Skadden

Cybersecurity and Data Privacy Update

July 18, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

The EU's Digital Operational Resilience Act (DORA) – 2024 Update

Executive Summary

As implementation of the EU's Digital Operational Resilience Act (**DORA**) approaches, financial market participants and their technology service providers (both in and out of Europe) face a critical compliance deadline. The new law will significantly impact financial entities and directly and indirectly affect information and communications technology (**ICT**) service providers. Key points to consider are:

- Financial entities operating in the EU must implement comprehensive ICT risk management, resilience testing and third-party risk management, effective January 17, 2025. DORA imposes stringent requirements on financial entities to establish robust ICT risk frameworks, continuous monitoring, incident response plans and business continuity measures.
- Financial entities are required to review and potentially amend contracts with technology service providers to ensure compliance with DORA, which includes preparing for heightened scrutiny and oversight. Companies will need to update internal policies and procedures to meet DORA's standards, emphasizing ICT asset management, encryption controls, vulnerability management and incident reporting. Board-level awareness and training on ICT risks will be crucial for compliance readiness and governance under DORA.
- If providing services to EU financial entities, technology service providers, whether located in the EU or abroad, must align their services and contractual terms with DORA to support clients' compliance requirements. Technology service providers should anticipate increased due diligence on existing operational and technical frameworks and additional demands from clients, including regarding readiness to provide comprehensive incident response plans and ongoing testing. Consideration of parties' exit and transition provisions will be essential.

Introduction

Much has already been written about the EU's upcoming Digital Operational Resilience Act, including in our 2023 alert on DORA's impact on alternative investment funds.

Given the further potential impact this legislation will have on both European and non-European financial market participants and tech providers, this article provides an update on the implementation process, an overview of DORA's direct and indirect effects, and considerations for in-scope entities to think about now.

A Reminder Regarding Scop

The direct impact of DORA is broad: The new law covers "financial entities" (**FEs**), which includes most types of financial services entities regulated in the EU, including banks, payments and e-money firms, investment firms, insurers and cryptoasset firms.

The EU's Digital Operational Resilience Act (DORA) – 2024 Update

This scope extends further than many comparable regimes; for example, the UK's requirements on operational resilience do not automatically apply to asset managers, financial markets infrastructure, certain investment intermediaries, credit brokers or insurance intermediaries.

In addition to DORA's direct impact on FEs, as detailed below, the indirect impacts on technology service providers to FEs ("ICT third-party service providers," or **ICT TPPs**) are anticipated to be even greater. To continue servicing their EU FE clients, ICT TPPs will need to show they can meet standards imposed by DORA on these clients.

Key Dates

DORA came into force on December 14, 2022, with operational mandates becoming effective on January 17, 2025. This offers a limited time frame for compliance. Detailed obligations will be specified in certain "Level 2" regulatory and implementing technical standards.

Of particular interest to ICT TPPs is the May 2024 Official Journal publication of Commission Delegated Regulation (EU) 2024/1502, which specifies the criteria for the designation of ICT TPPs as "critical" for financial entities.

In addition, the two tranches of regulatory and implementing technical standards are either finalised and in the Official Journal, or (in the case of Tranche 2) were finalised and submitted by July 17, 2024, for adoption by the European Commission.

This means DORA implementation projects will need to progress swiftly in H2 2024 to ensure these detailed requirements are met.

Relatedly and highlighting the importance of ICT TPPs, in May 2024 the European Supervisory Authorities[1] (**ESAs**) launched a voluntary "dry run" exercise for the collection of data for the "register of information" on ICT TPPs. Participants received feedback on data quality and completed a practice workshop.

Impact on Financial Entities

Implementation projects for FEs covered by DORA should be well developed. The key deliverables FEs will need to have in place by January 17, 2025, are:

- An established **ICT risk management framework** identifying all ICT supported business functions and all sources of ICT risks, cybersecurity threats and vulnerabilities.
- **Continuous monitoring and control of ICT systems and tools** to provide ongoing protection from and prevention of harm.
- Implementation of **advanced digital operational resilience testing** of ICT systems and development of a threat-led testing approach.
- An established **third-party risk management function** that includes (i) ensuring that contracts with ICT TPPs meet the requirements of DORA, (ii) maintaining a "register of information" related to ICT TPPs and (iii) implementing a process for risk concentration management.
- An **incident classification and reporting framework** for timely and accurate incident reporting to authorities.
- **Business continuity and IT service continuity plans**, including segregated and secure backup systems.
- **Clear governance structures** with top management accountability for ICT risk management.

FEs will also need to consider and implement technical standards to comply with DORA. The second batch of these standards was published on July 17, 2024, giving FEs only six months to complete implementation before DORA takes effect in January 2025.

Impact on ICT TPPs

Indirect impact

Even if not directly in-scope for DORA (and regardless of whether located in the EU), many ICT TPPs will be heavily impacted by the act's digital oversight.

ICT TPPs will need to consider whether they are providing ICT services that support the "critical or important functions" of their FE clients or that could otherwise be designated more broadly as a "critical ICT TPP," as further detailed below.

ICT TPPs should also be aware of the DORA obligations that will be imposed on their FE clients so the service providers can support these obligations if they want to continue providing services to such clients. The extent to which the ICT TPP is supporting a critical or important function at the client will determine the burden on the service provider. Some of the key obligations of FEs that ICT TPPs will need to support include:

- Ensuring that ICT TPP contracts contain the protections required by DORA.
- Maintaining a "**register of information**" related to ICT TPPs, including extensive due diligence.

[1] The ESAs comprise the European Banking Authority (**EBA**), the European Securities and Markets Authority (**ESMA**) and the European Insurance and Occupational Pensions Authority (**EIOPA**).

- Implementing a process for risk concentration management.
- Maintaining and periodically testing business continuity plans (**BCPs**) and ICT Disaster Recovery Plans, with a particular focus on "**critical or important**" functions contracted through ICT TPPs. This must be done at least yearly and after substantive changes to the FE's ICT systems.
- Defining a holistic ICT multi-vendor strategy showing key dependencies and explaining the rationale behind the procurement mix.
- Adopting and regularly reviewing a strategy to manage ICT third-party risk, considering the multi-vendor strategy referred to above.
- Identifying and documenting all processes dependent on ICT TPPs.
- At least every three years and where relevant, conducting threat-led penetration testing of key systems.

Direct Impact — 'Critical' ICT TPPs

Critical ICT TPPs (**CTPPs**) will be subject to direct regulatory supervision by the European Supervisory Authorities.

Designation as a CTPP

DORA provides a separate designation regime for CTPPs, designed to cover those ICT TPPs that (i) are systemically important to a high number of FEs, (ii) support critical or important functions and (iii) are difficult to substitute.

The criteria for designation is set out in Commission Delegated Regulation 2024/1772. The ESAs will identify ICT service providers critical to the financial system in two steps:

In Step 1 of the assessment, authorities will evaluate ICT TPPs against specific quantitative indicators and minimum relevance thresholds. The ESAs will gather this data as part of the register of information submitted by FEs. These indicators gauge the extent of ICT services provided to FEs.

- Providers will qualify as CTPPs if they serve 10% or more of these FEs or support critical functions for major financial institutions such as globally systemically important institutions (**GSIIs**) or other systemically important institutions (**OSIIs**).
- Additionally, ICT services supporting critical functions for significant financial market infrastructure (**FMIs**) or multiple significant FEs also qualify for consideration.

The outcome of Step 1 identifies ICT TPPs that may warrant further assessment in Step 2.

Step 2 involves a more detailed qualitative assessment using additional criticality indicators. Unlike Step 1, these indicators do not have minimum thresholds, but provide a deeper evaluation of the potential impact of service discontinuation on FEs' operations. This assessment considers factors such as:

- The consequences of service disruptions.
- Reliance on common subcontractors.
- Interdependencies among GSIIs, OSIIs, and other FEs using the same ICT TPPs.

The culmination of Step 2 is a proposed list of ICT TPPs designated as CTPPs, which is reviewed and recommended to the ESAs Joint Committee.

Third-country CTPPs (*i.e.*, those without an EU establishment) will be required to establish an EU subsidiary **within a year of CTPP designation** if they wish to continue to service FEs within the EU.

The designation process will start in January 2025 and the resulting first set of qualifying providers will be published by mid-2025.

Obligations for CTPPs

Each CTPP will have one ESA appointed as its "Lead Overseer" (LO). Each LO must ensure the CTPPs it supervises have comprehensive and effective rules, procedures, mechanisms and arrangements to manage ICT risks across the FE clients they service. An LO's assessments will focus on CTPPs' abilities to maintain robust operational resilience, and will cover the following:

- **Risk management:** evaluating effectiveness of risk management frameworks used to identify, assess and manage ICT risks, as well as the quality, security and scalability of a CTPP's services.
- **Governance and control:** ensuring CTPPs have appropriate governance structures, policies and controls to manage ICT risk, including board-level oversight.
- **Physical security standards:** ensuring appropriate physical protection of systems, networks, data, etc.
- **Incident reporting:** ensuring CTPPs have proper mechanisms to promptly and accurately identify and report significant incidents and take appropriate action to resolve them.
- **Operational resilience testing:** overseeing the implementation and outcomes of resilience testing, including vulnerability assessments and penetration testing.
- **Information sharing:** promoting and evaluating effectiveness of information-sharing arrangements regarding cyber threats and vulnerabilities.

- **Exit and transition:** approving mechanisms for data and application portability and interoperability related to exit and transition of services.

The LOs are empowered to audit any firms under their supervision, with reference to relevant national and international ICT standards.

The results of these assessments will form the basis of an annual oversight plan that the LO will provide to each CTPP, which will describe oversight objectives and actions planned on an individual basis.

Key Comparators – UK Operational Resilience Framework

The requirements imposed by DORA will overlap with existing frameworks that already apply to some firms. The biggest potential overlap will be with the UK's existing operational resilience regime and the forthcoming UK critical third-party (**CTP**) regime, with the latter expected to come into force in late 2024.

UK regulators intend for the UK CTP regime to be "as interoperable as reasonably practicable with" similar regimes, including DORA. While the UK and EU regulations seek similar outcomes, some notable differences between both operational resilience frameworks and the CTP/CTPP regimes include:

- The proposed UK rules are risk-agnostic and extend beyond ICT risks. The rules cover any services to UK-regulated firms and FMI entities provided by UK CTPs.
- The UK's approach is focused on resilience outcomes and principles, in contrast to DORA's prescriptive approach. UK CTPs will be in-scope of **six Fundamental Rules** that impose high-level standards to all services provided by CTPs.
- UK CTPs are subject to broader organisational requirements than CTPPs are under DORA — mirroring the requirements set by the UK Financial Conduct Authority (FCA) in the FCA Handbook for FSMA-authorised firms (meaning those subject to the Financial Services and Markets Act 2023). For example, the proposed UK rules include record-keeping requirements.
- UK CTPs will drive annual self-assessments, scenario testing and testing of incident management playbooks, while DORA assigns the responsibility to conduct these to the CTPPs' LOs.

The consultation on the UK rules closed on March 15, 2024.

What To Think About Now

FEs: As FEs prepare for the implementation of DORA, there are several critical steps they can consider in order to set up compliance:

- Consider which service providers could provide critical or important functions.
- Review contracts with service providers, identify any nearing contract review cycle and consider future-proofing contracts with DORA-compliant wording.
- Review internal onboarding and vendor approval policies and procedures to ensure DORA requirements are addressed, including updating the vendor due diligence questionnaire.
- Update incident response plans and communication playbooks to allow for compliance with DORA, particularly noting the time frames to be implemented.
- Establish board-level training and awareness of ICT risks.[2]

Some national authorities, including Germany's BaFin, recently published detailed implementation guidance for in-scope firms.[3]

Technology service providers: Regardless of whether a company could be designated as a CTPP, all entities providing technology services to FEs should consider:

- Future-proofing standard terms to include mandatory DORA provisions.
- Preparing information to satisfy FE clients' due diligence questionnaires.
- Reviewing internal policies and procedures to ensure standards required by DORA are met, including in relation to ICT asset management, encryption and cryptographic controls, vulnerability and patch management, and data security.
- Checking that comprehensive incident response plans and communication playbooks are in place and implementing regular training on such plans.
- Implementing procedures to allow for prompt incident reporting to clients and drafting client-facing documentation to evidence this.
- Designing exit and transition provisions to allow services to transition to and from the FE.

[2] See also our July 2024 alert "ECB Mandates Board Expertise in Addressing ICT and Security Risks."

[3] OneTrust, "Germany: BaFin Publishes Implementation Guidelines for DORA" (July 11, 2024).

The EU's Digital Operational Resilience Act (DORA) – 2024 Update

Contacts

Sebastian J. Barling
Partner / London
44.20.7519.7195
sebastian.barling@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Nicola Kerr-Shaw
Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

Susanne Werry
Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

David Y. Wang
Associate / London
44.20.7519.7149
david.y.wang@skadden.com