastructure to be protected cannot be housed in a separate room or if the room cannot be set up according to the requirements described herein, the technical infrastructure can also be placed in a cabinet specially equipped for this purpose. This can also make sense if a cabinet is the most economical alternative for housing technical infrastructure. The requirements for such rooms should then be transferred as effectively as possible to the cabinet and its shell.

1.2. Objective

The objective of this module is to protect a room or cabinet for technical infrastructure structurally, mechanically, and electronically in terms of information security. In principle, a "room" in this context is a room or cabinet within a building, but it can also be a container outside a building or a tent housing technical infrastructure. A room's protective safeguards should be designed to prevent the functional impairment of the technical components located in it to the greatest possible extent.

In this module, only the term “room” will be used for technical infrastructure. However, the requirements of this module can also be applied to cabinets.

1.3. Scoping and Modelling

Module INF.5 *Room or Cabinet for Technical Infrastructure* must be applied to rooms that are used to operate technical infrastructure. The module must also be applied if stationary containers (in the sense of large cabinets) are operated.

As a rule, rooms for technical infrastructure contain only technical components that are typically not housed in a data centre itself (see module INF.2 *Data Centre and Server Room*). In contrast to server rooms, they only contain IT systems that provide IT services in justified exceptional cases. One such exception relates to small information domains with, for example, only one or a very small number of servers or IT systems. This might apply to a small or medium-sized company with a small number of IT workstations and a server which is located in a separate room. In such cases, it is often sufficient to fulfil the requirements of this module instead of those detailed in module INF.2 *Data Centre and Server Room*. Requirements for cabling are dealt with in module INF.12 *Cabling*.

2. Threat Landscape

For module INF.5 *Room or Cabinet for Technical Infrastructure*, the following specific threats and vulnerabilities are of particular importance:

2.1. Incorrect Planning

Several problems can occur if a room for technical infrastructure is not planned correctly. Water may find its way in or IT components could overheat due to solar radiation if the location of a room is unsuitable. An unsuitable location may increase the likelihood of break-ins, as well. Bottlenecks can also occur if there the respective power supply is insufficient. If they were made using inferior materials, IT components are often more susceptible to failures and malfunctions. There is also the risk of rules and regulations not be considered and observed right from the planning stage. If unauthorised deviations have to be rectified later on, the costs may be unnecessarily high.

2.2. Unauthorised Site Access

If there is no site access control or burglary protection (or such safeguards are too weak), unauthorised persons may be able to enter a technical infrastructure room. They could cause damage there unintentionally (e.g. due to a lack of expertise) or intentionally (e.g. by stealing, replacing, manipulating, or destroying equipment).

2.3. Inadequate Ventilation

Inadequate ventilation in a room for technical infrastructure could result in the temperature range permitted for the installed equipment not being maintained. These devices could then fail or be forced to run continually.

2.4. Fire

A technical infrastructure room can be severely damaged or completely destroyed by a fire, causing the business processes or specialised tasks that depend on it to fail. There is a risk of fire in a room with power cables and power consumers. The circuit breakers or equipment fuses could fail to trip when the currents are too high, for example. On the other hand, negligence can also lead to fires: If people smoke in a technical infrastructure room, for instance, cables and devices made of combustible material could catch fire. In addition, sparks can be produced due to overvoltage or overheating, which can lead to a fire. A fire in a technical infrastructure room can also spread to other parts of the building. Conversely, a fire in a building can also spread to its technical infrastructure room.

2.5. Water

Flooding within a technical infrastructure room can cause water damage to both the components operated there and the room itself. Besides affecting the room, this water damage can also lead to short circuits in electrical equipment. Mould and corrosion can occur as a result. A leak in a water pipe could also flood a technical infrastructure room. Rainwater that enters the building during heavy rainfall via overloaded storm drains can also cause flooding.

2.6. Failure of the Power Supply

If the power supply fails in a technical infrastructure room, several components that run on electricity are usually affected. This can bring all the related operational processes to a halt. If the power supply is suddenly interrupted, this can also cause damage to electronic components, which can still have an impact after the power supply has been restored. Subsequent damage can also occur if an important component is not operational, such as a ventilation system. If a technical infrastructure room heats up, this can damage other devices or even cause them to fail.

2.7. Lightning and Overvoltages

In addition to the effects of a direct lightning strike, the induction effect of indirect lightning can also cause overvoltage peaks several hundred metres away from the point of impact. The induction can also have an impact in the vicinity of the down conductors of a lightning protection system. Under certain circumstances, these inductive overvoltage peaks can cause overvoltages on cable trays and on electronic devices within a technical infrastructure room, which can lead to functions being disrupted or devices failing completely.

2.8. Electromagnetic Interference Fields

Electromagnetic fields can be emitted from a source of interference, such as lift motors, transmitters, or the down conductors of lightning protection systems. These may interfere with switches, controllers, or IT systems. The interference voltage can cause electronic components to stop functioning reliably or even fail completely. The devices within a technical infrastructure room can also interfere with each other.

2.9. Electrostatic Discharge

Uncontrolled electrostatic discharges can damage or destroy equipment with sensitive electronic components in a technical infrastructure room. This can cause the equipment to stop functioning reliably or to fail completely.

3. Requirements

The specific requirements of module INF.5 *Room or Cabinet for Technical Infrastructure* are listed below. As a matter of principle, the Chief Information Security officer (CISO) is responsible for fulfilling the requirements. The CISO must also always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Employee, Planner, Building Services, Maintenance Personnel

3.1. Basic Requirements

For module INF.5 *Room or Cabinet for Technical Infrastructure*, the following requirements MUST be met as a matter of priority:

INF.5.A1 Planning the Room Protection [Planner] (B)

Adequate technical and organisational requirements MUST be defined and implemented for a room for technical infrastructure. The level of protection to be achieved for the room MUST be considered. Planning MUST take into account both legal rules and regulations and potential hazards related to environmental influences, intrusion, and sabotage.

INF.5.A2 Location and Size of the Technical Infrastructure Room [Planner] (B)

A technical infrastructure room MUST NOT be a passageway. It MUST be ensured that sufficient space is available for escape routes and the work activities planned.

INF.5.A3 Site Access Regulations and Control [Building Services, IT Operation Department] (B)

A technical infrastructure room MUST be protected against unauthorised access. There MUST be rules on who may enter the room, for which areas, for what purposes, and for how long. In this respect, it MUST be ensured that no unnecessary or excessive site access rights are granted. All instances in which a person accesses a technical infrastructure room SHOULD be individually recorded by a site access control system.

INF.5.A4 Protection Against Intrusion [Planner, Building Services] (B)

A technical infrastructure room MUST be protected against intrusion. Depending on the required security level of the room, suitable room-forming components SHOULD be selected, such as walls, ceilings, and floors, as well as windows and doors with appropriate resistance classifications in line with DIN EN 1627.

INF.5.A5 Avoidance of and Protection Against Electromagnetic Interference Fields [Planner] (B)

Electromagnetic fields MUST be avoided in the immediate vicinity of a technical infrastructure room. A sufficient distance to large machines such as lift motors MUST be maintained.

INF.5.A6 Minimising Fire Loads [Employee, Planner] (B)

Fire loads within and in the immediate vicinity of a technical infrastructure room MUST be minimised. Combustible materials MUST be avoided in room-forming components.

INF.5.A7 Prevention of Incorrect Use [Employee, Planner] (B)

A technical infrastructure room MUST NOT be used for other purposes (e.g. as a storeroom or cleaning cupboard).

INF.5.A9 Power Supply [Building Services] (B)

The power supply grid supplying a technical infrastructure room and the terminal equipment connected to it MUST be constructed as a TN-S system.

3.2. Standard Requirements

For module INF.5 Room or Cabinet for Technical Infrastructure, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

INF.5.A8 Avoidance of Uncontrolled Electrostatic Discharge [Planner] (S)

A dissipative floor covering SHOULD be installed in a technical infrastructure room in accordance with DIN EN 14041.

INF.5.A10 Maintenance of Air Temperature and Humidity [Building Services] (S)

It SHOULD be ensured that the air temperature and humidity in a room for technical infrastructure are within the limits specified on the data sheets of the equipment operated in the room. A suitable ventilation and air-conditioning system SHOULD be used for this purpose. This system SHOULD have sufficient capacity.

INF.5.A11 Avoidance of Pipes with Hazardous Liquids and Gases [Planner, Building Services] (S)

A room for technical infrastructure SHOULD only contain pipes that are absolutely necessary to operate the technology in the room. Sewage pipes, fresh water pipes, gas and heating pipes, and pipes for fuel or steam SHOULD NOT be routed through the space.

INF.5.A12 Protection Against Accidental Damage to Supply Lines [Planner] (S)

Supply lines outside a technical infrastructure room SHOULD be protected against accidental damage.

INF.5.A13 Protection Against Fire and Smoke Damage [Planner, Building Services] (S)

Irrespective of the building regulations pertaining to fire protection requirements that apply to a technical infrastructure room, all room-forming components, as well as doors and windows, SHOULD be equally smoke-tight. They SHOULD resist fire and smoke for at least 30 minutes. Fire loads in the vicinity of cable trays SHOULD be avoided.

INF.5.A14 Minimising Fire Hazards from Neighbouring Areas [Planner, Building Services] (S)

A technical infrastructure room SHOULD NOT be located in close proximity to other rooms with combustible materials in quantities exceeding typical office use.

INF.5.A15 Lightning and Overvoltage Protection [Planner, Building Services] (S)

A lightning and overvoltage protection concept should be developed and implemented in accordance with the principle of energetic coordination (see DIN EN 62305). A technical infrastructure room SHOULD be classified in accordance with lightning protection zone 2 (LPZ 2) at minimum. The lightning and overvoltage protection devices SHOULD be checked regularly to ensure they are fit for purpose and replaced if necessary.

INF.5.A16 Use of an Uninterruptible Power Supply [Building Services] (S)

The equipment that should be connected to a UPS SHOULD be checked. If a UPS is required, the backup time of the UPS SHOULD make it possible to shut down all the supplied components safely. Consideration SHOULD be given to the ageing of batteries in UPS systems.

If there are relevant changes, the capacity of existing UPS systems SHOULD be checked. UPS batteries SHOULD be kept within the required temperature range.

A UPS SHOULD be serviced and checked for functionality at regular intervals. For this purpose, the maintenance intervals provided by the manufacturer SHOULD be observed.

INF.5.A17 Inspection and Maintenance of Infrastructure [Building Services, IT Operation Department, Maintenance Personnel] (S)

At minimum, the recommended intervals and guidelines for inspection and maintenance recommended by the system manufacturer or those specified in standards SHOULD be followed for all components of physical and technical infrastructure. Cable and pipe penetrations through fire and smoke compartment boundary walls SHOULD be inspected to ensure that the partitions have the required approval for the purpose at hand and remain intact. Inspections and maintenance MUST be appropriately recorded.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.5 *Room or Cabinet for Technical Infrastructure* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

INF.5.A18 Location of the Technical Infrastructure Room [Planner] (B)

Within the respective building, a technical infrastructure room SHOULD be located in a place that is not exposed to internal or external hazards such as rain, water, or sewage. On floors above ground level, care SHOULD be taken to ensure that the room is not heated by solar radiation. If the room is located on the top floor of the building, care SHOULD be taken to ensure that water cannot enter through the roof.

INF.5.A19 Redundancy of the Technical Infrastructure Room [Planner] (H)

A technical infrastructure room SHOULD be designed redundantly. Both rooms SHOULD have a dedicated electrical sub-distribution that is directly supplied by the low-voltage main distribution panel (LVMDP). Both rooms SHOULD be assigned to different fire zones and, if necessary, have their own respective ventilation and air-conditioning systems.

INF.5.A20 Enhanced Protection Against Intrusion and Sabotage [Planner] (H)

A technical infrastructure room SHOULD be windowless. If there are windows, they SHOULD be adequately secured against intrusion from the outside depending on the storey of their location. If, in addition to windows and doors, there are other openings necessary for operations (such as ventilation ducts), these SHOULD have the same protection as the room envelope.

Intrusion detection systems SHOULD be used in line with VdS class C (according to VdS Guideline 2311). All required doors, windows, and other protected openings SHOULD be monitored via the intrusion system for closure, locking, and break-in. Any windows SHOULD always be closed.

The resistance class of room-forming components, windows, and doors SHOULD be adapted to the security needs of the room in question. The quality of locks, locking cylinders, and security fittings SHOULD correspond to the resistance class of the door at hand.

INF.5.A21 ELIMINATED (H)

This requirement has been eliminated.

INF.5.A22 Redundant Power Supply Design [Planner] (H)

In a technical infrastructure room, there SHOULD be a two-line power supply that runs all the way from the low-voltage main distribution board (LVMDS) to the consumer. These power supplies SHOULD be located in separate fire zones. The LVMDS SHOULD be redundant in operation.

INF.5.A23 Emergency Power Systems [Planner, Building Services, Maintenance Personnel] (H)

An organisation's energy supply SHOULD be supplemented by an emergency power system (EPS). The fuel supply for the EPS SHOULD be checked regularly. The EPS SHOULD also maintained at regular intervals. Load and functional tests, as well as test runs under load, SHOULD be conducted when performing maintenance.

INF.5.A24 Ventilation and Cooling [Planner, Building Services, Maintenance Personnel] (H)

Ventilation and cooling systems SHOULD be designed to be redundant in operation. It SHOULD be ensured that these systems are regularly maintained.

In case of very high protection needs, maintenance redundancy SHOULD also be ensured.

INF.5.A25 Increased Protection Against Fire and Smoke Damage [Planner] (H)

Room-forming components, as well as doors, windows, and ventilation flaps, SHOULD resist fire and smoke for at least 90 minutes. The supply lines SHOULD guarantee a functional integrity of at least 90 minutes.

In case of very high protection needs, the room envelope SHOULD be designed as a separate fire zone. Fire dampers controlled by smoke detectors SHOULD be installed in ventilation ducts. Cable trays SHOULD be routed through separate fire zones until they enter the room.

In case of very high protection needs, an early fire detection system and an automatic extinguishing system SHOULD be provided. Fire and smoke detectors SHOULD be connected to the fire alarm control panel. The early fire detection system and the automatic extinguishing system SHOULD be connected to the two-line power supply with UPS and EPS.

INF.5.A26 Monitoring of the Power Supply [Planner, Building Services] (H)

Suitable monitoring equipment SHOULD be installed and operated that can detect prohibitively high currents on the protective conductor system and thus on cable shields (as well as potentially disturbing harmonic oscillations) and flag them in a suitable location for follow-up and remedial action.

4. Additional Information

4.1. Useful Resources

In “DGUV Vorschrift 4 Unfallverhütungsvorschrift, Elektrische Anlagen und Betriebsmittel” [DGUV Regulation 4, Accident Prevention Regulation, Electrical Installations and Equipment], the German Social Accident Insurance (DGUV) provides guidelines for the correct handling of equipment.

The German Institute for Standardisation (DIN) provides specifications for floor coverings in the standard DIN EN 14041:2018-05.

The German Institute for Standardisation (DIN) provides specifications for physical security in buildings and rooms in the standard DIN EN 1627:2011-09.

The German Institute for Standardisation (DIN) provides specifications for the fire behaviour of building materials and building components in the standard DIN EN 4102:2016-05.

The International Electrotechnical Commission provides notes on lightning protection standards in BS EN/IEC 62305.

In the guideline VdS 2311:2017-04, the VdS provides specifications for the use of intrusion systems.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module INF.5 *Room or Cabinet for Technical Infrastructure*.

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.3 Water

G 0.4 Pollution, Dust, Corrosion

G 0.5 Natural Disasters

G 0.8 Failure or Disruption of the Power Supply

G 0.10 Failure or Disruption of Supply Networks

G 0.11 Failure or Disruption of Service Providers

G 0.18 Poor Planning or Lack of Adaptation

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.41 Sabotage

G 0.44 Unauthorised Entry to Premises

INF.6 Storage Media Archives

1. Description

1.1. Introduction

Storage media archives are closed rooms within an organisation that are used to store of all kinds of storage media. In addition to storage media used for digital information, this includes paper documents, film, and other media.

1.2. Objective

This module describes the typical threats and requirements regarding the information security of a storage media archive. The aim is to protect the information stored there and on other types of media.

1.3. Scoping and Modelling

Module INF.6 *Storage Media Archives* must be applied to all rooms that are used as archives for storage media.

This module deals with technical and non-technical security requirements for storage media archives. It does not cover recommendations related to proper archiving. These are included in module OPS.1.2.2 *Archiving*.

Within the IT-Grundschutz framework, no increased requirements are placed on archive rooms with regard to fire protection. However, additional fire protection requirements can be met by the containers in which storage media are stored.

2. Threat Landscape

For module INF.6 *Storage Media Archives*, the following specific threats and vulnerabilities are of particular importance:

2.1. Excessive Temperature and Humidity

Fluctuations in temperature or excessive humidity in areas where long-term digital storage media are kept can cause data errors and reduce the useful storage life of the media.

2.2. Insufficient Rules

If employees fail to close or lock the windows and doors after leaving a storage media archive, storage media or other information can be stolen. Sensitive information could then be viewed or passed on by unauthorised persons. Vulnerabilities can occur if employees are not sufficiently aware of the relevant regulations. It is not sufficient to merely lay down rules; they also need to be observed to ensure smooth operations. Many problems also arise when rules are in place, but not widely known.

2.3. Unauthorised Entry to Sensitive Rooms

If inadequate site access controls have been implemented, unauthorised persons may enter a storage media archive and view, steal, or manipulate sensitive information. This may affect the availability, confidentiality, or integrity of the archived information. This in turn can disrupt operations, even if no immediate damage is evident.

2.4. Theft

Since many storage media are very small, it is all the easier to put them into a bag unnoticed or make off with them by hiding them under clothing. If there are no other copies, the information on stolen storage media will be lost. Furthermore, the persons who have taken the storage media could read and disclose confidential information, which could result in further damage. In most cases, these consequences are considerably more significant than the costs of replacing the stolen storage media.

3. Requirements

The specific requirements of module INF.6 *Storage Media Archives* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Employee, Planner, Building Services, Fire Safety Officer

3.1. Basic Requirements

For module INF.6 *Storage Media Archives*, the following requirements MUST be met as a matter of priority:

INF.6.A1 Hand-Held Fire Extinguishers [Fire Safety Officer] (B)

In case of fire, suitable hand-held fire extinguishers MUST be easily accessible in a storage media archive. These hand-held fire extinguishers MUST be inspected and serviced regularly. Employees working near a storage media archive MUST be instructed in the use of hand-held fire extinguishers.

INF.6.A2 Site Access Regulations and Control [Building Services] (B)

A storage media archive MUST ONLY be accessible to authorised persons. Site access MUST be reduced to a minimum number of employees. Therefore, site access MUST be regulated and controlled. A concept MUST be developed for site access control. The effectiveness of the site access control safeguards it contains SHOULD be regularly reviewed. To prevent site access control from being bypassed or at least make this more difficult, the entire room MUST have mechanical resistance safeguards that satisfy the protection needs at hand; under no circumstances should they correspond to less than RC2 (in accordance with DIN EN 1627).

INF.6.A3 Protection Against Dust and Other Contamination (B)

It MUST be ensured that the media in a storage media archive are adequately protected against dust and dirt. The requirements for this MUST be analysed in the planning phase. A strict smoking ban MUST be observed in storage media archives.

INF.6.A4 Closed Windows and Locked Doors [Employee] (B)

A storage media archive SHOULD NOT have windows if they can be avoided. If there are windows, they MUST be closed when leaving the storage media archive. The door MUST also be locked when leaving the room. Fire and smoke doors MUST be closed.

3.2. Standard Requirements

For module INF.6 *Storage Media Archives*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

INF.6.A5 Using Protective Cabinets [Employee] (S)

The storage media and other media in storage media archives SHOULD be stored in suitable protective cabinets.

INF.6.A6 Avoidance of Water Pipes [Building Services] (S)

In storage media archives, unnecessary water-bearing pipes SHOULD generally be avoided. If water pipes are nevertheless laid through a storage media archive, they SHOULD be checked regularly to ensure that they are still watertight. In addition, precautions SHOULD be taken so that any water leaks will be detected at an early stage. For a storage media archive with high availability requirements, there SHOULD be response plans that specify exactly who is to be informed in case of a leak and how to proceed in general.

INF.6.A7 Compliance with Climatic Requirements [Building Services] (S)

It SHOULD be ensured that the maximum and minimum values permitted for temperature and humidity, as well as the dust content of the air in the room, are observed in a storage

media archive. The air temperature and humidity values SHOULD be recorded and documented several times a year for a period of one week. Any detected deviations from the target value SHOULD be corrected promptly. The air conditioning system used SHOULD be serviced regularly.

INF.6.A8 Secure Doors and Windows [Planner] (S)

Security safeguards such as windows, doors, and walls SHOULD be appropriate and up to the task of dealing with burglary, fire, and smoke. Depending on the protection needs at hand, a suitable resistance class SHOULD be implemented in accordance with DIN EN 1627. All security doors and windows SHOULD be checked regularly to ensure that they are still functioning properly. The entire storage media archive in question SHOULD have mechanical resistance safeguards that meet the relevant protection needs and correspond to RC3 (according to DIN EN 1627) at minimum.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.6 *Storage Media Archives* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

INF.6.A9 Alarm System [Building Services] (H)

An appropriate alarm system SHOULD be set up in storage media archives. This alarm system SHOULD be inspected and serviced regularly. It SHOULD be ensured that the recipients of alarm messages are able to react appropriately to them.

4. Additional Information

4.1. Useful Resources

The German Institute for Standardisation (DIN) provides specifications for physical security in buildings and rooms in the standard DIN EN 1627:2011-09.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module INF.6 *Storage Media Archives*.

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.3 Water

G 0.4 Pollution, Dust, Corrosion

G 0.16 Theft of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.24 Destruction of Devices or Storage Media

G 0.32 Misuse of Authorisation

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

INF.7 Office Workplace

1. Description

1.1. Introduction

An office room is an area within an organisation where one or several employees perform their tasks. This module describes the typical threats and requirements regarding the information security of an office room.

1.2. Objective

The aim of this module is to protect information processed in office rooms.

1.3. Scoping and Modelling

Module INF.7 *Office Workplace* must be applied to every room used as a place of work in the information domain under consideration.

This module deals with technical and non-technical security requirements for office rooms. It does not deal with recommendations on how to configure and safeguard the IT systems in such rooms. Information on this is included in SYS.2.1 *General Client*, as well as in the operating-system-specific modules.

General requirements for buildings are also not part of this module. These are included in module INF.1 *Generic Building*, which should be used in addition to this module. The present module also does not cover the cabling of office rooms. Module INF.12 *Cabling* must be implemented in this regard.

2. Threat Landscape

For module INF.7 *Office Workplace*, the following specific threats and vulnerabilities are of particular importance:

2.1. Unauthorised Site Access

If insufficient site access controls have been implemented, unauthorised persons may enter an office room and extract sensitive data or steal or manipulate devices. This may affect the availability, confidentiality, or integrity of devices and information. Even when no immediate damage is apparent, operations can still be disrupted. It is thus necessary to examine how such an event was possible, whether or not damage occurred, and whether data or devices were manipulated.

2.2. Impairment due to Unfavourable Working Conditions

Office spaces that are not furnished according to ergonomic principles or otherwise provide an unfavourable working environment are problematic. As a result, employees may be unable to work without disturbances or make optimal use of the IT available. Disturbances can include noise, heavy customer traffic, unfavourable lighting, or poor ventilation. They can restrict work processes and employee potential. Errors may also crop up during work and lead to a loss of data integrity.

2.3. Manipulations by Cleaning Staff, Third-Party Personnel, or Visitors

It is often more efficient to use an office for small or short meetings. In doing so, however, visitors could view internal information, jeopardise business processes, and manipulate IT systems in various ways. The same applies to cleaning and other third-party personnel. The possible threats range from improper handling of technical equipment and attempts to “play” with IT systems to the outright theft of documents or IT components. For example, cleaning staff can accidentally loosen a plug connection or water can get into IT equipment. Documents can also be misplaced or even disposed of as waste.

2.4. Manipulation or Destruction of IT, Accessories, Information, or Software in an Office Room

For many reasons, attackers may try to manipulate or destroy IT systems, accessories, and other storage media. The later the attacks are detected by employees or the organisation in question, the greater the knowledge acquired by the perpetrators, the more far-reaching the impact on the corresponding work procedure, and the more effective the attacks will be. For example, sensitive employee data could be viewed without permission. Storage media or IT systems could also be destroyed. This may result in significant downtime and process limitations.

2.5. Theft

As IT devices become ever more portable, it is becoming easier to put them in a pocket without being noticed. When storage media, IT systems, accessories, software, or information are stolen, it costs money to replace them. It also requires resources to restore proper working conditions. On the other hand, losses can occur due to a lack of availability, as well. Someone who steals an IT device could also view and disclose confidential information, which could

result in further damage. In many cases, this is significantly more severe than the mere material loss of the IT device.

In addition to expensive IT systems, portable end devices which can be transported easily and inconspicuously are often stolen. If office rooms are not locked or monitored or the IT systems are not secured sufficiently, the equipment can be stolen quickly without being noticed.

2.6. Exposed Cables

Depending on the position of power sockets and data network ports in an office room, cables could be laid across the room, including in areas where people walk. Exposed cables like these not only constitute tripping hazards which may result in personal injury. If people trip over such cables, this may also damage IT devices.

3. Requirements

The specific requirements of module INF.7 *Office Workplace* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Employee, Central Administration, Building Services, Supervisor

3.1. Basic Requirements

For module INF.7 *Office Workplace*, the following requirements MUST be met as a matter of priority:

INF.7.A1 Suitable Selection and Use of an Office Room [Supervisor] (B)

Rooms used as offices MUST be suitable for this purpose. Office rooms MUST be selected and equipped in accordance with the protection needs or protection level of the information processed in such rooms. Office rooms that are open to the public MUST NOT be located in security-sensitive areas. Germany's regulation on workplaces (*Arbeitsstättenverordnung*) MUST be implemented for workplaces and the equipment of office rooms.

INF.7.A2 Closed Windows and Locked Doors [Employee, Building Services] (b)

When employees leave their office rooms, all windows SHOULD be closed. If confidential information is located in an office room, the doors MUST be locked when leaving the room. This SHOULD be observed in particular in areas used by the public. The corresponding specifications SHOULD be included in suitable instructions. All employees SHOULD be required to comply with the instructions. In addition, regular checks MUST be carried out to ensure that the windows are closed when leaving an office room and, if necessary, that the

doors are locked. Furthermore, it MUST be ensured that fire doors and smoke control doors are actually closed.

3.2. Standard Requirements

For module INF.7 *Office Workplace*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

INF.7.A3 Exposed Cables (S)

The power connections and network access points in an office room SHOULD be located in the same places as the IT devices used. Cabling routed over the floor SHOULD be covered by a cable duct.

INF.7.A4 ELIMINATED (S)

This requirement has been eliminated.

INF.7.A5 Workplace Ergonomics [Central Administration, Supervisor] (S)

All employees SHOULD have ergonomic workplaces. Above all, the monitors SHOULD be positioned to allow ergonomic and undisturbed working. Here, it SHOULD be ensured that screens are not exposed to unauthorised persons. Germany's occupational protection ordinance for working at screens (*Bildschirmarbeitsschutzverordnung*, BildscharbV) SHOULD be implemented. All workplaces SHOULD be individually adjustable to ensure problem-free IT operations.

INF.7.A6 Workplace Cleanliness [Employee, Supervisor] (S)

All employees SHOULD be required to keep their workplaces tidy when they leave them. The employees SHOULD make sure that no confidential information can be viewed by unauthorised persons. All employees SHOULD carefully check their workplaces and ensure that no confidential information is freely accessible. Supervisors SHOULD check workplaces sporadically to ensure that no sensitive information is exposed.

INF.7.A7 Suitable Storage of Official Documents and Storage Media [Employee, Building Services] (S)

Employees SHOULD be instructed to lock up confidential documents and storage media when they are not in use. To this end, suitable containers SHOULD be provided in or near office rooms.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.7 *Office Workplace* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

INF.7.A8 Use of Anti-Theft Devices [Employee] (H)

If access to rooms cannot be limited in a suitable manner, anti-theft protection devices SHOULD be used for all IT systems. Anti-theft protection devices SHOULD also be used in areas frequented by the public.

4. Additional Information

4.1. Useful Resources

In "The Standard of Good Practice for Information Security", the Information Security Forum (ISF) provides guidelines for the physical security of buildings, rooms, and their surroundings in section CF19.

The German Institute for Standardisation (DIN) provides specifications for physical security in buildings and rooms in the standard DIN EN 1627:2011-09.

In its regulation on workplaces (*Arbeitsstättenverordnung*), the Federal Ministry of Labour and Social Affairs sets out requirements for setting up and operating workplaces to protect the health and safety of employees.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module INF.7 *Office Workplace*.

G 0.2 Unfavourable Climatic Conditions

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.44 Unauthorised Entry to Premises

G 0.46 Loss of Integrity of Sensitive Information

INF.8 Working from Home

1. Description

1.1. Introduction

Teleworkers, freelance employees, and the self-employed typically work from home. In contrast to a company office, these employees use a workplace on their own property. They thus need to be able to sufficiently separate their occupational and private environments. If employees work from home on an ongoing basis, various legal requirements must also be fulfilled; for example, their workplaces must meet the requirements regarding occupational health and ergonomics.

Meanwhile, a home workplace cannot be expected to meet the same infrastructural security requirements as the office rooms of an organisation. A home workplace is often also accessible to visitors or family members, for example. That is why safeguards must be taken to achieve a security level that is comparable to an office room.

1.2. Objective

This module shows how the infrastructure of a home workplace can be established and operated in a secure manner. The core objective of the module is to protect organisations' information when their employees work from home.

1.3. Scoping and Modelling

Module INF.8 *Working from Home* must be applied to all rooms that are used for teleworking.

The module contains basic specifications to be considered and fulfilled to counteract the threats relevant to home workplaces. However, it only defines specific requirements for the infrastructure of a stationary workplace that can be accessed by third parties. Security requirements for the IT systems used (e.g. clients and multifunctional devices) and, in particular, the technical aspects of teleworking (e.g. communication links) are not the subject of this module. They are described in module OPS.1.2.4 *Teleworking* or in the respective system-specific modules.

2. Threat Landscape

For module INF.8 *Working from Home*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Rules for Home Workplaces

Since home workplaces are located outside of the respective organisation, employees are mainly on their own in this environment. Insufficient rules for the home workplace environment may result in IT problems and increased downtime. If IT problems cannot be solved through remote administration, an IT support technician may need to travel to the home workplace in question in order to solve them. If the handling of internal and confidential information at home workplaces is not regulated in a transparent manner, employees may store the information incorrectly. If it is not possible to prevent espionage and unauthorised modifications involving such information, its confidentiality and integrity may be compromised.

2.2. Unauthorised Access to Sensitive Rooms of a Home Workplace

Rooms of a home workplace in which sensitive information is stored and processed or sensitive devices are kept or operated are considered sensitive rooms. Allowing unauthorised persons to enter these rooms without being monitored poses a significant risk to the confidentiality, integrity, and availability of the data present.

Examples:

- An employee has set up an office at home in a separate room, but does not always lock the door. When she leaves her children unsupervised for a moment, they begin playing in the unlocked home office. The children then use important documents for colouring.
- As an employee is working on a project at his home workplace, he has an unexpected visitor. Whilst the employee is making coffee in the kitchen, the visitor briefly wants to search for something on the Internet and accidentally infects the unlocked client with malware.

2.3. Impaired Use of IT due to Adverse Working Conditions at a Home Workplace

A home workplace that is not designed to be ergonomic or otherwise provides an unfavourable working environment may make it impossible to work without disturbances. This may also impair an employee's ability to make optimal use of IT. Factors like noise, disturbances caused by family members, and poor lighting or ventilation can have an unfavourable effect. This in turn hinders work processes and limits employee potential. Errors may also crop up during work and the protection of data integrity may be diminished.

2.4. Insecure Transport of Files and Storage Media

When documents, storage media, or files are transported between an organisation and a home workplace, the corresponding data can be lost. These items could also be stolen, read, or manipulated by unauthorised third parties. The transport of paper files and storage media may be insufficiently secured in many ways:

- If a unique item is transported and there is no corresponding backup, it will not be possible to achieve goals or complete tasks as planned if the item is lost.
- If unencrypted storage media fall into the wrong hands, this can lead to a serious loss of confidentiality.
- If sufficient access protection is not provided during transport, paper files and storage media can be copied or manipulated without this being detected.

2.5. Inadequate Disposal of Storage Media and Documents

If it is not possible for employees to dispose of storage media and documents properly at their home workplace, they may simply dispose of them in the household rubbish. Attackers may then use these items to obtain valuable information that can be used for targeted blackmailing attempts or industrial espionage. The consequences include everything from a loss of knowledge to threats to the existence of the organisation in question, such as if important contracts cannot be concluded or partnerships fail as a result.

2.6. Manipulation or Destruction of IT, Accessories, Information, or Software at a Home Workplace

The IT, accessories, information, and software that are used can be manipulated or destroyed more easily at a home workplace than within an organisation. A home workplace is often accessible to relatives and family visitors. Furthermore, it does not have the central protective safeguards of an organisation (e.g. gatekeeper services). If IT devices, accessories, information, or software are manipulated or destroyed at a home workplace, this often limits the respective employee's ability to work. It may also be necessary to replace destroyed IT components, information, and software solutions, which requires both time and money.

2.7. Higher Risk of Theft at Home Workplaces

A home workplace is usually not as secure as a workplace at a company or a public authority. Due to more elaborate precautions, such as security doors or a gatekeeper service, the risk of someone entering an organisation's building without authorisation is much lower compared to a private home. In most cases, burglars primarily steal objects that can be sold quickly and easily. At the same time, IT used for work may also be stolen. However, the information on stolen IT systems is often more valuable than the systems themselves. Burglars could attempt to make even more money through extortion or by transferring the data to a competitor than they could by selling such hardware.

3. Requirements

The specific requirements of module INF.8 *Working from Home* are listed below. As a matter of principle, the Employee is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Employee
Further responsibilities	

3.1. Basic Requirements

For module INF.8 *Working from Home*, the following requirements MUST be met as a matter of priority:

INF.8.A1 Securing Official Documents at the Home Workplace (B)

Official documents and storage media MUST be stored at a home workplace in such a way that they are inaccessible to unauthorised persons. Therefore, sufficient lockable containers (e.g. wheeled containers or cabinets) MUST be available. Every employee MUST leave their home workplace in a tidy condition and ensure that no sensitive information is freely accessible.

INF.8.A2 Transporting Working Material to the Home Workplace (B)

The storage media and documents that may be processed at a home workplace and transported between it and the respective organisation MUST be specified. In general, storage media and other documents MUST be transported securely. These rules MUST be communicated to all employees in a suitable manner.

INF.8.A3 Protection Against Unauthorised Access to the Home Workplace (B)

Employees MUST be informed of the rules and safeguards to be considered with regard to anti-burglary and site access protection. For example, they MUST be instructed to close windows and lock doors when leaving their home workplace.

It MUST be ensured that unauthorised persons cannot enter a home workplace or access work-related IT or documents at any time. These safeguards MUST be reviewed at appropriate intervals, or at least when domestic circumstances change.

3.2. Standard Requirements

For module INF.8 *Working from Home*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be implemented as a matter of principle.

INF.8.A4 Suitable Configuration of the Home Workplace (S)

A home workplace SHOULD be separated from the private areas of the home based on a suitable room layout. A home workplace SHOULD have office furniture that meets ergonomic requirements.

A home workplace SHOULD also be protected against burglary by suitable technical security safeguards. The security safeguards SHOULD be adapted to the local situation and the protection needs at hand.

INF.8.A5 Disposal of Confidential Information at the Home Workplace (S)

Confidential information SHOULD be disposed of securely. A special security policy SHOULD thus specify how to dispose of sensitive material. The required disposal options SHOULD be available.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.8 *Working from Home* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

INF.8.A6 Handling Official Documents with Increased Protection Needs at the Home Workplace (H)

If employees must process work-related documents or information with increased protection needs, it SHOULD be considered whether working from home is feasible at all. Otherwise, the home workplaces in question SHOULD be protected by extended high-quality technical safeguards.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for the physical and environmental security of buildings and rooms in annex A.11 of ISO/IEC 27001:2013.

The German Institute for Standardisation (DIN) provides specifications for physical security in buildings and rooms in the standard DIN EN 1627:2011-09.

The National Institute of Standards and Technology (NIST) has published NIST Special Publication 800-53, “Assessing Security and Privacy Controls for Federal Information Systems and Organizations”, which provides specifications on the physical and environmental security of buildings in appendix F-PS.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module INF.8 *Working from Home*.

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.3 Water

G 0.4 Pollution, Dust, Corrosion

G 0.13 Interception of Compromising Interference Signals

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.41 Sabotage

G 0.44 Unauthorised Entry to Premises

INF.9 Mobile Workplace

1. Description

1.1. Introduction

Good network coverage and powerful IT devices such as laptops, smartphones, or tablets make it possible for employees to work almost everywhere. This often means that work-related activities are not only performed in the rooms and buildings of an organisation, but at changing workplaces in various environments (e.g. hotel rooms, trains, or customer locations). The information processed in this way must be protected appropriately.

On the one hand, mobile working changes the duration, location, and distribution of working hours. On the other, it increases the demands placed on information security because the secure IT infrastructure found in an office environment cannot be assumed in mobile working environments.

1.2. Objective

This module describes security requirements for mobile workplaces. The aim is to achieve security conditions in such workplaces that are comparable to those of an office room.

1.3. Scoping and Modelling

Module INF.9 *Mobile Workplace* must be applied to all spaces that are regularly used as a mobile workplace.

This module contains basic specifications that are to be considered and fulfilled when employees work not only within an organisation, but regularly at changing external workplaces, as well.

Above all, it covers the organisational, technical, and personnel requirements that pertain to employees who perform at least part of their tasks in mobile environments. In order to protect IT systems, storage media, and documents used in mobile workplaces, all the relevant modules—such as SYS.3.1 *Laptops*, SYS.3.2 *General Smartphones and Tablets,* SYS.4.5 *Removable Media*, NET.3.3 *VPN,* and SYS.2.1 *General Client*—must be considered separately.

Security requirements for workstations that an organisation establishes on a permanent basis outside of its buildings (i.e. teleworking workstations) are not the subject of this module. These are described in module OPS.1.2.4 *Teleworking*. Security requirements for teleworking infrastructure are also not addressed here. This topic is dealt with in module INF.8 *Working from Home*.

2. Threat Landscape

For module INF.9 *Mobile Workplace*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Rules for Mobile Workplaces

If mobile working is insufficiently regulated, an organisation may suffer financial damage or other consequences. For example, failure to regulate the information that can be transported and processed outside of an organisation and the protective safeguards that must be considered could allow confidential information to fall into the wrong hands. Such information could be used against an organisation by unauthorised persons.

2.2. Degradation due to Changing Operational Environments

Since mobile storage media and end devices are used in a very wide range of environments, they are subject to numerous threats. These threats include, for example, damaging environmental conditions such as excessively high or low temperatures, dust, and moisture. Transport damage can also occur.

In addition to these influences, operational environments and their different security levels must be considered. Smartphones, tablets, laptops, and similar mobile devices are not only portable, but can also communicate with other IT systems. This could allow malware to be transmitted or sensitive information copied. It may also become impossible to fulfil tasks or visit customers, and IT systems may be damaged.

2.3. Manipulation or Destruction of IT Systems, Accessories, Information, or Software at a Mobile Workplace

IT systems, accessories, information, and software that are used in a mobile manner may be manipulated or destroyed more easily than when used within an organisation. A mobile workplace is often accessible to third parties. Furthermore, it does not have an organisation’s central protective safeguards, such as gatekeeper services. If IT systems, accessories, information, or software are manipulated or destroyed, this often impairs the respective mobile employee's ability to work. Furthermore, it may be necessary to replace destroyed IT components or software solutions, which requires both time and money.

2.4. Delays Caused by Temporarily Restricted Availability

In most cases, an employee using a mobile workplace does not have fixed working times and can be difficult to contact when on the move. This may delay the flow of information

significantly. Even sending information in an e-mail might not necessarily shorten an employee's response time because there is no guarantee that the employee will read the e-mail promptly. Depending on the situation and organisation at hand, temporarily limited availability can have different effects, but may limit the availability of information significantly.

2.5. Insecure Transport of Files and Storage Media

If documents, storage media, or paper files are transported between an organisation and mobile workplaces, the corresponding data can be lost; it can also be stolen, read or manipulated by unauthorised third parties. This may result in significant financial damage to the organisation. The transport of paper files and storage media may be insufficiently secured in many ways:

- If a unique item is transported and there is no corresponding backup, it will not be possible to achieve goals or complete tasks as planned if the item is lost.
- If unencrypted storage media fall into the wrong hands, this may result in a serious loss of confidentiality.
- If sufficient access protection is not available during transport, paper files and storage media can be copied or manipulated without this being detected.

2.6. Inadequate Disposal of Storage Media and Documents

If it is not possible to dispose of storage media and documents properly, these items usually land in the ordinary rubbish. This also applies to employees working on the move, who often throw drafts and other documents that seem useless directly into the nearest waste paper basket. Such items can also be left lying around in hotels or trains. However, if storage media or documents are not disposed of properly, attackers may use them to obtain valuable information that can be used for targeted blackmailing attempts or industrial espionage. The consequences include everything from a loss of knowledge to threats to the existence of the organisation in question, such as if important contracts cannot be concluded or partnerships fail as a result.

2.7. Loss of Confidentiality of Sensitive Information

At mobile workplaces, it is easier for attackers to access confidential information stored on hard disks, removable storage media, or paper, particularly if they are professional attackers. They may also eavesdrop on communication links. If information is read or disclosed without authorisation, this has serious consequences for the entire organisation in question. Among other things, a loss of confidentiality may result in the organisation violating laws or suffering from competitive disadvantages and financial damage.

2.8. Theft or Loss of Storage Media or Documents

A mobile workplace is generally not as secure as a workplace at a company or a public authority. Work-related IT systems and documents can therefore be stolen more easily—for example, during a train journey, from a hotel room, or from external conference rooms.

In addition, IT systems or components can be lost. Alongside the purely material damage caused by the immediate loss of a mobile IT system, further financial damage can also occur, such as if e-mails, notes from meetings, addresses, or other sensitive data are disclosed. This can also damage an organisation's reputation.

3. Requirements

The specific requirements of module INF.9 *Mobile Workplace* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Employee, IT Operation Department, Central Administration, Human Resources Department

3.1. Basic Requirements

For module INF.9 *Mobile Workplace*, the following requirements MUST be met as a matter of priority:

INF.9.A1 Appropriate Selection and Usage of a Mobile Workplace [IT Operation Department] (B)

An organisation MUST stipulate how employees are to select and use mobile workplaces in a suitable way. It MUST define the features that are desirable for a mobile workplace. It MUST also define the criteria that rule out a mobile workplace. At minimum, the following MUST be specified:

- workplace conditions that are allowed for processing sensitive information
- how employees at mobile workplaces should protect their information against unwanted third-party access
- whether a continuous network and power supply is required
- workplace environments that are absolutely forbidden

INF.9.A2 Regulations for Mobile Workplaces [Human Resources Department] (B)

For all work done on the move, the information that may be transported and processed outside the organisation at hand MUST be regulated, along with the protective safeguards to be taken. The framework conditions required in order for employees with mobile IT systems to access their organisation's internal information MUST also be defined.

There MUST be clear rules governing the transportation of IT components and storage media. These MUST specify the IT systems and storage media that are allowed to be transported, the persons authorised to transport them, and the basic security requirements to be considered.

Records MUST be kept as to who has used which mobile devices at what times while not on their organisation's premises.

The users of mobile devices MUST be made aware of the value of mobile IT systems and the information stored on them. They MUST be informed of the specific threats and safeguards regarding the IT systems they use. Moreover, they MUST be informed of the types of information that may be processed on mobile IT systems. All users MUST be informed of the rules they need to follow. They MUST be trained accordingly.

INF.9.A3 Site and Data Access Protection [Central Administration, Employee] (B)

Employees MUST be informed of the rules and safeguards to be considered with regard to intrusion and site access protection at mobile workplaces. When a mobile workplace is not in use, the windows and doors MUST be closed. If this is not possible, such as on a train, employees MUST store all their documents and IT systems in a secure location when they are absent or take them with them. It MUST be ensured that unauthorised persons cannot access work-related IT or documents at any time. If a workplace is only left for a short time, the IT systems in use MUST be locked so that they can only be used again after successful authentication.

INF.9.A4 Working with External IT Systems [IT Operation Department, Employee] (B)

An organisation MUST specify how employees may work with external IT systems. Every mobile employee MUST be informed about the dangers of third-party IT systems. The regulations MUST specify whether and how sensitive information may be processed on third-party IT systems. They MUST also specify how to prevent unauthorised persons from viewing such information. If employees work with external IT systems, it MUST be ensured in principle that all temporary data created during such periods is deleted.

3.2. Standard Requirements

For module INF.9 *Mobile Workplace*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

INF.9.A5 Prompt Reporting of a Loss [Employee] (S)

Employees SHOULD report any loss or theft of information, IT systems, or storage media to their organisation immediately. To this end, there SHOULD be clear reporting channels and contact persons within the organisation.

INF.9.A6 Disposal of Confidential Information [Employee] (S)

Confidential information SHOULD be disposed of securely, even on the move. Before old or defective storage media and documents are destroyed, they MUST be checked for sensitive information. If they contain sensitive information, storage media and documents MUST be returned and disposed of or destroyed using the respective organisation’s methods.

INF.9.A7 Legal Framework Conditions for Mobile Working [Human Resources Department] (S)

Framework conditions pertaining to labour regulations and occupational safety laws SHOULD be observed and specified for mobile working. All the relevant aspects SHOULD be clarified in employment agreements, or in separate agreements between mobile employees and their employers as a supplement to their employment contracts.

INF.9.A8 Security Policy for Mobile Workplaces [IT Operation Department] (S)

All the relevant security requirements for mobile workplaces SHOULD be documented in a security policy that is mandatory for mobile employees. Furthermore, this policy SHOULD be adapted to the existing security policies of the organisation in question and agreed with all its relevant departments. The security policy for mobile workplaces SHOULD be updated regularly. The employees of the organisation SHOULD be made aware of and trained in its current security policy.

INF.9.A9 Encryption of Portable IT Systems and Storage Media [IT Operation Department] (S)

It SHOULD be ensured that portable IT systems and storage media are secured in line with the respective organisation's internal guidelines. Mobile IT systems and storage media SHOULD be encrypted. Cryptographic keys SHOULD be stored separately from the corresponding encrypted devices.

INF.9.A12 Using a Screen Protector [Employee] (S)

When IT systems are used at mobile workplaces, employees SHOULD use privacy screens.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.9 *Mobile Workplace* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

INF.9.A10 Use of Anti-Theft Devices [Employee] (H)

If an IT system in use provides a means of anti-theft protection, this SHOULD be used. Anti-theft devices SHOULD always be used in places with increased public traffic or a high rate of user fluctuation. In this respect, employees SHOULD always take into account that the protection of the information stored on an IT system usually has a higher value than the cost of the system itself. The acquisition and usage criteria for anti-theft devices SHOULD be adapted to an organisation’s processes and documented.

INF.9.A11 Prohibiting Use of Insecure Environments [IT Operation Department] (H)

The minimum criteria that mobile working environments must fulfil to allow the processing of information with increased protection needs SHOULD be determined. The criteria should cover the following topics at minimum:

- access and viewing by third parties
- closed and, if required, lockable or guarded rooms
- secured communication options
- a sufficient power supply

4. Additional Information

4.1. Useful Resources

In annex A.11.2 of ISO/IEC 27001:2013, the International Organization for Standardization (ISO) specifies requirements for equipment of mobile workplaces.

In annex A.6.2.1 of ISO/IEC 27001:2013, the International Organization for Standardization (ISO) provides guidelines for developing a policy for mobile devices.

The Information Security Forum (ISF) provides guidelines for dealing with mobile devices in section PA2 of “The Standard of Good Practice for Information Security”.

The National Institute of Standards and Technology (NIST) has published NIST Special Publication 800-46, "Remote Access and Bring Your Own Device (BYOD)”, which provides guidelines on remote access technologies.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module INF.9 *Mobile Workplace*.

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

INF.10 Meeting, Event, and Training Rooms

1. Description

1.1. Introduction

Every organisation usually has one or more rooms for holding meetings, training courses, or other events. Specially equipped rooms are often designated for this purpose. Meeting, event, and training rooms are usually used by different persons and/or groups of persons and visitors, and generally for a limited period of time. IT systems that participants bring along are often operated together with the organisation's devices, as in the case of external laptops that are connected to overhead projectors. These different usage scenarios result in a particular risk situation that does not exist in the same way in other rooms of the organisation.

1.2. Objective

The aim of this module is to protect the information processed in meeting, event, and training rooms, along with the IT systems operated in such rooms. Moreover, it addresses the recommended procedure for visitors who use these rooms.

1.3. Not in scope and modelling

Module INF.10 *Meeting, Event, and Training Rooms* must be applied to all rooms used for meetings, events, and training.

This module addresses all the technical and non-technical security aspects of using meeting, event, and training rooms. It does not deal with detailed recommendations on how to configure and safeguard the IT systems in such rooms. Information on this is included in SYS.2.1 *General Client*, as well as in the operating-system-specific modules. Further security aspects relevant to meeting rooms, such as WLAN or video conferencing systems, are addressed in the modules of the layers NET.2 *Radio Networks* and NET.4 *Telecommunication*. Cabling in these rooms is specifically considered in module INF.12 *Cabling*. Requirements for

fire prevention are included in module INF.1 *Generic Building*. Requirements for monitoring visitors are included in module ORP.1 *Organisation*.

2. Threat Landscape

For module INF.10 *Meeting, Event, and Training Rooms*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Rules

If employees do not close the windows and doors after leaving a meeting, event, or training room or if confidential information is not removed from a whiteboard or flip chart, for example, this information could be seen by unauthorised persons. In general, employees should be provided with relevant rules to prevent such vulnerabilities from occurring. However, the specification of rules alone does not ensure they will be followed, nor does it ensure trouble-free operations. Many problems arise when rules are in place but employees are not aware of them. Employees often do not know, for example, that windows and doors must be locked after meetings or how they should deal with flip charts.

2.2. Incompatibility between External and In-House IT Systems

IT systems are becoming more mobile and increasingly being used in different environments. Users often find scenarios in which their own IT systems cannot be used as planned because they are not compatible with third-party IT systems. For example, older devices do not have the same connectors and plugs as newer devices. Moreover, there are devices that require the right adapter to interface with other devices. Without a suitable adapter, it may not be possible to connect a laptop that contains important data for a meeting to an overhead projector (for instance). Furthermore, attempts to connect IT systems despite their incompatibility may damage the devices or their stored data.

2.3. Threats Caused by Visitors

Organisations often find it difficult enough to ensure that their own employees are sufficiently aware of how to properly handle sensitive information and IT systems. In contrast to internal employees, it cannot be assumed that visitors will handle the information and information technology accessible to them in accordance with the guidelines of the organisation they are visiting, especially since they are usually not aware of such rules. If the organisation's own employees are careless, visitors can generally gain access to confidential information. This can also occur unwittingly, as in the case of a visitor who mistakenly enters an employee's office when looking for the toilet and finds a whiteboard displaying confidential information. Visitors can also destroy or damage devices intentionally to obtain confidential information.

2.4. Exposed Cables

Meeting, event, and training rooms are subject to frequent changes in terms of both the people who use them and the ways in which they are used. This sometimes also requires ongoing

changes in equipment, and thus changes in cabling in these rooms, as well. Depending on the positions of the connection points in a room (power sockets and data outlets), cables may be routed temporarily across the room, including in areas where people walk. Tripping hazards like these can not only cause injuries to people; IT systems can also be damaged if a person pulls on exposed cables when falling.

2.5. Theft

If the storage media (some of which are installed in a fixed location), IT systems, accessories, software or data installed in a meeting room are stolen, this will result in the expense of having to replace the equipment and restore it to working order. In addition, the meeting room will only be usable to a limited extent for as long as the stolen items are missing. This may cause bottlenecks in room allocation. Furthermore, confidential information can be stolen, misused, or shared with others.

In addition to expensive IT systems, portable end devices which can be transported easily and inconspicuously are often stolen. If meeting, event, and training rooms are not monitored or their IT systems are not secured sufficiently, equipment can be stolen quickly without anyone noticing. This applies in particular if, for example, rooms are not locked during meeting breaks.

2.6. Loss of Confidentiality of Sensitive Information

Confidential information can be disclosed due to technical failure, carelessness, a lack of knowledge, or deliberate acts. In such cases, this information can be present in different locations, such as on storage media within IT systems (e.g. hard disks), on removable storage media (e.g. USB pen drives or optical media), in printed form, or on whiteboards or flip charts. If information is read or disclosed in an unauthorised manner, this may have serious consequences for the organisation in question, such as legal violations, competitive disadvantages, or financial damage.

3. Requirements

The specific requirements of module INF.10 *Meeting, Event, and Training Rooms* are listed below. As a matter of principle, Central Administration is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Central Administration
Further responsibilities	Employee, IT Operation Department, Building Services

3.1. Basic Requirements

For module INF.10 *Meeting, Event, and Training Rooms*, the following requirements MUST be met as a matter of priority:

INF.10.A1 Secure Use of Meeting, Event, and Training Rooms [Building Services, IT Operation Department] (B)

The equipment present in such rooms MUST be protected appropriately against theft. Furthermore, the persons who manage the IT and other systems present in such rooms MUST be defined. It MUST also be specified whether visitors may use IT systems they bring along and, if so, under which conditions. Furthermore, the network access points and telecommunications interfaces that can be accessed by visitors MUST be specified.

INF.10.A2 ELIMINATED (B)

This requirement has been eliminated.

INF.10.A3 Closed Windows and Doors [Employee] (B)

The windows MUST be closed when leaving meeting, event, or training rooms. The doors MUST be locked when leaving rooms that contain IT systems or sensitive information. In addition, regular checks MUST be carried out to ensure that the windows and doors have been locked after leaving such rooms. Furthermore, it MUST be ensured that fire doors and smoke control doors are actually closed.

3.2. Standard Requirements

For module INF.10 *Meeting, Event, and Training Rooms*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

INF.10.A4 Planning Meeting, Event, and Training Rooms (S)

When planning meeting, event, and training rooms, the location of the rooms SHOULD be given special consideration. In particular, rooms often used together with or exclusively by visitors SHOULD NOT be located close to parts of the building where confidential information is regularly processed. The level of confidentiality of the information discussed or processed there SHOULD be specified for each room.

INF.10.A5 Exposed Cables (S)

Power connections SHOULD be placed in locations where projectors, laptops, or other devices requiring electricity are to be set up. Cabling routed over the floor SHOULD be covered by a cable duct.

INF.10.A6 Configuring Secure Network Access [IT Operation Department] (S)

It SHOULD be ensured that the IT systems visitors bring along cannot be connected to a given organisation’s internal IT systems via the data network. Only designated IT systems SHOULD be able to access the organisation's LAN. A data network for visitors SHOULD be kept separate from the organisation's LAN. Network access points SHOULD be configured so that third parties are prevented from reading internal exchanges of data. Network connections in

meeting, event, or training rooms SHOULD be safeguarded. The IT systems in meeting, event, and training rooms SHOULD be prevented from establishing simultaneous connections to the intranet and the Internet.

Furthermore, the power supply SHOULD be established separately from other rooms from the last sub-distributor.

INF.10.A7 Secure Configuration of Training and Presentation Computers [IT Operation Department] (S)

Dedicated training and presentation computers SHOULD have a minimum configuration. The applications that can be used on the training and presentation computers during each event SHOULD be specified. The training and presentation computers SHOULD only be connected to a separate data network that is isolated from the LAN of the organisation at hand.

INF.10.A8 Creating a Proof of Use for Rooms (S)

Depending on the ways in which meeting, event, and training rooms are used, the persons using the rooms and the corresponding times SHOULD be evident. Proof of use SHOULD also be provided for rooms where training on IT systems or particularly confidential meetings are held. It SHOULD be considered whether corresponding proof of use should also be implemented for rooms that are accessible to every employee.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.10 *Meeting, Event, and Training Rooms* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

INF.10.A9 Resetting Training and Presentation Computers [IT Operation Department] (H)

A procedure for resetting training and presentation computers to a pre-defined state after use SHOULD be specified. Changes made by users SHOULD be removed completely in such cases.

INF.10.A10 Ban on Carrying Mobile Phones (H)

Mobile phones SHOULD NOT be taken into confidential meetings and conversations. If necessary, this ban SHOULD be enforced by detectors.

4. Additional Information

4.1. Useful Resources

The International Organization for Standardization (ISO) provides guidelines for the physical and environmental security of buildings and rooms in annex A.11 of ISO/IEC 27001:2013.

In "The Standard of Good Practice for Information Security", the Information Security Forum (ISF) provides guidelines for the physical and environmental security of buildings and rooms in chapter CF19.

The German Institute for Standardisation (DIN) provides specifications for physical security in buildings and rooms in the standard DIN EN 1627:2011-09.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module INF.10 *Meeting, Event, and Training Rooms*.

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.21 Manipulation of Hardware or Software

G 0.24 Destruction of Devices or Storage Media

G 0.41 Sabotage

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

INF.11 General Vehicle

1. Description

1.1. Introduction

Organisations use a wide variety of vehicles in many different situations to cover short and long distances. In the context of this module, vehicles are generally classified as motorised means of land, air, or water-based transport that have a vehicle cabin or similar enclosure. Some examples include passenger cars, lorries, aircraft, or ships. In this module, only the generic term "vehicle" is used unless a specific type of vehicle is meant.

Almost all modern vehicles have integrated IT components (e.g. infotainment systems or internal analysis systems) which must be considered holistically in the context of information security. In addition, official tasks are often carried out not only in the rooms and buildings of an organisation, but also within vehicles, which may move between different locations and environments. A vehicle is thus also a mobile working environment in its own right which must be adequately secured by the organisation in question.

1.2. Objective

This module describes specific hazards that must be considered when organisations use vehicles with IT components or use vehicles in general as IT workstations. On this basis, the module defines the requirements that must be fulfilled by vehicle users and owners in order to ensure optimal vehicle operation from an information security perspective.

1.3. Scoping and Modelling

Module INF.11 *General Vehicle* must be applied once to each land, air, and water vehicle used by the organisation in question.

It is designed for users and operators of vehicles. Autonomous or remote-controlled vehicles, rail vehicles, and space vehicles are excluded from this module.

The type, equipment, place of use, and field of activity of a given vehicle may differ depending on the organisation at hand. In module INF.11 *General Vehicle*, only the typical operational

scenarios of vehicles are considered; special operational purposes, such as those pertaining to rescue helicopters or military vehicles, must also be considered on a case-by-case basis.

For this reason, there is no conclusive discussion of retrofitted, mission-specific IT systems or vehicle-specific specialised applications, such as those that are common in emergency vehicles or command vehicles. The equipment and the associated specialised applications of these vehicles must be dealt with individually.

Furthermore, in-vehicle networks (IVNs) established via communication buses such as CAN, LIN, or Flexray are not considered because they are usually not changed by the user.

In order to secure IT components that are carried by users or installed at a later point in time, all the relevant modules—such as SYS.3.1 *Laptops*, SYS.3.2 *General Smartphones and Tablets*, and NET.3.3 *VPN*, as well as the module layers NET.4 *Telecommunication* and NET.2 *Radio Networks*—must be considered separately.

In addition, before a vehicle is disposed of, the CON.6 *Deleting and Destroying Data and Devices* module must be applied to ensure that no sensitive information remains in the vehicle.

Since this module deals with all the relevant infrastructure aspects, there is no need to model INF.9 *Mobile Workplace*.

2. Threat Landscape

For module INF.11 *General Vehicle*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Rules for Vehicles

If there no sufficient regulation regarding the information that may be transmitted and processed via the networks made available to users by vehicles (e.g. via WLAN or Bluetooth) and the protective safeguards that are to be taken, confidential information may be disclosed. Failure to adequately regulate how such networks are to be secured and used could expose sensitive information such as personal data.

If vehicles are stolen or integrated IT components fail and there are no corresponding rules or established procedures, this can have serious consequences. There is a risk that sensitive information may remain in the vehicle and be accessed by unauthorised third parties.

If vehicles or the IT components installed in them are not commissioned properly, this can lead to extensive information security threats. Relevant settings (such as the automatic synchronisation of phone directories) could be incorrectly configured, or functional tests on aircraft could be skipped or carried out improperly. This in turn could lead to the aircraft's systems not functioning as intended during use and, in the worst case, to a total loss of the aircraft.

In the same way, the functionality of integrated IT components or the entire corresponding vehicle can be jeopardised if the vehicle is improperly switched off or temporarily taken out of service. Emergency vehicles are an example of this. If such vehicles are switched off for a longer period of time, there is a risk that their batteries will become completely discharged due

to their extensive equipment. As a result, a vehicle might no longer start and data could be lost in its integrated IT components.

2.2. Carelessness and Lack of Security Awareness in Handling Vehicles

Carelessness and a lack of security awareness when handling vehicles and their components pose a serious danger. If employees are not adequately trained on how to handle vehicles and their IT components, for example, or not aware of the possible risks, this can lead to improper use. For example, IT systems on the bridges of ships are used by different people. If a user changes essential settings without informing the other users, malfunctions could occur that the other users cannot understand.

Vehicles that are not properly locked present another threat. This could allow unauthorised third parties to simply enter a vehicle's cabin and view or steal all the IT components and stored information therein.

Furthermore, poorly trained staff could react inappropriately to faults and make the situation worse. If a user attempts to remedy a malfunction in a vehicle's integrated IT systems rather than contacting the responsible department, this could result in unforeseeable consequences. For example, relevant settings for security or data protection could be changed.

2.3. Unregulated Data Transmission to Third Parties and Insecure Communication Interfaces

In addition to wireless communication interfaces that are relevant or immediately apparent to users (such as Bluetooth or WLAN), many internal vehicle systems communicate directly with the manufacturer's IT systems via integrated mobile radio interfaces. Users typically cannot influence this exchange of information. This includes not only systems that are prescribed by law and transparent to the user (such as eCall), but also those that are not immediately apparent to the user. For example, many vehicle manufacturers collect detailed information about the location and mileage of a given vehicle or about the driver's behaviour. This could result in extensive personal data being aggregated on vehicle users without their knowledge or explicit consent to this data collection and processing.

Insecure vehicle communication interfaces represent a further threat. A lack of protective mechanisms in this regard can allow access to sensitive data. If, for example, an infotainment system allows Bluetooth pairing without security mechanisms, an unauthorised third party could pair their smartphone with it and synchronise address books without anyone noticing.

2.4. Improper Vehicle Modifications

While conventional passenger cars are very rarely modified by their operators, special-purpose vehicles often need to be adapted by their operators or specialised companies. Some examples include emergency vehicles or ships that are modernised or repurposed after their initial manufacture. If a vehicle is improperly modified in a situation like this (e.g. by installing additional cables inappropriately), this can lead to considerable damage or even the total loss of the vehicle.

Other modifications can also impair the operational capability of vehicles. If, for example, an infotainment system is manipulated to enable new or blocked functions, it may no longer be possible to install manufacturer updates and thus close potential vulnerabilities.

2.5. Manipulation, Unauthorised Access, and Theft Involving Vehicles

Information lying open in vehicles can often be seen from the outside if privacy screens have not been adequately implemented. This can attract the attention of potential attackers.

Vehicles are often left in publicly accessible car parks or moored at boat docks that are not protected by the corresponding organisation’s central protective safeguards (e.g. gatekeeper services or locked garages). In principle, this increases the risk of unauthorised entry. Insecure locking systems can be a weak point in this regard. For example, keyless locking systems can be easily bypassed by relay attacks.

IT systems, accessories, information, and software can thus often be manipulated, destroyed, or stolen more easily if they are left unattended in vehicles instead of on the respective organisation's premises. If IT systems, accessories, information, or software are manipulated or destroyed, it often restricts the ability of the employees in vehicles to work. The IT systems affected could even be manipulated by malware to forward the data they process to unauthorised third parties (for example). Furthermore, it may be necessary to replace destroyed IT components, which requires both financial and personnel resources.

2.6. Dangers in Connection with Maintenance, Repairs, and Updates

If vehicles and the IT components used in them are not maintained and serviced or their functionality is not checked regularly, this can lead to them failing or only being operational to a limited extent when needed.

A major challenge here lies in the fact that updates for the IT systems integrated into vehicles are not necessarily available when vehicles have their regular maintenance cycles. This means, for example, that updates can only be installed sporadically and after some delay.

As a rule, vehicles and the IT components installed in them cannot be fully maintained or repaired in the respective organisation's own workshops, which is why they are often handed over to external companies. The vehicles are usually not monitored on the premises of the external companies, which means third parties can gain comprehensive access to a vehicle and its IT components. This increases the risk of misuse of the IT components or the theft of sensitive information.

2.7. Threats During Decommissioning

When vehicles are taken out of service, they can be sold with some (or all) of the IT components installed. This could allow third parties to access the IT components and thereby obtain internal information or personal data, such as stored telephone numbers. In addition, an organisation's own components (e.g. SIM cards or crypto modules) can remain in the vehicles. Subsequent owners could thus gain unintentional access to them and could, for example, read information from these components (such as telephone numbers from the SIM card) for illegal purposes.

2.8. Unacceptable Temperature and Humidity in Vehicles

Every device has a temperature range within which it functions properly. If a room's temperature is outside of this range, IT components and other devices may fail and operations may be disrupted. The same applies to humidity. Vehicles are affected by different conditions that can lead to situations just like these. The interior of vehicles parked in the sun can reach up to 70 degrees (Celsius) and thus exceed the usual temperature range of lithium-ion batteries, for example.

3. Requirements

The specific requirements of module INF.11 *General Vehicle* are listed below. As a matter of principle, the Chief Information Security officer (CISO) is responsible for fulfilling the requirements. The CISO must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	**Roles**
Overall responsibility	Chief Information Security Officer (CISO)
Further responsibilities	Employee, Process Owner, Data Protection Officer, User, Procurement Department, IT Operation Department

3.1. Basic Requirements

For module INF.11 *General Vehicle*, the following requirements MUST be met as a matter of priority:

INF.11.A1 Planning and Procurement [Process Owner, Procurement Department, Data Protection Officer] (B)

The intended use of a vehicle MUST be planned before the vehicle is procured. The functional requirements for vehicles and, in particular, the requirements for information security and data protection of the IT components installed in them MUST be determined. The following aspects MUST be taken into account:

- operational scenarios of the vehicles
- the immediate operational environment of the vehicles
- the entire lifecycle of the vehicles

The vehicles MUST also have adequate locking systems unless they can be continuously secured by other safeguards or arrangements. During planning, consideration SHOULD be given to the fact that many vehicles can transmit data to the vehicle manufacturer and other third parties.

INF.11.A2 Maintenance, Inspection, and Updates [Process Owner, IT Operation Department] (B)

Vehicles and their IT components MUST be maintained in line with the manufacturer's specifications. This MUST take into account that conventional maintenance intervals may not correspond to the updates provided for integrated IT components. Those who are allowed to install such updates MUST be clearly defined along with the environment required for this purpose. Over-the-air (OTA) updates MUST also be installed in a regulated manner.

Maintenance and repair work MUST be carried out by authorised and qualified personnel in a secure environment. The manner in which external companies are to be dealt with SHOULD be clarified prior to such maintenance. If vehicle maintenance takes place at external organisations, checks SHOULD be carried out to ensure that all the unnecessary portable IT systems belonging to the vehicle are removed.

When vehicles are put back into operation, a checklist MUST be used to verify that all the complaints and deficiencies in question have been rectified. The functionality of the IT components involved MUST also be checked.

INF.11.A3 Regulations for the Use of Vehicles [IT Operation Department, Process Owner, User, Data Protection Officer] (B)

Before any activity is carried out in a vehicle that may have an impact on the security of the information processed in the vehicle, it MUST be determined whether the activity is permissible. In this context, the information that may be transported and processed MUST be clearly regulated. In addition, the protective safeguards to be taken MUST be specified. This MUST apply to any kind of information, including that which is exchanged in conversations in vehicles. The framework conditions that are required for employees to access specific types of information at their organisation MUST be clarified.

Furthermore, the extent to which infotainment systems, applications, and other vehicle services may be used MUST be regulated. The manner in which interfaces are to be secured MUST also be specified. Existing business and service directives MUST describe how IT carried in vehicles may be used and stored.

3.2. Standard Requirements

For module INF.11 *General Vehicle*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

INF.11.A4 Creating a Security Policy [Process Owner, IT Operation Department] (S)

All the security requirements relevant to IT within vehicles SHOULD be documented in a security policy that is mandatory for employees. The policy SHOULD be known to all the relevant employees in the organisation in question and should form the basis of their handling of vehicles. The policy SHOULD clearly define responsibilities for individual tasks. The security policy SHOULD be reviewed and updated as appropriate.

INF.11.A5 Drawing Up a Security Concept (S)

For each vehicle, an inventory list SHOULD be drawn up that contains the following:

- the IT components permanently installed or associated with the vehicle (e.g. handheld radios in emergency vehicles)
- the specialised procedures that are executed on the vehicle's integrated IT components
- instructions and operational documentation
- the mobile devices linked to the infotainment system

The inventory list SHOULD be updated regularly and as appropriate. It SHOULD be checked that all inventoried IT components belonging to the vehicle are still present. In addition, the inventory list SHOULD be used to check that no mobile devices have been connected to the infotainment system without authorisation.

INF.11.A66 Establishing Instructions [Process Owner, User] (S)

Instructions in the form of checklists SHOULD be available for all the fundamental situations related to vehicle information security. The instructions SHOULD be integrated into the corresponding security policy and made available in suitable checklists while the vehicle in question is in use. This SHOULD also account for the possibility that the vehicle may be stolen. In particular, the instructions SHOULD address the following scenarios:

- failure of vehicle IT components
- emergency situations such as accidents
- unauthorised vehicle entry
- theft of a vehicle or objects stored therein that are relevant to information security

The responsibilities for each task SHOULD be documented in the checklists. The instructions SHOULD be followed by vehicle users in the corresponding situations. The checklists SHOULD be used to document how users proceeded in such situations.

INF.11.A7 Proper Handling of Vehicles and Sensitive Information [Process Owner, User] (S)

An organisation SHOULD supplement its instructions on vehicle use with guidelines on when, how, and where vehicles may be parked or docked properly. These guidelines SHOULD mainly define environments that adequately protect vehicles from unauthorised access or damage. Furthermore, the information and IT systems that may be kept in vehicles SHOULD be considered. Sufficient safeguards SHOULD be taken to protect access.

Vehicle cargo SHOULD be securely stowed. It SHOULD be ensured that sensitive information cannot be viewed, overheard, or stolen by unauthorised persons from outside vehicles. Employees SHOULD be made aware of the basic operation of vehicles and the IT components involved. Employees SHOULD also be informed of the security risks at hand.

INF.11.A8 Protection against Weather-Related Influences [User, Process Owner] (S)

Vehicles and the IT components installed in them SHOULD be adequately protected against weather-related influences. Additional protective safeguards SHOULD be taken depending on

the type of vehicle, location, and operational environment. Appropriate protective safeguards SHOULD be taken to address extreme weather conditions that occur at short notice.

These protective safeguards SHOULD be documented in the form of checklists in instructions on vehicle use.

INF.11.A9 Ensuring Fuel Supplies [Process Owner] (S)

Before vehicles are deployed, the manner in which they will be supplied with fuel during operations SHOULD be planned. Vehicles SHOULD always be sufficiently supplied with fuel during operations.

INF.11.A10 Disposal [IT Operation Department, Process Owner] (S)

When vehicles are decommissioned, no sensitive information SHOULD remain in them. Before vehicles are decommissioned for the last time, the corresponding inventory list SHOULD be used to check that no inventoried items or any other relevant objects have been left behind.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.11 *General Vehicle* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

INF.11.A11 Replacement Arrangements in the Event of Breakdowns [Process Owner] (H)

Preparatory safeguards SHOULD be taken within the organisation in question in case there is a problem with a driver or a vehicle. Depending on the importance of vehicles, replacement vehicles SHOULD be available. Alternatively, a framework agreement SHOULD be concluded with a suitable external organisation. Replacement drivers SHOULD also be available.

INF.11.A12 Anti-Theft System or Security Guards [Process Owner, Employee] (H)

An alarm system SHOULD be in place. Land-based vehicles SHOULD also have an immobiliser. If a vehicle is abandoned, the alarm and immobiliser SHOULD be activated. Alternatively, vehicles SHOULD be guarded.

INF.11.A13 Damaging Third-Party Interference [Process Owner] (H)

Depending on the type of vehicle, appropriate safeguards SHOULD be taken to protect vehicles from potential third-party interference (such as radio interference) in the planned operational environment.

INF.11.A14 Protection of Sensitive Information from Unauthorised Access and Disclosure [IT Operation Department, Process Owner] (H)

Vehicles and their IT components SHOULD be secured in such a way that sensitive information cannot be read, manipulated, or deleted by unauthorised persons. In this context, the manufacturer safeguards SHOULD be checked and adapted if necessary.

INF.11.A15 Physical Protection of Interfaces [IT Operation Department, Process Owner] (H)

All internal and external physical interfaces of vehicles SHOULD be physically secured against unauthorised use and external influences.

INF.11.A16 Fire Extinguishing System [Process Owner] (H)

Vehicles SHOULD have a fire extinguishing system capable of extinguishing a fire from the outside and inside. Alternatively, suitable fire-fighting equipment SHOULD be stored in vehicles.

INF.11.A17 Network Separation of the In-Vehicle Network with a Special Vehicle Network via Gateways (H)

In general, an organisation SHOULD ensure that no information is exchanged in an unauthorised and undefined manner between

- in-vehicle networks (IVNs, which are typically connected to the networks of vehicle manufacturers) and
- mission-specific IT components.

Gateways with standardised protocols (e.g. in line with Standard CiA 447) SHOULD be used for this purpose. The gateways SHOULD be approved by the vehicle manufacturer.

4. Additional Information

4.1. Useful Resources

The scientific article “IT-Sicherheit und Datenschutz im vernetzten Fahrzeug” [IT Security and Data Protection in the Networked Vehicle] by the Fraunhofer Institute (DOI: 10.1007/s11623-015-0434-4) provides a general overview of networked vehicles, possible applications, the required data, and the resulting threats.

The scientific article "Security Issues and Vulnerabilities in Connected Car Systems" from the 2015 IEEE Conference highlights threats that arise from vehicle networking.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module INF.11 *General Vehicle*.

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

INF.12 Cabling

1. Description

1.1. Introduction

The proper and standards-compliant installation of cabling is part of the basis for secure IT operations. A fundamental distinction must be made between electrical cabling and IT cabling in this regard.

The electrical cabling of IT systems and other devices includes all cables and distributors in a given building, from the feed-in point of the distribution network operator to the connections of end devices.

The IT cabling in an organisation includes all communication cables and passive components such as patch panels or marshalling panels/splice distributors. It therefore forms the physical basis of the internal communication networks. IT cabling ranges from the transfer points from an external network to the connection points of the network users at hand. Transfer points include the connection of a telecommunications provider or the DSL connection of an Internet provider, for example.

Despite this distinction, the fundamental requirements for both types of cabling are identical. The cabling within an organisation should thus always also be considered as a whole.

1.2. Objective

The aim of this module is to protect all electrical cabling and IT cabling from failure, manipulation, and malfunction.

1.3. Scoping and Modelling

Module INF.12 *Cabling* must be applied once to the cabling in buildings and rooms as a supplement to module INF.1 *Generic Building*. The requirements of the present module should always be applied to both IT and electrical cabling.

2. Threat Landscape

For module INF.12 *Cabling*, the following specific threats and vulnerabilities are of particular importance.

2.1. Cable Fires

Cable fires can cause considerable damage to an information domain. A cable fire can cause short circuits or interrupt conductors, for example. As a result, protective devices can also fail. Furthermore, cable fires can produce caustic gases depending on the insulation materials present.

2.2. Inadequate Dimensioning of Cabling

When workplaces, server rooms, or data centres are planned, these plans are often aligned exclusively with current requirements. However, future requirements often demand additional capacity in terms of the power grid and data cables. This may become necessary as soon as additional servers are used or if technical standards change, for example. However, cabling can only be expanded to the extent allowed by existing cables and cable routes.

2.3. Insufficient Documentation on Cabling

If the exact locations of cables are not known because this has been insufficiently documented, cables may be damaged during construction work inside or outside a building. Inadequate documentation also makes it difficult to inspect and repair cables.

Furthermore, it cannot be assumed that all cables in the installation zones in question were installed according to the current standards.

2.4. Inadequately Protected Distributors

In some cases, power supply or data network distributors are installed and left unlocked in areas that are generally accessible. Unauthorised persons could thus open and manipulate such distributors and cause failures in the power or data supply.

2.5. Cable Damage

The less protection is afforded to cables when they are laid, the greater the risk is that they will be intentionally or unintentionally damaged. Besides causing the direct failure of connections, damage can also lead to disruptions later on. Damaged insulation may only affect the functional properties of a cable after a long time has passed.

2.6. Voltage Fluctuations, Overvoltage, and Undervoltage

Fluctuations in supply voltage can occur in all areas of networks. While extremely short and minor events have little or no effect on IT systems, larger fluctuations can lead to

malfunctions. The connected systems can be damaged or even brought down entirely. Destructive overvoltages can also occur.

2.7. Use of Low-Quality Power Strips

In many situations, there are not enough power sockets installed in a given space to operate all the devices needed. Power strips are often used to compensate for this. If these power strips are poor in quality, they can present a major fire hazard.

In many cases, several power strips are chained together to provide sockets for all the devices in use. Connecting power strips in series poses an overload risk that can result in an incomplete short circuit (and a major fire hazard, as well).

2.8. Unauthorised Cable Connections

In some cases, cable connections are made between IT systems or other technical components that are not intended or authorised. This can cause to security problems or malfunctions.

Such cable connections may allow unauthorised access to data networks, IT systems, information, or applications. Unauthorised cable connections can also transmit information to the wrong recipients. The connection can be disrupted, as well.

2.9. Impairment of Lines

The electrical signal transmission in communication cables can be negatively affected by electrical and magnetic fields. A special form of this line interference is crosstalk. In this case, currents and voltages from nearby lines are transmitted to a communication cable as interference signals.

2.10. Eavesdropping and Manipulation of Cables

Eavesdropping attacks on data cables are an information security risk that should not be ignored. In principle, there is no such thing as a cable impervious to eavesdropping. Cables differ in quality only with regard to the effort required to tap them. Whether a cable is actually being tapped can only be determined using sophisticated instruments.

In addition, deliberate manipulation of cables (which can include their outright destruction) poses a danger to the organisation in question. Malfunctions of cables can be caused with manipulative intent. Such manipulations often aim to disrupt IT operations or damage a particular organisation.

3. Requirements

The specific requirements of module INF.12 *Cabling* are listed below. As a matter of principle, the Process Owner is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the

implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibilities	Roles
Overall responsibility	Process Owner
Further responsibilities	IT Operation Department, Building Services

3.1. Basic Requirements

For module INF.12 *Cabling*, the following requirements MUST be met as a matter of priority:

INF.12.A1 Selection of Appropriate Cable Types [IT Operation Department, Building Services] (B)

When selecting cable types, the necessary transmission features MUST be checked. The relevant standards and regulations MUST be observed. The environmental conditions present during operation and installation MUST also be taken into account. With regard to environmental conditions, the following factors MUST be considered:

- temperatures
- cable paths
- tensile forces during installation
- type of installation
- distance between end points and possible sources of interference

INF.12.A2 Planning Cable Routing [IT Operation Department, Building Services] (B)

Cables, cable routes, and cable trays MUST be dimensioned adequately from both a functional and a physical perspective. In this respect, future requirements MUST also be taken into account, such as sufficient space for possible technical expansions in cable channels and trays. When routing IT and power cabling together in a tray, crosstalk MUST also be prevented among the individual cables. Care MUST be taken to ensure that IT cabling and electrical cabling are routed with the amount of separation specified in the relevant standards. Cables MUST be routed to avoid identifiable sources of risk.

INF.12.A3 Proper Installation [IT Operation Department, Building Services] (B)

Installation work on cabling MUST be carried out competently and carefully. All the relevant standards MUST be observed during installation. A person with corresponding expertise MUST check that cabling is installed properly at all stages. Whether the right cables and connection components have been delivered MUST be checked at the time of delivery. Care MUST be taken to ensure that the installation does not cause any damage. In addition, the cable routes MUST be chosen in a way that prevents the installed cables from being damaged by normal use of the surrounding building.

INF.12.A4 EMC-Compliant Power Supply [Building Services] (B)

The power supply at hand MUST be EMC (electromagnetic compatibility) compliant. To this end, the corresponding power distribution network MUST be designed as a TN-S system. When setting up and operating the power distribution network, the separation distances recommended in the relevant standards MUST be observed to the greatest extent possible. Precautions MUST be taken against external irradiation, power line emissions, and detection of transient currents.

3.2. Standard Requirements

For module INF.12 IT *Cabling*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

INF.12.A5 Requirements Analysis for Cabling [IT Operation Department, Building Services] (S)

As a general rule, the requirements that may affect the economic efficiency of a cabling installation and its ability to meet all current and future requirements SHOULD be analysed. This requirements analysis SHOULD initially project how the cabling will be used within the organisation in question in the short term. On this basis, estimates SHOULD be made as to how usage might evolve over the longer term. Furthermore, the security objectives of availability, integrity, and confidentiality MUST also be taken into consideration during requirements analysis for cabling.

INF.12.A6 Cabling Approval [IT Operation Department, Building Services] (S)

There SHOULD be an approval process for cabling. Cabling SHOULD always be approved only after all the tasks at hand (possibly within the framework of a milestone) have been completed. The party responsible for its installation SHOULD have reported the tasks as completed and ready for approval. In addition, inspections by the client SHOULD not have revealed any unacceptable defects. The approval date SHOULD be selected so that there is enough time in advance to prepare for the approval inspections. The contractor involved MUST provide written evidence of compliance with all the applicable standards and regulations no later than the approval date. The actual scope of the services rendered MUST be verified during the approval process. A checklist SHOULD be drawn up for the approval report. The approval report MUST be signed in a legally binding manner by the participants and all the persons in charge. The report MUST be part of the internal documentation of cabling.

INF.12.A7 Overvoltage Protection [Building Services] (S)

Every electrical network SHOULD be protected against overvoltage. For this purpose, a corresponding overvoltage protection concept MUST be created that complies with the applicable standards. Emergency power systems (EPS) and uninterruptible power supplies (UPS) MUST be included in the overvoltage protection concept.

INF.12.A8 Removing and Disabling Cables No Longer Required [IT Operation Department, Building Services] (S)

If power cables are no longer required, they SHOULD be properly and completely removed. After cables have been removed, firestop seals MUST be professionally sealed.

Cables that are currently no longer needed but can be reasonably left in place as a reserve with the existing technology SHOULD be maintained in a serviceable condition. At minimum, such cables MUST be labelled accordingly at their end points.

In principle, an overview of cables that are no longer needed SHOULD be created. The documentation SHOULD show which cables have been removed or disabled.

INF.12.A9 Fire Prevention in Trays [Building Services] (S)

Trays SHOULD be adequately dimensioned. Trays SHOULD have adequate ventilation.

INF.12.A10 Documentation and Labelling of Cabling [IT Operation Department, Building Services] (S)

An organisation SHOULD ensure that it has internal and external documentation for its cabling. The internal documentation MUST include all records on the installation and operation of the cabling. The internal documentation SHOULD be comprehensively produced and maintained in such a way that operations and further development are supported as effectively as possible. The external documentation (labelling of connections to support operations) of the cabling SHOULD be kept as neutral as possible.

Every change in the network SHOULD be documented. An interim or working version of the documentation SHOULD be adapted immediately (i.e. on the same day as a given change). The master documentation MUST be updated no later than four weeks after completion of the respective work. Whether a document management system can be used for the documentation SHOULD be checked. The documentation SHOULD be reviewed and updated regularly. All technical equipment documented within the scope of cabling MUST be checked with regard to documentation compliance after four years at the latest.

INF.12.A11 Neutral Documentation in Distributors [IT Operation Department, Building Services] (S)

There SHOULD be documentation in every distributor that reflects the current marshalling and line assignments. The documentation in the distributor MUST enable safe switching.

The documentation in the distributor SHOULD be kept as neutral as possible. The documentation in the distributor SHOULD only list existing and used connections and accumulating reserve cables. If possible, no references to the way cables are used SHOULD be given. References SHOULD be limited to those that are expressly prescribed. All further information SHOULD be provided in review documentation.

INF.12.A12 Inspection of Electrical Installations and Existing Connections [IT Operation Department, Building Services] (S)

All electrical installations and equipment SHOULD be inspected regularly according to DGUV Vorschrift 3 [DGUV Regulation 3] in line with the implementation instructions mentioned in section 5, "Tests". Any irregularities detected MUST be documented immediately. Any

irregularities detected MUST also be reported immediately to the responsible organisational units. The responsible organisational units MUST remedy the detected irregularities promptly enough to ensure there is no threat to people. The availability of the electrical installations and equipment MUST be ensured to the extent they are required.

INF.12.A13 Avoidance of Electrical Ignition Sources [Building Services] (S)

The use of electrical appliances and equipment intended for private use SHOULD be clearly regulated within an organisation. All electrical equipment MUST be tested and deemed safe by a qualified electrician before it is used. The use of power strips SHOULD be avoided whenever possible. If additional sockets are required, they SHOULD be professionally retrofitted by a qualified electrician.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.12 *Cabling* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

INF.12.A14 A-B Supply [Building Services] (B)

Instead of a single-line power supply, a two-line A-B supply SHOULD be considered to supply important IT components and other consumers. The functionality of the power supply SHOULD be continuously monitored by suitable technical equipment.

INF.12.A15 Material Protection of Cabling [IT Operation Department, Building Services] (H)

Consideration SHOULD be given to securing cables and distributors against unauthorised access in all rooms of a building, especially in rooms frequented by the public and in areas that are difficult to see. In any case, the number and extent of places where power supply equipment and data network access points are accessible to unauthorised persons SHOULD be minimised.

INF.12.A16 Use of Cabinet Systems [Building Services] (H)

Electrical connections and distributors SHOULD be placed or built into cabinet systems. The dimensioning of the cabinet systems SHOULD take into account the growth expected for the planned period of use.

INF.12.A17 Redundancies for IT Cabling [IT Operation Department] (H)

Consideration SHOULD be given to creating redundant primary IT cabling that is routed through independent trays. Whether or not redundant connections to IT or telecommunication providers should be installed SHOULD also be examined. In case of high or very high availability requirements, consideration SHOULD be given to installing redundant secondary and tertiary cabling in the relevant buildings. Redundantly designed parts of the secondary cabling SHOULD be routed through different fire zones. If redundant cabling is used, its proper functioning SHOULD be checked at regular intervals.

4. Additional Information

4.1. Useful Resources

The German Institute for Standardisation (DIN) publishes specifications that apply to cabling. The following standards are relevant in this regard:

- DIN 4102, "Fire Behaviour of Building Materials and Elements"
- DIN IEC 60364, "Erection of Low-Voltage Installations"
- IEC 62305, Lightning Protection Standard DIN EN 62305 / VE 01805-305:2006
- IN VDE 0100, "Erection of Low-Voltage Installations"
- DIN VDE 0105-100, "Operation of Electrical Installations"
- DIN 41494-8, "Mechanical Structures for Electronic Equipment"
- DIN EN 50173, "Information Technology – Generic Cabling Systems"
- DIN EN 50174, "Information Technology – Cabling Installation"
- DIN EN 50310:2017-02, "Telecommunications Bonding Networks for Buildings and Other Structures"
- DIN EN 50346:2010-02, "Information Technology – Cabling Installation – Testing of Installed Cabling"
- DIN IEC 60297, "Mechanical Structures for Electrical and Electronic Equipment"

The German Social Accident Insurance Institution for the health and welfare services (BGW) has published further regulations for electrical cabling in DGUV Regulation 3, “Electrical Installations and Equipment, Accident Prevention Regulation”.

The International Organization for Standardization (ISO) provides guidelines for IT cabling in the standard ISO/IEC 11801:2002-09, “Information Technology – Generic Cabling for Customer Premises”.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module INF.12 *Cabling*.

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.8 Failure or Disruption of the Power Supply

G 0.9 Failure or Disruption of Communication Networks

G 0.12 Electromagnetic Interference

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.21 Manipulation of Hardware or Software

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.37 Repudiation of Actions

G 0.41 Sabotage

Federal Office
for Information Security

INF.13 Technical Building Management (TBM)

1. Description

1.1. Introduction

Facility management (FM), which is also known as building management, is responsible for all services that arise in the planning and utilisation phases of buildings, building complexes, properties, or property portfolios. The term "building" is used in this module as a blanket term. Exceptions to this are highlighted explicitly.

FM focuses on specific sites and objects. It can be subdivided into technical, infrastructural, and commercial FM.

According to DIN 32736, technical building management (TBM) comprises all services that maintain the technical function and availability of a building. These services include, among others:

- Operational management
- Documentation
- Energy and environmental management
- Information management
- Modernisation
- Refurbishment
- Conversion
- Monitoring of technical warranties

The fundamental technical functions of a building are provided by its building services, which are operated, maintained and further developed by TBM. According to VDI 4700 Sheet 1, building services comprise all the technical and use-specific equipment installed in a building and connected to it, as well as technical equipment in outdoor facilities and fittings (see also section 4.1, *TBM-Specific Terminology Used*). If building services are to be automated and

applied across trades, additional technical infrastructure for building automation and control systems (BACS) is used. BACS is thus a central tool of TBM. A building can also be operated by TBM without BACS, but BACS is always supported by TBM. Certain components of BACS, such as real-time-capable industrial Ethernet switches, can also be attributed to building services.

While building services in the past were usually operated independently of IT and process control and automation technology (operational technology, OT), network transitions are increasingly being established to these areas today. In addition, aspects of building services are used around the clock. Therefore, changes often have to be carried out parallel to productive use.

The basic values of information security must also be taken into account in TBM because the loss of system availability, confidentiality, and integrity can have far-reaching effects in TBM, even to the point of dangers to life and limb.

1.2. Objective

The objective of this module is to establish information security as an integral component of planning, implementation, and operation within the framework of TBM.

1.3. Scoping and Modelling

INF.13 *Technical Building Management (TBM)* is to be applied to every organisation's TBM as soon as buildings with building services are planned, constructed, or operated.

This module encompasses the tasks and processes required for the planning and operation of building services systems (see section 4.1, *TBM-Specific Terminology Used*). Technical infrastructure for the automated operation of buildings is dealt with in module INF.14 *Building Automation and Control Systems (BACS)*. This module must be applied in addition to INF.13 *Technical Building Management (TBM)* if the building services to be operated are automated and controlled across all systems. In this sense, TBM also includes BACS processes.

Furthermore, it is possible that the systems to be managed also include those that are modelled by modules from the IND *Industrial IT* and SYS *IT Systems* layers (e.g. IND.2.1 *General ICS Components* or SYS.4.4 *General IoT Devices*). The aspects of the ORP and OPS layers that are relevant to TBM must also be taken into account, in particular the sub-layers OPS.1 *In-house Operation* and OPS.2 *Operation through Third Parties*, as well as the modules ORP.2 *Personnel* and ORP.4 *Identity and Access Management*. If cloud services are used for TBM, module OPS.2.2 *Cloud Usage* must be taken into account for the selection of these services.

The modules OPS.1.2.5 *Remote Maintenance* and IND.3.2 *Remote Maintenance in Industry* must be used to secure remote access in TBM.

INF.13 *Technical Building Management (TBM)* does not deal with the physical safety of buildings; this is dealt with in module INF.1 *Generic Building*. Similarly, the aspect of safety does not play a prominent role in this module, but is covered in module IND.2.7 *Safety Instrumented Systems*.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module INF.13 *Technical Building Management (TBM)* the following specific threats and vulnerabilities are of particular importance.

2.1. Lack of a Basis for Planning TBM

If the demand organisations (see section 4.1, *TBM-Specific Terminology Used*) have not yet been determined when a building is being constructed, the contact persons, objectives, and needs pertaining to TBM will not be available. This can lead to a situation where the TBM in operation does not correspond to the actual demand because this could not be ascertained at the time of planning and implementation.

2.2. Lack of Documentation in TBM

The number of service providers involved in TBM is often large. If the documentation of responsibilities with contact persons and associated SLAs is incomplete or not accessible, this leads to avoidable delays when important systems fail, which may even result in personal injury.

A lack of documentation of the security certifications of building services systems, including dates for necessary renewals, can lead to expired certifications not being renewed in time. This can result in violations of the law, danger to life and limb depending on the building services system in question, and damages not being settled via the appropriate insurance policies.

2.3. Compromised Interfaces with TBM

TBM has technical interfaces to areas requiring special protection, such as safety instrumented systems (SIS), security services, and fire alarm systems. If these interfaces are compromised intentionally or unintentionally due to errors in TBM, this can result in legal violations and dangers to life and limb.

For example, if a visual or audible warning is overridden in the event of a fire alarm in a data centre, people in the room will not be able to leave before the room is flooded with extinguishing gas. Similarly, a false fire alarm can lead to escape doors being opened (allowing unauthorised access) or doors being closed (which may trap people inside).

2.4. Inadequate Monitoring of Building Services

If building services are insufficiently monitored, safety-relevant events such as corresponding malfunctions in building services may be detected too late (or not at all). Depending on the event, this can lead to further damage or danger to life and limb.

If, for example, a heating system failure is not reported when the outside temperature is below zero, the rooms affected will cool down considerably before the failure is noticed and remedial action can be taken.

2.5. Insufficient Role and Authorisation Management

If TBM or individual parts thereof are physically separated from the rest of an organisation's IT, a dedicated user and authorisation management system is usually also set up. If this is inadequately designed and implemented, the possibility of several employees using the same user account or the organisation failing to delete the authorisations of departed internal or external employees or service providers cannot be ruled out. This could allow TBM to be accessed without authorisation.

3. Requirements

The specific requirements of module INF.13 *Technical Building Management (TBM)* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	Building Services
Further responsibilities	Planner, IT Operation Department, Top Management

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

INF.13.A1 Assessment of the Current Situation When Taking Over Existing Buildings (B)

When existing buildings are taken over, the installed building services systems, building fabric and equipment, and existing documentation MUST be recorded and assessed with regard to their condition (age, support status, future viability, completeness of documentation, etc).

INF.13.A2 Regulation and Documentation of Responsibilities and Authorities in the Building [Top Management, Planner] (B)

Since there are usually different responsibilities and authorities for different areas in a building, the corresponding rights, duties, tasks, competencies, and related processes MUST be regulated and documented.

In this context, the organisational structures in the building MUST also be considered and documented. In particular, all demand and operator organisations MUST be recorded. If TBM is carried out by an external operator organisation, the associated rights, duties, tasks, and competencies MUST be governed by a contract in accordance with module OPS 2.1 *Outsourcing for Customers*.

Furthermore, the interfaces and reporting channels—including for escalation—among all the parties involved MUST be defined and documented. The coordination of different operator organisations MUST also be regulated and documented.

Access to the documentation MUST be regulated. All documentation, including the associated contact information, MUST always be up to date and available.

INF.13.A3 Documentation of Building Facilities (B)

All the building facilities pertaining to building services and BACS MUST be documented. Any existing documentation MUST be merged, organised from the perspective of TBM, and supplemented with TBM-specific information.

Access to the documentation MUST be regulated. All documentation, including the associated contact information, MUST always be up to date and available.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

INF.13.A4 Creation of a Security Policy for TBM (S)

Based on an organisation's general information security policy, an overall security policy for TBM SHOULD be established and implemented in a comprehensible way. Specific security policies for the different subject areas of TBM SHOULD be derived from this overall security policy. The security policy for TBM SHOULD comprehensibly describe requirements and specifications on how TBM is implemented. The security policy SHOULD be reviewed both regularly and whenever required and updated as necessary to reflect the current state of the art and include the latest findings. It SHOULD be known to all employees responsible for TBM and be integral to their work.

INF.13.A5 Planning TBM (S) [Planer]

TBM, the underlying infrastructure, and the associated processes SHOULD be planned appropriately. This planning SHOULD at least include a detailed requirements analysis and a sufficient rough conceptual design, along with detailed and implementation planning.

The requirements analysis SHOULD specify requirements for TBM infrastructure and TBM processes. Here, all the essential elements of TBM SHOULD be taken into account. The security policy for TBM SHOULD also be considered. If the demand organisation in question has not yet been defined at the time of planning, basic requirements in line with the current state of the art SHOULD be established at minimum in the context of universal planning.

For the requirements specification, the interfaces of the systems to be managed SHOULD also be documented (e.g. to ensure the compatibility of the TBM solution and the systems to be managed).

In addition, before commissioning service providers or purchasing hardware or software for the systems to be managed by TBM, the TBM requirements SHOULD be specified in a TBM requirements specification. This specification SHOULD also take into account the performance of tests (see also INF.13.A22 *Performing System Tests in TBM*).

If artificial intelligence (AI) functions are used in TBM, the responsible manufacturer SHOULD be asked whether and how information security is adequately taken into account in this regard.

The rough conceptual design SHOULD be carried out according to INF.13.A6 *Drawing Up a TBM Concept*.

The detailed and implementation planning for TBM SHOULD take into account all the points addressed in the security guideline and the TBM concept.

INF.13.A6 Drawing Up a TBM Concept (S) [Planner]

Based on the security policy drawn up for TBM, a TBM concept SHOULD be established and consistently maintained. In doing so, the following minimum aspects SHOULD be taken into account as required:

- Methods, techniques, and tools for TBM
- Protection of access and communication
- Protection at the network level; in particular, the assignment of TBM components to network segments
- Scope of monitoring and alerts
- Logging of events and administrative access
- Reporting chains in the event of malfunctions and security incidents
- Processes required for TBM
- Provisioning of TBM information for other areas of the organisation
- Integration of TBM into contingency planning

The TBM concept SHOULD be reviewed both regularly and whenever required and updated as necessary to reflect the current state of the art and include new findings.

In addition, a gap analysis of the specifications of the concept and the current state SHOULD be carried out on a regular basis. In particular, whether the systems are configured according to the specifications SHOULD be checked. The results SHOULD be documented in a transparent manner. Deviations SHOULD be eliminated.

INF.13.A7 Creating a Radio Frequency Register (S)

To enable an organisation to use radio frequencies with as little interference as possible, a radio frequency register SHOULD be created that lists the systems and users of the frequency spectrum at the organisation's sites. If frequencies could potentially be used by different systems and users, the primary user SHOULD be established for each frequency. This SHOULD be coordinated between IT and TBM. If OT is used in buildings, this SHOULD also be coordinated.

The radio frequency register SHOULD be reviewed both regularly and whenever required and updated if necessary.

INF.13.A8 Creation and Maintenance of an Inventory for TBM (S) [Planner]

An inventory SHOULD be created and maintained for the documentation of systems managed by TBM. The inventory SHOULD be kept complete and up to date. The inventory SHOULD show responsibilities and authorities for all systems.

The elements of the TBM infrastructure itself SHOULD also be documented.

INF.13.A9 Regulation of the Use of Computer-Aided Facility Management (S) [Planner]

If a computer-aided facility management (CAFM) system is used, its use SHOULD be comprehensively planned and designed. If processes are mapped and supported in CAFM, appropriate roles and authorisations SHOULD be defined, especially if external service providers are involved in the processes.

INF.13.A10 Regulation of the Use of Building Information Modelling (S) [Planner]

Building information modelling (BIM) SHOULD be used whenever possible for the digital modelling of all relevant building data. When using BIM, the BIM project delivery plan SHOULD be specified.

Furthermore, the BIM architecture SHOULD be comprehensively planned and designed. Information security SHOULD also be adequately ensured for BIM tools.

INF.13.A11 Adequate Hardening of Systems in TBM (S)

All systems in TBM and the systems operated by TBM SHOULD be adequately hardened. These hardening measures SHOULD be documented, reviewed both regularly and whenever required, and adjusted if necessary.

For all systems in TBM and the systems operated by TBM, it SHOULD be ensured during procurement that they can be hardened appropriately and, in particular, that security-relevant updates will be provided for the systems' planned service life.

Systems that do not receive security-relevant updates SHOULD not be used if corresponding vulnerabilities are exposed. If this is not possible, the affected systems SHOULD be separated by network segmentation and their communication controlled and regulated.

INF.13.A12 Secure Configuration of TBM Systems (S)

All systems in TBM and systems operated by TBM SHOULD be configured securely.

At minimum, these configurations SHOULD be tested before a system is put into operation. Configuration changes during productive operations SHOULD be tested on a test instance before activation or only carried out according to the principle of dual control.

The configuration of systems SHOULD be backed up to enable quick re-installation of an error-free version (rollback). Rollback tests SHOULD be set up on a test system or performed during maintenance windows. The configurations SHOULD be stored centrally.

Automated distribution of software updates and configurations SHOULD be set up for similar systems, including devices at the automation and field level (see section 4.1, *TBM-Specific Terminology Used*).

Configuration changes SHOULD be made known to all the parties involved in operational and service processes (fault clearance, on-call service, maintenance, etc). In particular, these include:

- Changes to access mechanisms or passwords
- Changes to communication and control parameters for integrated systems

In the event of a malfunction, it SHOULD be ensured that a maintenance technician can operate or parameterise the system affected (for example).

Furthermore, whether systems are configured according to the corresponding specifications SHOULD be checked both regularly and whenever required. The results SHOULD be documented in a transparent manner. Deviations from the specifications SHOULD be corrected.

INF.13.A13 Secure Connection of Restricted Trusted Systems in TBM (S) [Planner]

Systems with limited trustworthiness that need to be integrated into TBM for important operational reasons SHOULD be connected via a system that controls and regulates their communication by means of firewall functions. This system SHOULD be the responsibility of TBM.

INF.13.A14 Consideration of Special Roles and Authorisations in TBM (S)

The TBM role and authorisation concept at hand SHOULD take into account both the demand organisations and the operator organisations of TBM systems and building services systems. This SHOULD be carefully planned, especially if TBM is provided across the entire organisation in question.

INF.13.A15 Protection Against Malware in TBM (S)

If anti-virus programs cannot be run on a system in line with module OPS.1.1.4 *Protection Against Malware*—for example due to resource constraints or real-time requirements—appropriate alternative protection methods SHOULD be used.

Each external system and storage medium SHOULD be checked for malware before being connected to a TBM system or transferring data.

INF.13.A16 Process for Changes in TBM (S)

Changes SHOULD always be announced and agreed with all the trades (see section 4.1, *TBM-Specific Terminology Used*) and operator and demand organisations involved. In addition, provisions SHOULD be made for the event that rolling back flawed changes is not possible, or only possible with a great deal of effort. Therefore, tests should be carried out in change management before a change is executed, including on the possibility of rolling back the change. The respective depth of testing SHOULD be determined for the different types of changes. A correspondingly high depth of testing SHOULD be provided for the introduction of

new systems and for major changes to existing systems (see INF.13.A22 *Performing System Tests in TBM*).

INF.13.A17 Provisions for Maintenance and Repairs in TBM (S)

Building facilities SHOULD be maintained at regular intervals. A maintenance schedule SHOULD be drawn up for this purpose. The security aspects to be observed during maintenance and repair work SHOULD be regulated. The interdependencies of different trades SHOULD also be taken into account. The persons responsible for the maintenance or repair of facilities SHOULD also be specified. The maintenance tasks carried out SHOULD be documented.

It SHOULD be ensured at all times that maintenance and repair work carried out by third parties is monitored, only carried out in a coordinated manner, and approved upon completion. For this purpose, internal Building Services employees SHOULD be designated to authorise and observe maintenance and repair work, support it if necessary, and approve it upon completion.

INF.13.A18 Proactive Maintenance in TBM (S) [Planner]

Appropriate proactive maintenance SHOULD be carried out for systems managed by TBM. For this purpose, regular maintenance intervals SHOULD be defined for each system. Whether predictive maintenance can be used in addition to regular maintenance SHOULD also be considered for each system, along with the extent to which the regular maintenance intervals can be extended as a result.

INF.13.A19 Conceptualisation and Implementation of Monitoring in TBM (S) [Planner]

A concept for monitoring in TBM SHOULD be developed and implemented. This SHOULD specify how the systems to be managed by TBM can be integrated into a monitoring system that is as uniform as possible and which values should be monitored. For this purpose, the necessary interfaces for monitoring important states of systems that are managed by TBM SHOULD be specified during a requirements analysis. In addition, the systems used for TBM SHOULD be integrated into the monitoring.

The concept SHOULD be reviewed both regularly and whenever required and updated as necessary to reflect the current state of the art and include the latest findings.

Status messages or monitoring data SHOULD ONLY be transmitted using secure communication channels.

INF.13.A20 Provisions for Event Management in TBM (S) [Planner]

Events that occur in TBM SHOULD be categorised, filtered, and classified with regard to their significance and influence. Threshold values SHOULD be defined for such events to enable their automated classification. Depending on the classification of the events, appropriate measures for monitoring, alerting, and reporting channels (escalation) SHOULD be defined along with measures for logging.

INF.13.A21 Logging in TBM (S)

Events that have been appropriately classified in event management SHOULD be logged. In addition, events relevant to the security of the systems at hand SHOULD be logged.

All attempts to access configurations and all instances of manual and automated control access SHOULD be logged. Depending on the level of protection required, full logging (including metadata and the content of changes) SHOULD take place.

Logging SHOULD be consolidated on a central logging instance.

Logging data SHOULD ONLY be transmitted using secure communication channels.

In case of security-critical events, alarms SHOULD be raised automatically.

INF.13.A22 Performing System Tests in TBM (S) [Planner]

TBM systems and systems managed by TBM SHOULD be tested with regard to their functional and non-functional requirements before they are put into operation and whenever major system changes are made. This SHOULD include checking of the target and actual behaviour of functions and settings. For non-functional requirements, information security requirements SHOULD also be tested and additional load tests should be performed if required. A specification containing a description of the test environment, the test depth, and the test cases (including the criteria for a successfully completed test) SHOULD be created for the tests. The completion of tests SHOULD be documented in a test report.

The test specification SHOULD be reviewed both regularly and whenever required and updated as necessary to reflect the current state of the art and include the latest findings.

INF.13.A23 Integration of TBM into Vulnerability Management (S)

TBM systems and systems managed by TBM SHOULD be continuously monitored for possible vulnerabilities.

For this purpose, information on vulnerabilities that have become known SHOULD be obtained regularly and taken into account accordingly. This SHOULD include a review of the configuration of the systems at hand to determine whether it offers a favourable environment to known vulnerabilities.

Furthermore, it SHOULD be decided for which systems vulnerability scans should be carried out regularly, or at least when the systems are put into operation and in case of major system changes. For vulnerability scans, the scan depth SHOULD be specified. Whether a passive or an active scan is to be performed SHOULD also be specified. In production environments, passive scans SHOULD be preferred. Active scans SHOULD only be performed in production environments if they are necessary and personnel are called in to resolve any errors or failures that may occur as a result of the scan.

INF.13.A24 Ensuring Control of Cloud-Based Processes for TBM (S) [Planner]

If cloud-based services are used in TBM, control of all TBM processes SHOULD remain in the TBM system. This SHOULD be included in the terms of a corresponding contract when using a service from a cloud provider.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

INF.13.A25 Establishment of a Test Environment for TBM (H) [Planner]

In case of increased protection needs, a test environment SHOULD be set up for TBM systems and those managed by TBM. This makes it possible to test hardware and software before they are put into operation and in case of changes, and to reduce errors in productive operation. In addition, provisions SHOULD be specified for dealing with systems for which a test environment cannot be established.

INF.13.A26 Securing BIM (H) [Planner]

If security-critical information is also captured in BIM, appropriate security and hardening measures SHOULD be provided both at the level of the BIM architecture and for the implementation and operation of the BIM solution. The protection SHOULD include a tightened role and authorisation concept and more advanced protection measures such as encryption, segmentation, and higher level authentication mechanisms (in particular, two-factor authentication).

INF.13.A27 Establishment of a Private Cloud for TBM (H) [Planner]

For higher protection needs, cloud services related to TBM SHOULD be located in a private on-premise cloud or a private cloud with a trusted cloud provider. The use of a public cloud SHOULD be avoided.

INF.13.A28 Secure Use of Artificial intelligence in TBM (H)

If artificial intelligence (AI) functions are used in TBM when there is an increased need for protection, only AI that is demonstrably secure SHOULD be used. At the very least, care SHOULD be taken to ensure that no data is routed to networks that do not belong to the organisation in question or are not trustworthy.

For cloud-based AI services, the criteria of the BSI AI Cloud Service Compliance Criteria Catalogue (AIC4) SHOULD be considered in addition to the requirements of module OPS.2.2 *Cloud Usage*.

INF.13.A29 Integration of TBM into SIEM (H) [IT Operation Department]

If a system is used for security information and event management (SIEM), the TBM systems and, where possible, the systems managed by TBM SHOULD be integrated accordingly in order to be able to detect and analyse security incidents across systems and applications.

INF.13.A30 Performing Penetration Tests in TBM (H)

Penetration tests SHOULD be carried out as needed to adequately secure TBM systems and systems managed by TBM. At minimum, penetration tests SHOULD be carried out in a test environment before productive operation and in case of major system changes.

If AI functions are used in TBM, these SHOULD be included in the penetration tests.

4. Additional Information

4.1. TBM-Specific Terminology Used

Automation level

The automation level is located between the field level and the management level in the automation pyramid. It brings together the data supplied by the field level and the specifications handed down by the management level. This is where the control and regulation of building services systems takes place, but also the monitoring of thresholds, switching states, and meter readings.

Building

This term is used synonymously to refer to buildings, building complexes, properties, and property portfolios in module INF.13 *Technical Building Management (TBM)* and the associated Implementation Guidance. Furthermore, the term “building” describes not only houses and halls, but structures like television towers or oil rigs, as well.

Building automation and control systems (BACS)

According to VDI 3814-1, building automation and control systems (BACS) comprise all products and services designed for the target-oriented operation of building services.

Building complex

A building complex is a group of buildings that are structurally connected to each other and are perceived as an overall unit.

Building information modelling (BIM)

According to VDI 2552 Sheet 2, BIM is a methodology for the planning, execution, and operation of buildings in a collaborative approach based on a digital information model.

Building services (BS)

According to VDI 4700 Sheet 1, building services (BS) include all technical facilities and use-specific facilities installed in a building and those connected to them, as well as technical facilities in outdoor facilities and equipment. Certain components of BACS can also be attributed to building services, such as real-time-capable industrial Ethernet switches.

Building services system

A building services system describes the totality of all technical components that interact to fulfil certain functions. According to DIN 276 (“Building costs”), examples include heating systems, ventilation systems, and lighting systems.

Computer-aided facility management (CAFM)

According to VDI 3814 Sheet 2.1, CAFM serves as a tool for collecting, processing, preparing, and archiving data and information with the aim of supporting the operating processes and tasks in the operational phase of a building.

Control centre

A control centre (along with operating and observation units) is a technical tool for visualising current processes, states, and situations of processes, including TBM and especially BACS processes.

Demand organisation

According to DIN EN ISO 41011, a demand organisation is an organisational unit within or outside a given organisation that is authorised to make demands of building services, BACS, or TBM for its requirements and to bear the costs of meeting these demands.

Examples: a tenant within a building, an owner of a building, or a service provider within an organisation, such as a canteen.

Field level

The field level represents the lowest level of the automation pyramid and comprises different components of BACS or OT. As a rule, sensors and actuators are operated here. Sensors record information (e.g. movement, brightness, temperature) and send it to the automation level. Actuators receive control information and convert it into switching signals (e.g. for lighting, heating, air conditioning and ventilation systems).

Property

A property comprises a plot of land and the building(s) developed on it. This development includes all immovable property—that is, buildings and other things that cannot be easily removed from the land.

Property portfolio

A property portfolio is the totality of the properties owned by a given entity.

System

In module INF.13 *Technical Building Management (TBM)* and the associated Implementation Guidance, this term not only refers to an IT system in the traditional sense (cf. modules of the SYS layer), but also includes all BACS components, including all field-level components (such as sensors and actuators).

Technical Building Management (TBM)

According to DIN 32736, Technical Building Management (TBM) comprises all services that maintain the technical function and availability of a building. TBM thus takes over the operation, maintenance, modernisation, and documentation of components for building services and defines all the necessary processes.

Trade

In construction, a trade generally comprises the work that can be assigned to a self-contained construction service area. It is a functional area that can include, in particular, various building services systems.

Example: air-conditioning systems (cost group 430 in DIN 276), which include ventilation systems, air-conditioning systems, and refrigeration systems.

4.2. Abbreviations

Abbreviation	Meaning
AI	Artificial intelligence
AIC4	AI Cloud Service Compliance Criteria Catalogue
BACS	Building automation and control systems
BIM	Building information modelling
BM	Building management
BS	Building services
BSI	Federal Office for Information Security
CAFM	Computer-aided facility management
CISO	Chief Information Security Officer
CRT	Cross-reference table
DIN	*Deutsches Institut für Normung* (German Institute for Standardization)
ICS	Industrial control system
IT	Information technology
OT	Operational technology
SIEM	Security information and event management
SIS	Safety instrumented systems
SLA	Service level agreement
TBM	Technical Building Management
VDI	*Verein Deutscher Ingenieure* [Association of German Engineers]

4.3. Useful Resources

Standards and documents cited:

- AI Cloud Service Compliance Criteria Catalogue (AIC4), Federal Office for Information Security, February 2021, available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/AIC4/AI-Cloud-Service-Compliance-Criteria-Catalogue_AIC4.html
- BSI-CS 108—Remote Maintenance in Industry, BSI publication on cyber security, July 2018, available at https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf
- DIN 276—Building Costs, German Institute for Standardization (DIN), December 2018, available from Beuth-Verlag
- DIN 32736—Facility management—Terminology and scope of services, German Institute for Standardization (DIN), August 2000, available from Beuth-Verlag
- VDI 4700 Sheet 1—Terminology of civil engineering and building services, The Association of German Engineers (VDI), October 2015, available from Beuth-Verlag

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module INF.13 *Technical Building Management (TBM)*:

G 0.9 Failure or Disruption of Communication Networks

G 0.10 Failure or Disruption of Supply Networks

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.41 Sabotage

G 0.43 Attack with Specially Crafted Messages

G 0.44 Unauthorised Entry to Premises

G 0.47 Harmful Side Effects of IT-Supported Attacks

Federal Office
for Information Security

INF.14 Building Automation and Control Systems (BACS)

1. Description

1.1. Introduction

Building automation and control systems (BACS) automate the operation of buildings fully or partially across all trades and provide the technical infrastructure for this purpose. The fundamental technical functions of a building are provided by its building services, which are operated, maintained, and developed further by Technical Building Management (TBM) services. BACS are thus a central tool of TBM for implementing the operating objectives set for a given building. They include all the products and services involved in the automated operation of building services across various areas. Some of the criteria followed in setting related objectives might include functionality, energy efficiency and sustainability, security, availability, or convenience. BACS can be scaled to services for buildings, building complexes, properties, or property portfolios. In this module, the general term “building” is used to refer to all these things. Any exceptions to this are explicitly cited.

Among other things, BACS perform automation tasks such as automated measurement, control, and regulation, as well as tasks for the monitoring, service and diagnosis, optimisation, operation, and management of building services.

Within a given building, BACS are provided for one or several demand organisations (e.g. tenants). For this purpose, building services are usually controlled separately for different BACS areas—for example, for demand organisations or parts of a building.

In a building, BACS can be implemented by several parallel BACS depending on the building services used. A BACS represents the technical implementation of building automation and control and can also be used for several buildings within a building complex or a property. Different BACS can cooperate, but can also be operated completely independently of each other.

Whereas building services were often not universally automated in the past, BACS are now increasingly being used for overarching control of building services across trades. For this

purpose, technologies are being employed more and more often that were originally only used in information technology (IT) and industrial process control and automation technology (operational technology, OT)—communication via the Internet and cloud services, for instance.

1.2. Objective

The objective of this module is to establish information security as an integral component of the planning, realisation, and operation of BACS.

1.3. Scoping and Modelling

INF.14 *Building Automation and Control Systems (BACS)* must be applied to the BACS of an organisation from the point that the building services in its buildings are controlled by BACS. This module is only applicable to BACS interfaces to building services systems; the interfaces of building services systems to internal networks and network structures are not the focus here.

INF.14 *Building Automation and Control Systems (BACS)* deals with systems and services that must be taken into account when BACS (which may consist of several BACS) are planned, set up, and operated. It also deals with specific conditions that apply to networks and network components of BACS.

The following content is also significant, but dealt with elsewhere:

- The general requirements for BACS and building services, which do not predominantly address aspects for automated measurement, control, and regulation across multiple areas, are dealt with in module INF.13 *Technical Building Management (TBM)*. This module should always be considered along with the present module.
- Requirements for general infrastructure, in particular for buildings and rooms or workplaces, are dealt with in the modules of layer INF Infrastructure (e.g. module INF.1 *Generic Building*).
- If parts of the BACS an organisation requires are provided by another organisation, such as a service provider in the role of building operator (operator organisation), module OPS.2.1 *Outsourcing for Customers* must be applied to the provision and operation of the BACS.
- Specific requirements for BACS components that can also be used for the area of industrial IT or OT are addressed in the modules of the IND Industrial IT layer (see e.g. module IND.2.3 *Sensors and Actuators* or module IND.2.7 *Safety Instrumented Systems*).
- Module NET.1.1 *Network Architecture and Design* deals with the basic aspects of networks to the extent that they apply not only to office IT, but also to BACS and industrial IT. General requirements for the protection of network components are dealt with in the module group NET.3 *Network Components* (see e.g. module NET.3.1 *Routers and Switches*).
- In addition, all appropriate organisational and technical modules for servers and applications must be applied. For remote access to BACS components, for example, OPS.1.2.5 *Remote Maintenance* must be applied.

- If the networking of buildings is cloud-based, module OPS.2.2 *Cloud Usage* must also be applied.

2. Threat Landscape

Since the IT-Grundschutz modules cannot address individual information domains, typical scenarios are used to demonstrate the threat landscape. For module INF.14 *Building Automation and Control Systems (BACS)*, the following specific threats and vulnerabilities are of particular importance.

2.1. Inadequate Planning of BACS

BACS are used for coordinated control of building services systems across multiple areas. Inadequate planning of BACS can thus lead to damage to property or assets and, in the worst case, to personal injury.

In one example, the central control system of a single access entry control system could fail due to insufficient redundancy planning and people could be trapped in an airlock.

The threat landscape in this regard is also exacerbated in BACS by the complexity of the required planning. Here, heterogeneous groups of building services systems (trades) and the multitude of different service providers and BACS areas have to be taken into account.

2.2. Incorrect Integration of Building Services Systems into BACS

BACS control building services systems across multiple areas. If only one system is integrated incorrectly or inadequately, it can restrict the functionality of all the other BACS.

For example, incoming messages may be misinterpreted or simply not reach the BACS, causing it to react incorrectly or not at all. If information from an access control system is incorrectly received or not received at all, for instance, the heating and sun shading for corresponding rooms may not be controlled appropriately.

2.3. Use of Insecure Systems and Protocols in BACS

The business services systems controlled by BACS often use components that may not receive updates due to their age and thus contain vulnerabilities or no longer correspond to the current state of the art. This often results from substandard development and maintenance processes on the manufacturer side or from software that uses insecure protocols due to a lack of computing and storage capacity.

In addition, manufacturers often fail to provide patches, so that insecure BACS-relevant components are also used over a very long period of time. The risk is increased by the fact that access to such components must also be enabled in BACS.

2.4. Poor Configuration of BACS

Depending on which areas of BACS are affected, incorrect configurations can impair operational processes, allow prohibited physical access to protected areas, and cause harm to systems, buildings, and people.

Consider the following examples:

- Incorrectly configured air conditioning, which can lead to overheating and failure of IT systems or, in some weather conditions, even impair people's health
- Building services systems that are not configured in an integrated way, which can lead to personal injury and system damage if, for example, power and extinguishing systems are not operated in a coordinated manner
- Incorrectly configured access systems, which can lead to personal injury if doors cannot be opened in an emergency

These hazards are particularly relevant for BACS when a lack of opportunities to conduct corresponding testing makes it impossible to detect a faulty configuration before going live. This can also occur in the event of a faulty update or a faulty update process that renders a BACS unusable.

2.5. Manipulation of Interfaces of Stand-Alone Building Services Systems to BACS

Manipulated interfaces between BACS the building services systems to which they are connected can lead to faulty responses in the BACS.

A manipulated message from a fire alarm system can lead to all doors being opened automatically, for example, thus granting unauthorised persons access to a building.

2.6. Inadequately Protected Access to BACS

BACS comprise a large number of components that provide, exchange, and receive information across systems, such as for determining the location of personnel or for room automation. These devices communicate via LAN and WLAN, but also using other wireless technologies such as Bluetooth.

If such network access attempts are not adequately protected, an attacker can use them to carry out DoS attacks. They can also manipulate or sabotage BACS and possibly even access all the rest of the affected organisation's IT. Manipulated BACS can then cause an increase in data volume, even to the point of overloading networks and components. Inadequate access protection can also result in data leaks or the installation of malware.

2.7. Inadequately Secured BACS Control Elements

If easily accessible control elements of BACS are inadequately secured, they can be used to attack such systems. Examples of these elements include wall-mounted control elements or control elements of gatekeepers that can be used to open doors or gates remotely.

If such control elements are inadequately protected, (e.g. due to a lack of authentication), this can enable unauthorised access.

Inadequately protected connections of control elements such as LAN or USB interfaces can also open the door to unauthorised users.

2.8. Inadequately Secured Mobile Communication Connections

Especially at the field and automation level, BACS components are frequently used that are connected to the respective manufacturer or a service provider (e.g. a weather service) via a mobile communication interface. If these interfaces and their communications are insufficiently protected and continuously active, they offer unauthorised users and attackers access to the corresponding BACS network.

3. Requirements

The specific requirements of module INF.14 *Building Automation and Control Systems (BACS)* are listed below. The CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. The CISO must always be involved in strategic decisions.

The IT-Grundschutz Compendium also defines additional roles to which appropriate personnel should be assigned as required.

Responsibilities	**Roles**
Overall responsibility	Building Services
Further responsibilities	Planner, Administrator, IT Operation Department

Exactly one role should have *overall responsibility*. There may also be *further responsibilities*. If one of these additional roles is primarily responsible for the fulfilment of a requirement, this role is listed in square brackets after the heading of the requirement.

3.1. Basic Requirements

For this module, the following requirements MUST be met as a matter of priority.

INF.14.A1 Planning BACS (B) [Planner]

For the trades controlled by BACS, a plan for designing the BACS in a secure manner MUST be established.

BACS MUST be taken into account when planning the new construction, conversion, extension, or refurbishment of a building. BACS MUST therefore be considered in planning and construction processes for all BACS-relevant components and building services systems, including in connection with building information modelling (BIM).

Within the scope of BACS planning, the BACS to be set up MUST be specified. The extent to which building services systems are to be controlled automatically via BACS MUST be specified.

BACS SHOULD be planned in a way that minimises the different BACS, communication protocols, and interfaces used for the coupling and integration of building services systems. Secure and standardised protocols and interfaces SHOULD be used. When taking decisions regarding the necessary systems, protocols, and interfaces, the expected functionality SHOULD be weighed against a potential increase in effort to ensure operational and information security.

The planning SHOULD be documented, reviewed both regularly and whenever required, and adjusted to the state of the art if necessary.

Furthermore, the planning SHOULD be compared against the current configuration both on a regular basis and as required (gap analysis).

INF.14.A2 Defining Commissioning and Interface Management for BACS (B)

Due to the large number of building services systems and building components that are connected in BACS, the commissioning procedure for the building services systems and BACS-relevant components involved MUST be coordinated and defined across the multiple areas at hand. This process MUST be implemented in a coordinated manner to ensure a fully functional building.

Clear interfaces MUST also be defined between the operator organisations of the BACS and the BACS-relevant components, as well as between the operator organisations of the building services systems.

Commissioning and interface management MUST be documented. The specifications MUST be checked and readjusted both regularly and whenever required. In particular, the specifications must be adapted in case of changes within the BACS.

INF.14.A3 Secure Connection of Building Services and Building Services Systems (B)

For all building services systems, BACS, and BACS-relevant components, it MUST be specified whether actions may be triggered by other building services systems, BACS, and BACS-relevant components. If this type of integration is allowed, rules SHOULD be set regarding which automated actions may be triggered by which information from a BACS.

If a building services system is to be coupled with a BACS but cannot or must not be integrated into the BACS, the building services system information to be reported to the BACS MUST be defined.

Both the integration of building services systems into a BACS and the non-reactive coupling of building systems to BACS MUST be adequately secured. The connections between building services systems MUST also be adequately secured.

In particular, the sequence and function chains within or between BACS MUST be adequately planned for this purpose. All transitions between trades and technologies MUST be taken into account.

These process and function chains MUST be comprehensively tested and readjusted in the event of any malfunction.

The specifications MUST be fully documented. The documentation SHOULD be checked both regularly and whenever necessary to ensure that it is still up to date. In case of deviations, the cause MUST be identified and corrected.

INF.14.A4 Consideration of Hazard Detection Systems in BACS (B) [Planner]

Hazard detection systems (including security systems) MUST be coupled to BACS in a non-reactive manner. They MUST NOT be integrated into BACS.

Physically separate network components and physically separate segments MUST be used for the corresponding network connections. If radio networks are used for coupling, the respective building services systems MUST be designated as primary users for the frequency ranges used. Certified mechanisms SHOULD be used for communication via radio networks.

INF.14.A5 Documentation of BACS (B)

The many different components and points of access pertaining to BACS MUST be documented. This documentation MUST be checked and adapted both regularly and in case of changes within the BACS in question.

In particular, all deactivated physical communication interfaces, protocols, and points of access to the BACS MUST be documented. Furthermore, all interactions and dependencies of BACS-relevant components, as well as of building services systems integrated into or coupled with BACS, MUST be documented. The available and utilised security features of the protocols in use SHOULD be documented.

The documentation SHOULD be coordinated for all BACS with regard to their content and data structures.

INF.14.A6 Separation of BACS Networks (B) [Planner, IT Operation Department]

BACS networks MUST be at least logically separated from office networks and other networks of the organisation at hand. Any communication between BACS and other IT systems MUST be controlled and regulated. For this purpose, appropriate components with security functions (a firewall function at minimum) MUST be provided at all the transitions in such segmentation.

If BACS are set up centrally for a building complex or property, the BACS communication across buildings via LAN, WLAN, WAN, radio networks, or Internet connections MUST also be separated at the network level.

3.2. Standard Requirements

Along with the Basic Requirements above, the following requirements correspond to the state-of-the-art technology for this module. They SHOULD be met as a matter of principle.

INF.14.A7 Drawing Up a Security Policy for BACS (S)

Based on the general security information security policy of the organisation in question and its overarching security policy for TBM, the security requirements for all BACS SHOULD be specified in a corresponding security policy. This policy SHOULD be known to all persons involved in planning, procuring, implementing, and operating BACS and be integral to their

work. The contents and implementation of the required policy SHOULD be reviewed regularly and adjusted if necessary, and the results of these reviews SHOULD be documented in a comprehensible manner.

The security policy SHOULD also specify the development and testing requirements for the use of BACS.

INF.14.A8 Requirements Specification for BACS (S)

Based on an organisation's BACS security policy, an overall requirements specification SHOULD be established for the BACS at hand, along with a separate requirements specification for each individual system. From these requirements, it SHOULD be possible to derive all the elements essential for the architecture and design of each BACS and the intercoupling thereof.

The overall requirements specification SHOULD be documented and adapted to the state of the art both on a regular basis and as needed. Furthermore, the implementation of the requirements SHOULD be checked regularly.

Only components that provide authentication (via a changeable user name and password at minimum) SHOULD be used in BACS.

INF.14.A9 Developing a BACS Concept (S)

Based on an organisation's BACS security policy and requirements specifications, an overall concept SHOULD be developed for the BACS at hand. Detailed concepts SHOULD be derived from this overall concept and developed for all BACS. At minimum, the following points SHOULD be adequately considered in these concepts:

- All building services systems integrated into the respective BACS
- All building services systems coupled with the respective BACS
- All BACS-relevant components and their respective communication links

The concepts SHOULD describe all the relevant technical and organisational requirements. The concepts SHOULD be checked regularly and updated if necessary.

INF.14.A10 Formation of Independent BACS Areas (S) [Planner]

In BACS, different BACS areas SHOULD be planned and implemented in a way that minimises dependencies among them and makes it possible to control them independently. A disruption in one BACS area SHOULD have little or no impact on other BACS areas.

In particular, it SHOULD be possible to control the buildings within a building complex or property separately.

Accordingly, the established BACS areas SHOULD also be visible in the BACS management system.

INF.14.A11 Securing Freely Accessible Ports and Access Points in BACS (S) [Planner]

The connection of components (especially unauthorised, unknown components and third-party devices) SHOULD be controlled and restricted, particularly in the case of freely accessible Ethernet ports, USB ports, and other BACS interfaces.

Connections of unauthorised or unknown components SHOULD be included in corresponding event logging. Direct IP-based communication from such components to BACS SHOULD be prevented (see INF.14.A13).

For freely accessible LAN or WLAN connections, network access control in line with IEEE 802.1X or comparable security mechanisms SHOULD be used. This SHOULD include locating insufficiently authenticated and authorised components in separate network segments.

Freely accessible interfaces used for temporary maintenance purposes (such as USB ports on BACS components) SHOULD only be activated when required.

INF.14.A12 Use of Secure Transmission Protocols for BACS (S)

For the configuration, maintenance, and control of BACS-relevant components based on Ethernet and IP, secure protocols SHOULD be used if communication does not take place via trusted network segments.

Outside of trusted network segments, communication via Ethernet and IP between BACS SHOULD be encrypted. Encryption SHOULD be carried out using up-to-date encryption mechanisms.

INF.14.A13 Network Segmentation in BACS (S) [Planner]

Network segmentation SHOULD be implemented within a BACS network in a manner that separates individual BACS, individual building services systems, and individual groups of building services systems within each BACS as required.

Appropriate rules SHOULD be defined for the transitions between the segments and used to implement components with security functions (stateful packet filters at minimum).

INF.14.A14 Use of BACS-Appropriate Access Protection (S)

For BACS, identity and access management in line with module ORP.4 *Identity and Access Management* SHOULD be used that adequately meets the requirements of the BACS at hand. For this purpose, a BACS-internal authentication solution or a suitable replication of a central authentication solution used by the organisation in question SHOULD be implemented in line with the relevant requirements. All BACS-relevant components SHOULD be integrated into the authentication solution whenever possible.

Operators of BACS, operators of building services systems, and demand organisations SHOULD be adequately considered in the corresponding role and access concept with regard to BACS. This SHOULD be carefully planned and coordinated, especially if the BACS are provided across multiple organisations.

All BACS-relevant components, including field-level components and control elements, SHOULD be able to implement suitable functions to secure access. Components that do not

provide access protection or offer access parameters from the manufacturer that cannot be modified SHOULD NOT be used.

INF.14.A15 Security of BACS-Specific Networks (S)

If communication security mechanisms are available in BACS-specific networks such as BACnet, they SHOULD be used. At minimum, mechanisms for authentication and encryption SHOULD be used.

For BACS-specific networks that cannot implement adequate security mechanisms, consideration SHOULD be given to switching them to a BACS-specific network with adequate security mechanisms.

In principle, communication with BACS-specific networks SHOULD be controlled and, if necessary, regulated by coupling elements with security functions.

INF.14.A16 Securing Wireless Communication in BACS Networks (S) [Planner]

In BACS networks based on wireless communication such as EnOcean, the security mechanisms of the respective radio technology SHOULD be used to secure communications. In particular, appropriate authentication and encryption SHOULD be implemented on the air interface. If this is not possible with the mobile devices in use, communications involving these devices SHOULD be controlled at the transition to wired networks (e.g. by a component with a firewall function).

Furthermore, possible interference in the propagation of radio waves (e.g. due to shadowing) SHOULD be taken into account when planning BACS networks.

INF.14.A17 Securing Mobile Communications in BACS Networks (S) [Planner]

If mobile communications are used in the context of BACS, the security mechanisms of the respective mobile networks SHOULD be used for such BACS networks.

If public mobile networks such as 5G or Sigfox are used in BACS, uncontrolled direct IP-based communication with BACS-relevant components SHOULD be prevented.

BACS components SHOULD only be equipped with a dedicated connection to a public mobile network if this is essential for their operation. For this purpose, the BACS components for which a connection to public mobile networks is necessary SHOULD be checked and determined.

If it is not possible to separate BACS networks in the public mobile network (e.g. using slicing in the case of 5G), IP communication SHOULD be decoupled in the communication channel at hand by means of an application layer gateway (ALG).

If mobile technologies are used in BACS as part of the public mobile infrastructure of a mobile operator, one or more virtual mobile networks SHOULD be implemented and made exclusively available to the BACS using each respective mobile technology.

If autonomous private mobile networks are set up locally on a given campus in BACS using mobile technologies such as LTE and 5G, the transition between these mobile networks and other networks SHOULD be secured by a coupling element with a firewall function.

Segmentation into several virtual mobile networks SHOULD be implemented for private mobile networks, as well.

INF.14.A18 Secure Integration of BACS-External Systems (S)

The communication of BACS with BACS-external systems SHOULD be only be possible via defined interfaces and IT systems. This communication SHOULD be authenticated and encrypted.

The possible interfaces to BACS-external systems SHOULD be limited to those required.

INF.14.A19 Use of Dedicated Address Ranges for BACS Networks (S) [Planner]

For BACS, dedicated address ranges SHOULD be used that differ in particular from the address ranges of office IT and OT. For these address ranges, the ranges from which static addresses are to be assigned and the BACS-relevant components that are to receive static addresses SHOULD be defined.

If the network areas connected to BACS (e.g. building services systems) use identical address areas (replicating system configurations), they MUST be located in separate segments to prevent address conflicts. In this case, cross-segment communication MUST be secured by appropriate mechanisms—for example, using an ALG or network address translation (NAT).

INF.14.A20 Avoiding Broadcast Communication in BACS Networks (S) [Planner]

In BACS networks, the broadcast load on OSI Layer 2 or OSI Layer 3 for uninvolved systems and components SHOULD be minimised to avoid overloads. For this purpose, communication SHOULD be switched to group-specific multicasts or considered accordingly in segmentation planning.

INF.14.A21 Displaying Validity of Information in BACS (S)

BACS SHOULD make it clear whether the information they display in terms of time, place, value, state, or event is based on information that was received as planned. Information showing simulated or “frozen” values SHOULD be recognisable or trigger an alarm depending on the protection needs of the BACS at hand.

INF.14.A22 Ensuring Autonomous Functioning of BACS and Building Services Systems (S) [Planner]

Within BACS, it SHOULD be ensured that building services systems also function autonomously according to their protection needs, independent of their connection to BACS. In particular, BACS SHOULD be configured in such a way that there are no dependencies on TBM, other BACS, or building services systems that would prevent their operation. A building services system SHOULD remain operational and perform its functions for a certain period of time according to the respective protection needs, even if its connection to BACS fails.

NF.14.A23 Use of Physically Robust Components for BACS (S) [Planner]

Depending on the circumstances in which BACS components are to operate, corresponding physically robust components SHOULD be used that are especially intended or designated for

harsh environmental conditions. If appropriately robust components are not available, suitable compensatory measures SHOULD be taken.

INF.14.A24 Time Synchronisation for BACS (S)

All components and building services systems connected in BACS SHOULD use a synchronous time to ensure automated measurement, control, and regulation (see also OPS.1.2.6 *NTP Time Synchronisation*). BACS that are interconnected SHOULD also use a synchronous time. If BACS span multiple building complexes or properties, time synchronisation SHOULD be ensured for all these buildings.

If real-time communication is required within a BACS, PTP or a comparable mechanism SHOULD be used for time synchronisation instead of NTP.

INF.14.A25 Dedicated Monitoring in BACS (S)

A suitable monitoring concept SHOULD be established and implemented for all components that are relevant to BACS operations. The availability and significant parameters of BACS-relevant components SHOULD be continuously monitored. Error conditions and defined thresholds that are exceeded SHOULD be reported to the operator organisation automatically.

At minimum, alarms SHOULD be triggered by BACS if building services systems fail or important functions for automated control and regulation are not available. In addition, particularly safety-relevant events and other events for which automatic alarm messages should be generated SHOULD be defined.

Status messages and monitoring data SHOULD ONLY be transmitted using secure communication channels.

INF.14.A26 Logging in BACS (S)

As a supplement to OPS.1.1.5 *Logging*, status changes in BACS-relevant components and security-relevant events SHOULD be logged. In addition, all instances of write access to configurations of building services systems (and, if applicable, BACS-relevant components) SHOULD be logged, along with all manual and automated changes to the states of these systems and components.

The logging data to be merged on a central logging instance SHOULD be determined.

Logging data SHOULD ONLY be transmitted using secure communication channels.

INF.14.A27 Consideration of Interactions Between BACS Components in Contingency Planning (S)

The impact that BACS and the planning and concepts derived from them have on contingency planning SHOULD be analysed initially and at regular intervals in a transparent way. In particular, it SHOULD be determined how interactions with other building services, BACS-relevant systems, and TBM can be minimised in the event of a failure of building services systems or BACS-relevant components due to a technical defect or attack. Within the scope of contingency planning, it SHOULD also be determined which maintenance personnel are responsible for the affected building services systems and BACS-relevant systems and which reporting channels can be used to reach them. In addition, the authorisations the maintenance personnel have to remedy emergencies SHOULD be determined.

Contingency planning SHOULD also specify how any necessary emergency operation of building services systems will be ensured in the event of a BACS failure. A restart sequence SHOULD be defined for all building services systems and BACS (including all BACS-relevant components) and documented in the corresponding plans for restoration of service.

3.3. Requirements in Case of Increased Protection Needs

The following section lists generic suggestions for this module with respect to requirements that go beyond a level of protection based on the current state of the art. These SHOULD be taken into account in the event of increased protection needs. Final specification is performed within an individual risk analysis.

INF.14.A28 Physical Separation of BACS (H) [Planner]

In case of increased protection requirements, BACS networks SHOULD be realised as physically separated zones according to module NET.1.1 *Network Architecture and Design*.

Depending on the protection requirements at hand, dedicated, restrictively regulated Internet access SHOULD be provided for connections to manufacturer clouds, for example.

Depending on the protection needs of BACS, connections to untrusted networks and to the respective organisation's own office or OT networks SHOULD be prevented where applicable.

INF.14.A29 Separation of Individual Building Services Systems (H)

In order to secure individual building services systems with increased protection requirements within BACS, such building services systems SHOULD be located in separate network segments. To control communication, firewall functions SHOULD be positioned directly before the system network.

INF.14.A30 Provision of a Dedicated BACS Time Server for Time Synchronisation (H)

For BACS with increased protection needs (including at the individual system level), a dedicated BACS time server SHOULD be provided that is directly coupled to an atomic or radio clock (stratum 0) and supports the connection of further downstream BACS time servers.

4. Additional Information

4.1. BACS-Specific Terminology Used

Alarm system

Alarm systems are building services systems that can detect and report hazards such as intrusion, fire, and smoke. They detect hazards by interacting with sensors or operating units and generate hazard messages that are sent to a central component.

BACS area

A BACS area comprises one or more rooms intended for similar use (which may be distributed horizontally, vertically, or in a combination of both) and includes several BACS segments.

Examples: a corridor, a floor, a wing of a building, a production hall.

BACS segment

A BACS segment is the smallest spatial unit for which BACS functions are applicable. A BACS segment should not be confused with a network segment, which is separated from the rest of a network by security elements.

BACS-specific networks

A BACS-specific network is a network that uses cabling that is usually not based on Ethernet technology (e.g. the KNX bus system) or uses specific protocols that are not based on IP and Ethernet according to IEEE 802.3 (e.g. BACnet). Specific protocols may be necessary due to real-time communication requirements or a reduced protocol scope.

Building automation and control systems (BACS)

According to VDI 3814-1, building automation and control systems (BACS) comprise all products and services that support the automated, target-oriented operation of building services.

According to VDI 3814-1, a single building automation and control system (also abbreviated as BACS) represents the technical realisation of building automation and comprises the following parts:

- BACS management
- System automation and control
- Room automation

Like in the case of operational technology (OT), system automation and room automation consist of the (functional) automation level (e.g. system controls) and the field level (e.g. actuators and sensors).

Building services (BS)

According to VDI 4700 Sheet 1, building services (BS) include all technical facilities and use-specific facilities installed in a building and any further facilities connected to them, as well as technical facilities in outdoor facilities and equipment. Certain components of BACS can also be attributed to building services, such as real-time-capable industrial Ethernet switches.

Building services system

A building services system describes the totality of all technical components that interact to fulfil certain functions in a building. According to DIN 276 (“Building costs”), examples include heating systems, ventilation systems, or lighting systems. In cases involving automation, systems are integrated into or coupled with BACS.

Control centre

A control centre (see also "control and display device") is a technical tool for visualising current workflows, states, and situations of BACS processes.

Control and display device (CDD)

According to DIN EN ISO 16484-2, control and display devices (also referred to as control centres or control rooms) comprise any user facilities that act as an interface to the operating and management functions of a BACS.

Coupling of systems or installations

According to VDI 3814-2-2, the coupling of systems and installations enables them to send their information to BACS without limiting or losing their self-sufficiency. This means a system or installation coupling generally has no adverse effects.

Examples: a fire alarm system or intruder alarm system.

Demand organisation

According to DIN EN ISO 41011, a demand organisation is an organisational unit within or outside of a given organisation that is authorised to make corresponding demands of building services, BACS, or TBM for its requirements and to bear the costs of meeting these demands.

Examples: a tenant within a building, the owner of a building, a service provider within an organisation (e.g. a canteen)

Integration of systems or installations

According to VDI 3814, the integration of systems or installations enables them to exchange information with M-BACS and thereby influence each other.

System integration in the context of BACS must be distinguished from embedded systems. These are intelligent elements that are embedded in other systems and take over largely invisible monitoring, control, processing, or regulation functions in the surrounding system.

Local override (LOR)

According to VDI 3814-1, a local override is an interface to BACS-relevant components that enables limited operation independent of automation devices with priority display, switching, and/or control. Example: the manual priority operation of fans.

Management building automation and control systems (M-BACS)

Management building automation and control systems (M-BACS), which are also referred to as building management systems, are a component of a BACS that handles information processing tasks for the management of the BACS (e.g. functions for higher-level energy management, maintenance management, fault management, and room booking management).

Non-reaction

A non-reactive connection between a building services system and BACS means that the building services system supplies information to the BACS, but cannot be influenced by it on the basis of this information. The system thus remains autonomous.

Property

According to VDI 3814-1, a property comprises one or more buildings that are usually adjacent.

Room automation and control (RAC)

Room automation (RA) is a BACS component that handles all tasks related to cross-system automation in the room under consideration (e.g. the operation of the technology installed in the room).

System automation and control (SAC)

System automation and control (SAC) is part of BACS. It implements automation for the energy-efficient, economical, and safe operation of building services systems. SAC controls building services system and their status variables via actuators. These are in turn recorded by the sensors of each building services system.

Trade

In construction, a trade generally comprises the work that can be assigned to a self-contained construction service area. It is a functional area that can include, in particular, various building services systems.

Example: air-conditioning systems (cost group 430 in DIN 276), which include ventilation systems, air-conditioning systems, and refrigeration systems.

Technical Building Management (TBM)

According to DIN 32736, Technical Building Management (TBM) comprises all services that maintain the technical function and availability of a building. TBM thus handles the operation, maintenance, modernisation, and documentation of components of building services and defines all the necessary processes.

4.2. Abbreviations

Abbreviation	Meaning
5G	5th generation of mobile communications
BACS	Building automation and control systems
BIM	Building information modelling
BS	Building services
CISO	Chief Information Security Officer
CRT	Cross-reference table
DIN	*Deutsches Institut für Normung* (German Institute for Standardization)
DOS	Denial of service
EN	European standard
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information technology
KNX	Konnex bus
LAN	Local area network
LTE	Long-Term Evolution (wireless broadband communication standard)
NAT	Network address translation (NAT)
NTP	Network Time Protocol
OSI	Open Systems Interconnection

Abbreviation	Meaning
OT	Operational technology
PTP	Precision Time Protocol
RA	Room automation
SAC	System automation and control
SLA	Service level agreement
TBM	Technical Building Management
USB	Universal Serial Bus
VDI	*Verein Deutscher Ingenieure* [The Association of German Engineers]
VDMA	*Verband Deutscher Maschinen- und Anlagenbau* [Mechanical Engineering Industry Association]
WAN	Wide area network
WLAN	Wireless local area network

4.3. Useful Resources

Standards and documents cited:

DIN EN ISO 16484—Building automation and control systems (BACS)

- DIN EN ISO 16484-1—Building automation and control systems (BACS)—Part 1: Project specification and implementation, DIN/EN/ISO, March 2011, available from Beuth-Verlag
- DIN EN ISO 16484-2—Building automation and control systems (BACS)—Part 2: Hardware, DIN/EN/ISO, October 2004, available from Beuth-Verlag
- DIN EN ISO 16484-3—Building automation and control systems (BACS)—Part 3: Functions, DIN/EN/ISO, December 2005, available from Beuth-Verlag
- DIN EN ISO 16484-5—Building automation and control systems (BACS)—Part 5: Data communication protocol, DIN/EN/ISO, December 2017, available from Beuth-Verlag

DIN 32736—Building management—Terminology and scope of services, German Institute for Standardization (DIN), August 2000, available from Beuth-Verlag

DIN EN ISO 41011—Facility management—Vocabulary, DIN/EN/ISO, April 2019, available from Beuth-Verlag

DIN 276—Building Costs, German Institute for Standardization (DIN), December 2018, available from Beuth-Verlag

VDI 4700 Sheet 1—Terminology of civil engineering and building services, The Association of German Engineers (VDI), October 2015, available from Beuth-Verlag

VDI 3814—Building automation and control systems (BACS)

- VDI 3814 Sheet 1—Building automation and control systems (BACS)—System basics, The Association of German Engineers (VDI), January 2019, available from Beuth-Verlag
- VDI 3814 Sheet 2.1—Building automation and control systems (BACS)—Planning—Requirements planning, The Association of German Engineers (VDI), January 2019, available from Beuth-Verlag

- VDI 3814 Sheet 2.2—Building automation and control systems (BACS)—Planning—Planning content, system integration, and interfaces, The Association of German Engineers (VDI), January 2019, available from Beuth-Verlag
- VDI 3814 Sheet 2.3—Building automation and control systems (BACS)—Planning—Concept of operation and user interfaces, The Association of German Engineers (VDI), September 2019, available from Beuth-Verlag
- VDI 3814 Sheet 3.1—Building automation and control systems (BACS)—BACS functions—Automation functions, The Association of German Engineers (VDI), January 2019, available from Beuth-Verlag
- VDI 3814 Sheet 4.1—Building automation and control systems (BACS)—Methods and tools for planning, building, and acceptance tests—Identification, addressing, and lists, The Association of German Engineers (VDI), January 2019, available from Beuth-Verlag
- VDI 3814 Sheet 4.2—Building automation and control systems (BACS)—Methods and tools for planning, building, and acceptance tests—Requirements, content of planning, and system integration, The Association of German Engineers (VDI), January 2019, available from Beuth-Verlag
- VDI 3814 Sheet 4.3—Building automation and control systems (BACS)—Methods and tools for planning, building, and acceptance tests—BACS automation scheme, BACS function list, BACS functional description, The Association of German Engineers (VDI), November 2020, Draft, available from Beuth-Verlag
- VDI 3814 Sheet 6—Building automation and control systems (BACS)—Qualification, roles, and competencies, The Association of German Engineers (VDI), April 2020, Draft, available from Beuth-Verlag

VDMA 24774—IT security in building
automation. VDMA, German Engineering Federation, February 2021, available from Beuth-Verlag

5. Appendix: Cross-Reference Table for Elementary Threats

Every requirement in this module can be used to derive security safeguards. Implementing these safeguards will help mitigate the Elementary Threats (G0) which are relevant for the issue or target object at hand. In the cross-reference table, each requirement of this module is mapped to the relevant Elementary Threat(s).

This cross-reference table can thus be used to determine which Elementary Threats are covered by which requirements. The letters in the second column indicate which key security objectives are primarily addressed by each requirement. These key security objectives are confidentiality (C), integrity (I), and availability (A).

The following Elementary Threats are relevant for module INF.14 *Building Automation and Control Systems (BACS)*:

G 0.9 Failure or Disruption of Communication Networks

G 0.10 Failure or Disruption of Supply Networks

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.37 Repudiation of Actions

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.46 Loss of Integrity of Sensitive Information