NIS2: uncertainty and compliance for cyber security

July 2025

Annika Nitschke

The Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA), the AI Act – the EU is currently enforcing numerous new regulations, making the introduction of the Network and Information Security Directive (NIS2) feel like a distant memory. Nevertheless, it remains a highly relevant issue, with many questions still unanswered, posing significant challenges and uncertainties for businesses. In this article, we aim to provide an overview of the current situation and offer guidance on how to prepare for NIS2.

As an EU directive, NIS2 must be transposed into national law by the Member States. This deadline passed more than half a year ago, but the implementation status across the EU remains very uneven. While around a third of the Member States[1] have already fully implemented the directive, others are still significantly behind, with some having only just completed drafts of laws that still require approval. In Germany, for instance, new elections have delayed the legislative process, with ongoing revision of the existing draft, and it remains uncertain when the law will be passed. Meanwhile, the European Commission has initiated proceedings against some states for non-compliance.

What does this mean for companies?

NIS2 is likely to come into effect immediately upon adoption into national law, with no staged transition period expected in any country. Therefore, companies must prepare, even though the exact requirements remain unclear.

There is no doubt that many measures, especially risk management and security awareness, are crucial for a proactive approach to protect against cyber attacks. Such measures should be implemented as they are in a company's best interest, regardless of regulatory mandates. However, country-specific compliance requirements remain unclear as only a few countries, such as Belgium, have published implementation guidance so far.

When in doubt, we recommend that companies initially align with an established cyber security standard like ISO 27001 to create a solid baseline. Affected companies should start assessing their current compliance maturity and considering how they will meet NIS2-specific incident reporting obligations according to Article 23, to identify and address potential gaps early on. Although country-specific details, such as the responsible authorities, may not yet be defined, there is no doubt that major incidents must be reported promptly. This requires processes for detection and reporting, as well as the allocation of sufficient resources for related tasks.

Companies operating in multiple markets face even more challenges

International businesses must keep track of various legislative developments and country-specific requirements, as countries outside of the EU are also revising their cyber-security laws. In the UK, for example, the Cyber

1 Belgium, Croatia, Cyprus, Denmark, Finland, Greece, Hungary, Italy, Latvia, Lithuania, Malta, Romania, Slovakia, Slovenia.

Security and Resilience Bill (CS&R) was announced in 2024 and is expected to enter Parliament this year. Beyond Europe, we see a clear global trend toward strengthening cyber-security frameworks, with countries tailoring their approaches to address specific national concerns and align with international standards, such as Canadas Critical Cyber Systems Protection Act (CCSPA) or the recent Cybersecurity Act in Singapore.

With our in-depth knowledge of regulations and international cyber-security standards, Analysys Mason can help you interpret and map requirements across jurisdictions or gain transparency through our customised reporting solutions to monitor the implementation status of requirements in your company. We can also support you in developing the necessary documentation and customised processes to meet requirements and stay ahead of legislative developments.