Skadden

Cybersecurity and Data Privacy Update

August 14, 2025

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

Avenue Louise 480
1050 Brussels
32.2.639.0300

22 Bishopsgate
London EC2N 4BQ
44.20.7519.7000

NIS2 Update: EU Cyber Authority Sets Out Compliance Expectations, but Implementation Is a Work in Progress

Executive Summary

- **What is new:** On 26 June 2025, the EU Agency for Cybersecurity (ENISA) published guidance documents setting out security measures that regulated organisations should have in place to comply with the EU's critical infrastructure cybersecurity law (NIS2).
- **Why it matters:** These expansive security standards will require significant investment for many newly regulated entities, and member states' varying NIS2 implementations add a further layer of complexity.
- **What to do next:** As companies assess their 2026 security and compliance budgets, they should determine what expanded security efforts will be required —prioritizing the greatest enforcement risks — and plan implementation and funding for the coming months and years.

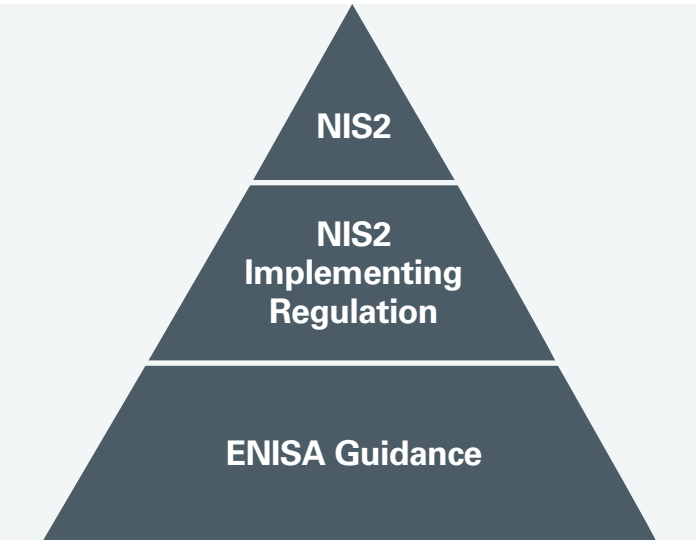
The Guidance

The guidance, though not strictly binding, further clarifies ENISA's expectations of NIS2-regulated entities, building upon both the text of NIS2 and the European Commission's NIS2 Implementing Regulation 2024/2690 on cyber risk management.[1] (For an overview of NIS2, see our previous client alert "Navigating the New Cybersecurity Landscape: Key Implications of the EU's NIS 2 Directive.") As an example:

1. NIS2 requires companies to have security measures covering "the use of multi-factor authentication."
2. The NIS2 Implementing Regulation expands on this obligation, stating that companies' multifactor authentication measures "shall ensure that users are authenticated by multiple authentication factors … in accordance with the [risk] classification of the asset to be accessed."
3. The guidance further expands on the Implementing Regulation, stating that companies should "enforce [multifactor authentication] on internet-facing systems, such as email, remote desktop and VPNs," and document this compliance through configuration logs. The guidance also maps ENISA's expectations to widely-used international standards such as ISO 27001.

[1] The Implementing Regulation and published guidance apply only to companies operating in digital sectors (such as cloud computing, data centres, managed services and online search engines) but are likely to influence regulators' compliance expectations more broadly.

NIS2 Update: EU Cyber Authority Sets Out Compliance Expectations, but Implementation Is a Work in Progress



The guidance, and in particular ENISA's commitment to aligning regulatory obligations with existing international standards that many companies have already adopted, is welcome, and sets out a helpful blueprint for technical implementation of NIS2 compliance programs. However, the scale of ENISA's guidance (stretching to nearly 200 pages of security measures) reinforces the extent of investment and documentation regulators expect for comprehensive NIS2 compliance. Companies should target their NIS2 compliance programs to focus on systems (*e.g.*, operationally critical systems) and topics (*e.g.*, incident response and vendor management) that present the greatest enforcement risk to avoid spreading limited compliance resources too thinly.

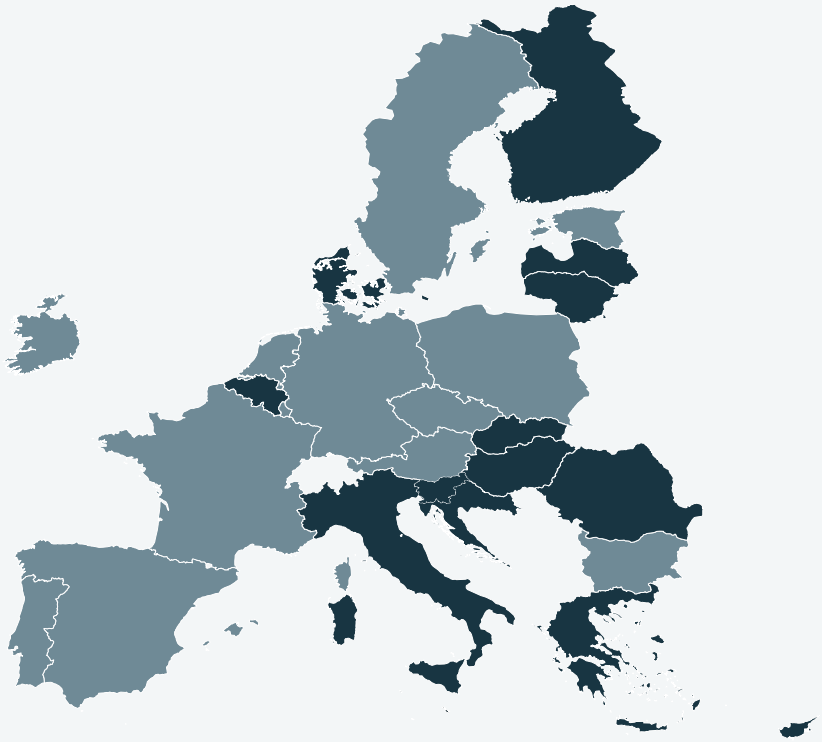
As part of the guidance, ENISA published a "roles and skills" summary, mapping the internal expertise and responsibilities required to meet NIS2 obligations and emphasizing that NIS2 compliance requires cross-functional teams, including IT, cybersecurity, legal and compliance specialists.

NIS2 Implementation Status

While ENISA continues to advance NIS2, EU member states' implementation has lagged behind. Despite continued complaints from the European Commission, including a public rebuke, 13 out of 27 states have not yet implemented NIS2 into local law. This challenges companies to hit a moving compliance target.

EU NIS2 Directive – Transposition

- **Act adopted:** Belgium, Croatia, Cyprus, Denmark, Greece, Finland, Hungary, Italy, Lithuania, Latvia, Malta, Romania, Slovakia, Slovenia
- **Legislative process ongoing:** Austria, Bulgaria, Czech Republic, Estonia, France, Germany, Greece, Ireland, Luxembourg, Netherlands, Poland, Portugal, Spain, Sweden



NIS2 Update: EU Cyber Authority Sets Out Compliance Expectations, but Implementation Is a Work in Progress

While approximately half of member states have already transposed NIS2 into national law (some, like Latvia and Lithuania, even ahead of the October 2024 deadline), others are moving more slowly. Several countries, including Germany, Ireland, the Netherlands and Poland, have advanced draft legislation that outlines national frameworks, regulators and sector-specific requirements. Meanwhile, member states such as Spain, Estonia and Sweden remain at an earlier stage of the process.

Approaches to key implementation elements also vary. For example, many countries, including Belgium, Hungary and Italy, have aligned liability provisions for management bodies with national existing civil law regimes.

Reporting obligations under NIS2 also vary significantly across member states, creating a fragmented compliance landscape for cross-border entities. Definitions of "significant incidents," reporting thresholds and timelines differ, with some countries imposing stricter requirements than NIS2 does. For example, entities in Cyprus must submit early warnings within six hours of detection — well ahead of NIS2's 24-hour requirement. This divergence in national rules increases administrative and compliance burdens for organizations operating across multiple EU jurisdictions.

Given this uncertainty, companies should take a phased approach to compliance, focused on addressing core compliance obligations that are likely to be consistent across member states, while leaving flexibility to address jurisdiction-specific quirks once more member states complete their implementations.

What To Do Now

Given the breadth of NIS2's obligations and the ongoing uncertainty surrounding its implementation, companies need to scope and target their NIS2 compliance efforts to make the most of limited compliance resources. In particular, companies should:

- Continue to progress NIS2 compliance programs, focusing on systems (*e.g.*, operationally critical systems) and documentation (*e.g.*, incident response plans) that present the greatest enforcement risk.
- Ensure that management bodies (*e.g.*, boards) are updated on NIS2 compliance progress, as those management bodies can be held personally liable for NIS2 noncompliance.
- Take advantage of ENISA's mapping to existing international standards to identify areas where existing information security documentation can be leveraged — for example, where policies prepared for ISO 27001 compliance can be reused with minimal changes for NIS2 compliance — and identify gaps in that documentation.
- Track NIS2 implementation status in the jurisdictions in which a company operates, and identify areas where compliance efforts can be advanced before local implementation is complete.

Contacts

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

Aleksander J. Aleksiev
Associate / London
44.20.7519.7000
aleksander.aleksiev@skadden.com

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

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com