NIS2 update

KPMG Netherlands

May 2025

In May 2023, we released a whitepaper on the Network and Information Systems Directive (NIS2) and its impact on Information Technology (IT) and Operational Technology (OT). Since then, our work on client engagements has enabled us to identify and collect a series of common compliance challenges that organisations across different industries and sectors face under NIS2.

This update offers the latest insights into the key challenges NIS2 poses for businesses as well as the internal difficulties companies encounter when working to meet its compliance requirements. These insights are drawn from KPMG's recent projects, shared knowledge within the KPMG EMA community, and updates from the EU and Member States.

As of October 18, 2024, EU Member States were required to transpose the NIS2 Directive into national law. However, progress has been uneven - some met the deadline with draft laws, while others expect to complete transposition in the second half of 2025. In November 2024, the European Commission issued a formal warning, giving remaining Member States two months to transpose. Although NIS2 is now in effect, most countries still lack fully enforced national laws, leaving many organisations unprepared for compliance.

External challenges with NIS2 transposition

Despite NIS2's aims of establishing a unified approach to cybersecurity across the EU, we see increasing disharmony and fragmentation across different jurisdictions. Based on the KPMG's recent NIS2 projects we perform for our clients, we have insights into these challenges. This section addresses:

- NIS2's impact on businesses
- Scope and classification disharmony
- Incident reporting variations

NIS2's impact on business

The NIS2 Directive impacts all organisations within its scope. However, there are three categories where we see significant impact in terms of compliance:

Scope and classification disharmony

There is inconsistency among Member States in how they scope and classify entities under NIS2.

For example, a German draft law introduced a third tier for critical facilities, unlike the standard two-tier system (essential and important entities) outlined in the NIS2 Directive and adopted by other Member States.

Inconsistent classification of entities under NIS2 creates confusion and potential compliance gaps for organisations operating across multiple jurisdictions. This fragmentation introduces complexity, as businesses may face varying requirements and compliance expectations depending on how each Member State interprets and applies the directive - undermining the goal of a unified EU-wide approach.

Member State draft laws also differ in their security framework and industry standard requirements. For example, the Cybersecurity Centre for Belgium introduced a mandatory conformity assessment with three differing options. These three options are; (1) the certification of the entity under the CyberFundamental Framework, a (2) certification under the ISO/IEC 27001 norm, or (3) an inspection by the inspection service of the CCB. Other Member States, however, do not call out an exclusive certification framework or may call out frameworks such as NIST CSF 2.0.

The disharmony in scope and classification between Member States adds complexity for organisations with regional or global operations, as they must align with differing standards and frameworks to ensure effective and compliant.

Incident reporting variations

Varying incident reporting timelines and entity classifications across Member States are making it increasingly difficult for organisations to standardise their response processes, heightening the risk of non-compliance with local requirements.

For instance, Cyprus' latest draft law shortens the early warning notification window from 24 hours to just 6, diverging from the NIS2 Directive's baseline and the approach taken by most other Member States.

While the above example is the exception rather than the norm, it underscores how variations in national transposition of the Directive complicate compliance. This lack of standardisation makes it harder to streamline incident response processes, increasing the risk of errors or delays. Moreover, the inconsistency raises administrative burden and legal exposure, as a uniform, cross-border compliance strategy becomes impractical.

Summary

NIS2 impacts businesses differently depending on their sector and size, but the broader challenge lies in how national interpretations are undermining its goal of a unified approach. Instead of consistent rules, organisations face a patchwork of local requirements - making compliance increasingly complex and difficult to manage.

Internal challenges with directive requirements

Having worked in-depth on preparing organisations for NIS2 compliance across sectors and industries, our experience has highlighted some recurring challenges when implementing the compliance requirements.

This section addresses:

- Scoping challenges – the devil is in the detail
- Ensuring accountability for the 'Management Body'
- Complexity in incident reporting requirements
- Securing Operational Technology
- Supply chain security challenges for customers

Scoping challenges – The devil is in the detail

In November 2024, a European cybersecurity authority reported that 92% of surveyed organisations were aware of the general scope and provisions of the NIS2 Directive. However, beneath this growing high-level awareness lies complex scoping details and grey areas that remain difficult to interpret and apply.

Determining whether an entity falls within the scope of NIS2 requires a detailed understanding of how its products and services align with Annex I and II. A basic document review is often inadequate, as many organisations struggle to pinpoint exactly which products are produced where, and how they fit within complex supply chains.

For example, in the manufacturing sector, it is not enough for products to fall within the subsectors listed in Annex II of NIS2 (e.g., medical devices, electrical equipment, or motor vehicles); organisations must also determine whether those products align with the relevant activities defined under NACE Rev. 2 - the EU's statistical classification of economic activities.

The following food sector case study is another example of scoping complexity.

Case study: scoping challenges in the food sector

Even when organisations are faced with what they see as a simple applicability assessment, we see that scoping challenges still arise. As an example, the food sector falls into Annex II of the NIS2 Directive. According to the definition of the food sector (Art. 3 (2) Regulation [EC] No 178/2002), we see the boundaries of the sector are far reaching. The sector includes drink, chewing gum and any substance, including water, intentionally incorporated into the food during its manufacture, preparation or treatment. However, the definition excludes several factors, such as animal feed. For those companies which produce both human food and animal feed, insights such as this can be extremely useful to help scope NIS2 applicability smartly.

For the food sector, additional scoping complications arise from the overlap with another EU Directive, the Critical Entities Resilience Directive (CER). The scope of CER covers all sectors within Annex I of NIS2 and adds large-scale food production, processing, and distribution to its scope. **This is particularly interesting, as NIS2 underlines that entities identified as critical under CER shall be essential under NIS2.** This complicates the understanding, as with the food sector being placed in Annex II under NIS2, most organisations have assumed that their entity classification would not be essential but rather important.

The scope of the Directive depends not only on the sector and activity, but also the size of the organisation including thresholds on the number of employees. However, defining 'employees' is not always straightforward. Organisations must consider full-time staff, part-time workers, temporary hires, and contractors to determine their compliance requirements.

The way an organisation is legally structured can also pose challenges in determining which entities fall within the scope. In our experience, smart scoping helps organisations prioritise effectively – and in some cases, reduce the number of entities impacted. Conducting a legal scoping exercise across the full entity structure is one of the most effective ways to manage this complexity and mitigate compliance risk.

Ensuring accountability for the 'Management Body'

Organisations are facing challenges in ensuring management body accountability, a key requirement of NIS2, due to several reasons:

- The term 'management body' remains ambiguous in both scope and implication under NIS2. Legal counsel should be involved in interpreting this at the legal entity level, particularly as Member States require accountability from a designated legal representative within their jurisdiction who can be held liable.
- What qualifies as sufficient training for management bodies is often unclear and varies across Member States. Determining appropriate frequency, securing buy-in from entity management, and shifting cybersecurity from a perceived IT issue to a core business priority remain key challenges for compliance.
- Ensuring management accountability is particularly complex for multinational organisations with layered legal structures or centralised security functions operating across – or even outside – the EU. NIS2 requires these organisations to keep management informed on cybersecurity risks, initiatives, and investments, while also ensuring they actively oversee and approve related risk management measures.

Maintaining high levels of awareness and engagement among management is crucial, but compliance complexity increases with multiple entities and regions.

Complexity in incident reporting requirements

Article 23 outlines the reporting obligations for 'significant' incidents. We often see organisations struggle with the timelines imposed by these requirements, in terms of reporting swiftly to the correct authorities, and on time. Some key questions often raised are:

- Classification of significance: *What criteria determine whether an incident is significant?*
- Reporting responsibility: *Who is responsible for preparing and communicating early warnings, incident notifications, and the final report? And where should I report?*
- Involved departments: *Which departments need to be involved in the reporting process (also considering Management Body accountability)?*

To help with understanding scenarios that may and may not fall under the NIS2 reporting obligations, we have outlined the following examples.

Example scenario	Incident reportable?
Cyber attack in EU takes down a data centre which means the facility cannot load out or deliver product	**Likely yes** | Cyber-attack on network and information systems with operational impact
Flood in EU takes down a data centre which means the facility cannot load out or deliver product	**Likely yes** | Disruption on network and information systems with operational impact
Supplier is unable to provide key product to company facilities/sites because of a storm	**Likely no** | Disruption to business operations but no impact on network and information systems; however, this may be reportable under CER

One of the key challenges our clients face is the complexity of incident reporting across multiple jurisdictions. Incidents can span several countries – whether it's the source of the incident, cross-border impacts, or supply chain disruptions. While NIS2 sets a harmonised baseline, each Member State maintains its own regulators, reporting portals, and sector-specific requirements. This fragmented landscape can result in duplicative or even conflicting reporting obligations, made more difficult by the absence of a unified EU-wide reporting platform.

Isolating reportable incidents with network segmentation

Implementing appropriate network segmentation can enable organisations to precisely identify and isolate incidents that are reportable under NIS2. By demonstrating that certain incidents are not linked to the critical components that fall within the scope of NIS2 requirements, organisations can streamline reporting processes and reduce the number of incidents flagged for regulatory notification.

Network segmentation is also applicable for securing operational technology. Organisations with the so-called 'flat-pancake' network architecture often lack the necessary segregation, segmentation and zoning essential for protecting critical OT assets and operations.

Network segmentation can therefore serve as a foundational control enabling better isolation of critical systems, limiting lateral movement during an attack, and supporting more precise incident response and regulatory reporting.

Securing Operational Technology

With traditional security efforts focused on IT, the growing need to secure OT introduces significant new challenges. Historically, companies have prioritised operational safety and continuity over cybersecurity in their OT environments, creating a long-standing gap that many organisations are now working to close – driven in part by the urgency of NIS2 compliance. While risk assessments are routine in OT settings, they have often overlooked cybersecurity, leaving critical systems exposed.

Adding to this complexity, local entities and associated sites often struggle to implement effective security measures within the constraints of global strategies. High-level mandates overshadow the specific security needs of individual sites, hindering the deployment of tailored OT security protocols.

To address this gap, organisations must establish clear visibility into their OT environments. Core risk management practices – such as maintaining an asset inventory – are foundational. Asset inventories can also support cybersecurity by enabling effective threat detection, monitoring, and incident response.

Cybersecurity must be fully integrated into OT risk assessments to guide OT security strategy. These assessments should not only reflect the organisation's operational context but also be aligned with evolving cyber threats and regulatory requirements.

Balancing global strategy with local OT security needs is essential. Organisations should enable local teams to implement tailored controls while aligning with corporate and regulatory frameworks, supporting sustainable security and compliance across the organisation.

Supply chain security challenges for customers

Organisations must establish a robust third-party security program under NIS2. There are three key challenges customers face during this process:

1. Lack of visibility: Gaining insights into third-party ecosystems is often challenging. Without a clear understanding of these relationships, organisations find it challenging to assess the operational importance and cyber risk exposure of each third party. It is critical that understanding the third-party population for NIS2 is broader than just IT service providers, but also those key suppliers for business operations (e.g., raw materials supplier).
2. Complexity in third-party risk assessments: Organisations frequently face a complex landscape when conducting supplier risk assessments. Identifying and understanding the potential cybersecurity vulnerabilities introduced by each supplier is crucial for effectively mitigating supply chain risks.
3. Contractual gaps: Many organisations are yet to establish appropriate contracts with suppliers. The lack of essential security clauses leaves organisations exposed to potential breaches and compromises within their supply chain.

To address these challenges, organisations must gain a complete view of their third-party landscape by identifying all suppliers affected by NIS2. This allows organisations to review their existing supplier population as well as establishing an understanding of the risks posed by said suppliers.

Updating contracts with the right security clauses is essential. Asking suppliers to update contractual terms can lead to negotiations, highlighting the importance of a clear contract strategy involving both legal and sourcing teams. Striking the right balance between security requirements and contractual obligations is key to building a secure and resilient supply chain.

Confronting these challenges

Each area reveals that the details and complex nature of NIS2 requirements make compliance far from straightforward, requiring careful analysis and tailored strategies. To navigate these issues effectively, it is essential to integrate the NIS2 compliance topic into the strategic agenda of your organisation. Management should be actively engaged and help to align all affected departments (e.g., legal, supply chain, etc.).

How KPMG can help

Many organisations can see the surface of the NIS2 iceberg on the horizon and prepare for what's visible. However, our experience shows the real complexity lies beneath.

This paper offers a glimpse below the waterline, uncovering challenges such as fragmented local transposition, scoping grey areas across organisational and legal structures, inconsistent incident response timelines, securing operational technology amid IT/OT convergence, and ensuring full visibility into supply chains and interdependencies. These are just some examples of the true depth of NIS2 compliance.

Building on our experience, we offer an end-to-end program that supports organisations in achieving their compliance goals – from scoping analysis and project management to risk assessments, improvement plans, roadmaps, and full implementation.

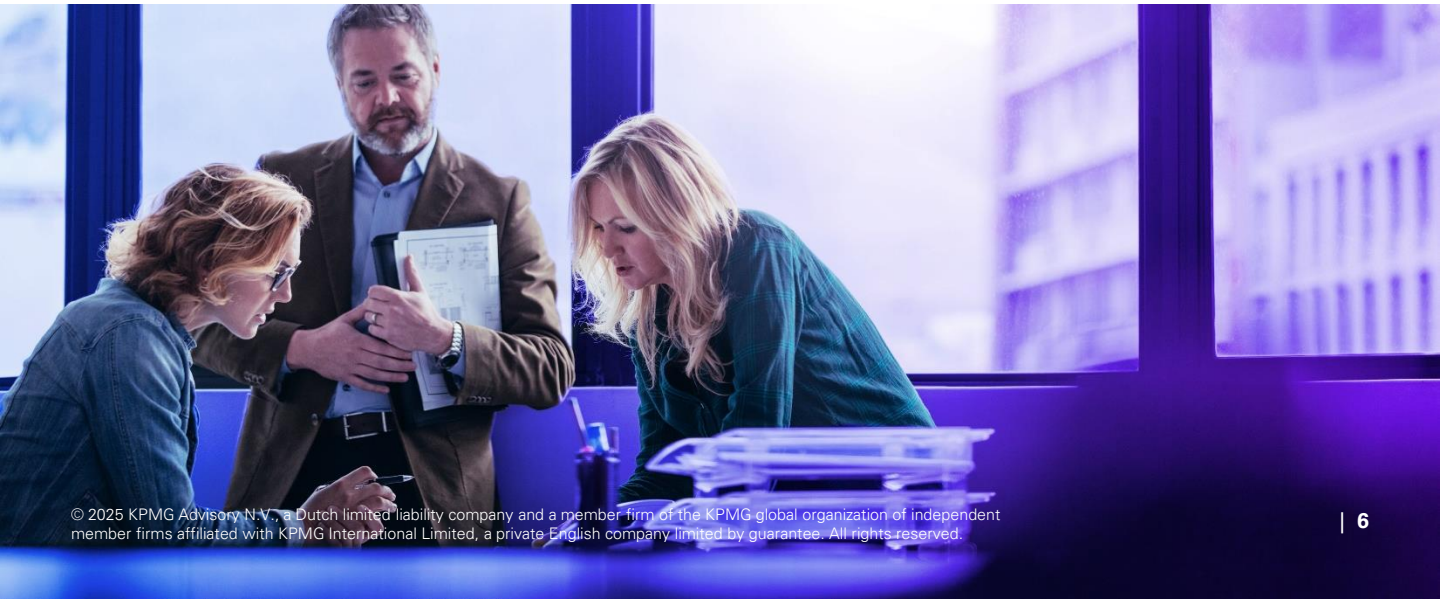
As a trusted partner, we are there every step of the way, providing tailored support to meet each client's specific needs.

KPMG have conducted multiple NIS2 improvement programs and have a specialist team capable of conducting a multi-phase program to assist with NIS2 readiness.

Implementation support

This approach is designed for organisations that wish to immediately address the common challenges addressed in this whitepaper. Our discussions centre around topics such as:

- **Management body accountability |** To ensure management body accountability, organisations should assess training needs, tailor interactive sessions to specific roles, comply with legal requirements, and document all activities and feedback.
- **Incident response and reporting |** Incident response and reporting involve assessing readiness and creating strategies to rapidly contain incidents to mitigate damage.



- OT Security | Preparing for NIS2 involves thoroughly assessing and securing your operational technology (OT) environment. This includes identifying assets, integrating security measures, managing updates, monitoring threats, and ensuring secure access to systems.
- Third-party risk management | Organisations should focus on key projects for third-party risk management, including identifying third parties, developing and integrating a TPRM strategy, and assessing the effectiveness of these measures.

Assessment

In some cases, our clients start with an assessment to gain a clear understanding on how NIS2 affects the company, and to develop a clear action plan to prepare for implementation.

- Scope analysis | Applicability assessment to determine which products and / or services are within the scope of NIS2, incorporating supply chain considerations.
- Gap and risk assessment | Combination of the scope analysis with NIS2 requirements to create short-term action plans in a compliance remediation plan. A central gap analysis and local risk assessments are conducted.
- Action Plan | Creation of a practical remediation plan with short- and long-term action plans, advising on how to build measures with an additional legal review.

We act as your trusted partner throughout the entire project, from determining scope to implementing and monitoring controls.

Take action today and leverage our specialised services to fortify your organisation's cybersecurity posture in alignment with the NIS2 Directive.

Our experts

Ronald Heil
Partner - Cyber & TechLaw
KPMG Advisory N.V.
heil.ronald@kpmg.nl
+31 (0)6 51369785

''Working with many national and international organisations it is a pleasure to see that society takes NIS2 seriously and that we already have improved our security posture and operational resilience compared to pre-NIS2 period. That being said, many need help with the "iceberg".

Michiel van Veen
Director - Cyber & TechLaw
KPMG Advisory N.V.
vanveen.michiel@kpmg.nl
+31 (0)6 52078818

''Steering NIS2 programs has shown me the challenge organisations face in the forthcoming cybersecurity compliance landscape. It has a critical role in shaping broader C-level decisions. Confronting the challenge of NIS2 not only addresses risks effectively but it can also be a strategic enabler in driving business success''.

Hamish Wishart
Senior Consultant - Cyber & TechLaw
KPMG Advisory N.V.
wishart.hamish@kpmg.nl
+31 (0)6 23034710

Meret Keeris
Manager - Cyber & TechLaw
KPMG Advisory N.V.
keeris.meret@kpmg.nl
+31 (0)6 10905367