NIS2 (Cbw) Update

KPMG Netherlands

July 2026

Building on our earlier NIS2 publications from 2023 and 2025, which covered the Network and Information Security Directive's (NIS2) impact on IT and OT as well as practical lessons learned from client engagements and insights shared within the KPMG EMA community, this update looks at the next phase of NIS2 readiness in the Netherlands. With the Dutch Cyberbeveiligings-wet (Cbw) entering its final legislative stage, organisations should no longer treat NIS2 as a topic to monitor from a distance. The focus is now shifting towards concrete preparation, implementation and demonstrable readiness.

From interpretation to execution

NIS2 is no longer a topic that organisations can push down the line. For Dutch organisations, the Cbw has now passed the final stage of the legislative process, following debate and voting in the Senate on 6 and 7 July 2026. The law will enter into force on 15 August 2026, marking a clear shift from legislative monitoring to practical implementation.

After a period in which many organisations focused primarily on understanding the Directive and assessing its relevance, the focus now needs to shift towards implementation, prioritisation and auditable readiness. This requires concrete decisions around scope, ownership, dependencies and assurance. In practice, this means confirming which legal entities, services and activities are in scope, assigning clear accountability across business, IT, security and supply chain functions, and preparing evidence that controls and reporting arrangements work in day-to-day operations.

The key question is therefore no longer only "Are we in scope?", but "What do we need to do now to be ready, defensible and demonstrably in control?

What organisations should do now

- Confirm scope: determine which legal entities, services, activities and dependencies fall within scope of NIS2 and the Cyberbeveiligingswet (Cbw).
- Assign ownership: clarify accountability across management, business, IT, security, legal and supply chain functions.

- **Prioritise implementation:** identify the most critical gaps in risk management, incident reporting, supplier security and governance, and translate these into a concrete action plan.
- **Build evidence:** document decisions, controls, reporting lines and implementation progress so that readiness can be demonstrated in practice.

The focus is now on demonstrable action and effective control. Boards, regulators and customers increasingly expect organisations to show not only that policies exist, but that decisions, controls and reporting arrangements work in practice.

EU-level refinements to NIS2

On 20 January 2026, the European Commission proposed targeted amendments to NIS2 as part of a broader cybersecurity package, alongside a proposal to revise the Cybersecurity Act. The official framing is clear: the package is intended to strengthen EU cyber resilience while also simplifying compliance, reducing fragmentation and making ENISA more operationally effective.

The Commission explicitly presents the NIS2 amendments as a simplification exercise. According to its published Q&A, the changes are intended to increase legal clarity, reduce unnecessary administrative burden for 28,700 companies, including 6,200 micro- and small-sized enterprises, and introduce a new small mid-cap category to reduce compliance costs for a wider group of organisations. This is a strong indication that implementation frictions are now being addressed at EU level, even while national rollout is still ongoing.

What the amendments are trying to achieve

- Simplification of scope and jurisdiction to reduce uncertainty and lower compliance burden.
- More harmonised supervisory tools, especially for cross-border entities, with a stronger coordinating role for ENISA.
- Streamlined ransomware-related reporting and data collection, reflecting the growing role of ransomware as a regulatory and operational concern.
- Closer alignment with the revised Cybersecurity Act, particularly through certification-based compliance pathways and a broader EU certification architecture.

The scope refinements are also important in practical terms. The proposal explicitly brings operators of submarine data transmission infrastructure and providers of European Digital Identity Wallets into the category of essential entities, while also refining scope language in existing sectors such as energy and chemicals. This confirms that scoping remains a live issue, not a closed exercise.

Practical implications for organisations

For in-scope organisations, the message is not to pause NIS2 implementation while waiting for the final amendment text. The 2026 package should be treated as a direction of travel, not a reason to delay. Organisations should continue building against the current NIS2 baseline, while monitoring potential changes in areas such as scope, certification, ransomware reporting, ICT supply chain security and cross-border supervision.

What NIS2 implementations are teaching us

Across our work with organisations preparing for NIS2, five practical lessons stand out:

1. Scoping remains one of the hardest problems in practice
2. End-to-end business processes also include supply chain dependencies
3. Accountability goes beyond management body training
4. Incident reporting still raises operational questions
5. Country-specific deviations that still matter

1. Scoping remains one of the hardest problems in practice

Understanding applicability under NIS2 remains one of the most challenging aspects of implementation. While the intent of the Directive is clear for many organisations, real complexity arises when translating sector definitions into legal entities, products, services and operations. Determining which activities are in scope, how these align with Annex I or II, where the relevant operations are performed and how national transpositions interpret these factors often proves more complex than expected.

Once translated into real-world business operations, where activities, services and legal entities cut across sectors, functions and countries, scoping becomes a far more nuanced legal and organisational exercise rather than a straightforward classification.

Beyond legal entities: scoping NIS2 through critical service delivery

NIS2 scoping cannot be addressed through legal entity assessments alone. Organisations also need to understand how end-to-end business processes operate, which services are critical to NIS2-relevant activities, and which systems, sites and functions support those services. These processes are rarely self-contained; they are supported by shared systems, platforms and functions that cut across organisational, national and EU boundaries. For multinational organisations, this includes assessing whether disruptions in non-EU activities or shared support functions could cascade into significant incidents affecting an in-scope EU entity.

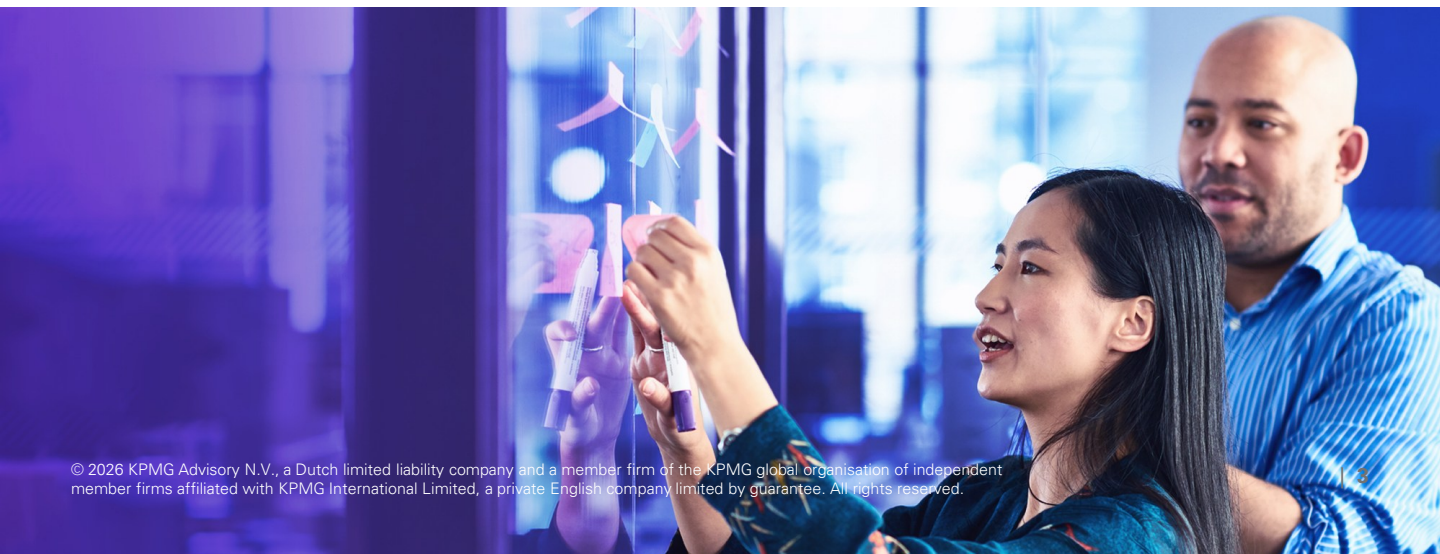
As supervisory focus sharpens, end-to-end visibility and an understanding of dependencies have become core requirements for correct NIS2 scoping and effective risk management.

Furthermore, while EU scope definitions provide the baseline, national implementations can narrow, expand or complicate its application. The 2026 amendment proposal reinforces that scoping should not be seen as a one-off exercise, but something organisations need to revisit as laws, technologies and business models evolve.

2. End-to-end business processes also include supply chain dependencies

A key challenge for both scoping and implementation is gaining a clear view of how supply chain partners and third parties support end-to-end business processes.

Supply chain dependencies under NIS2 extend beyond traditional IT suppliers. They may include logistics providers, subcontractors, site dependencies, external support services and non-EU third parties that contribute to the delivery of critical or NIS2-relevant services.



In practice, organisations need to understand not only who their suppliers are, but also which processes, systems, sites, applications and external dependencies support their critical services. Without this end-to-end view, it becomes difficult to identify critical dependencies, apply proportionate security measures and reduce the risk of cascading disruption that could lead to a reportable incident.

As NIS2 implementation progresses, many organisations are also seeing a rapid increase in supply chain requests, including questionnaires, contractual assurances and evidence of cybersecurity controls. To manage this efficiently, organisations should move towards structured third-party risk management, including standardised TPRM playbooks, defined supplier requirements, expected response models and evidence expectations.

3. Accountability goes beyond management body training

In our 2025 NIS2 Market Update, we already identified management body accountability as a recurring implementation challenge. At the time, organisations were still trying to interpret what "management body" means in practice and how accountability should be organised across legal entities, centralised security functions and multinational operating models.

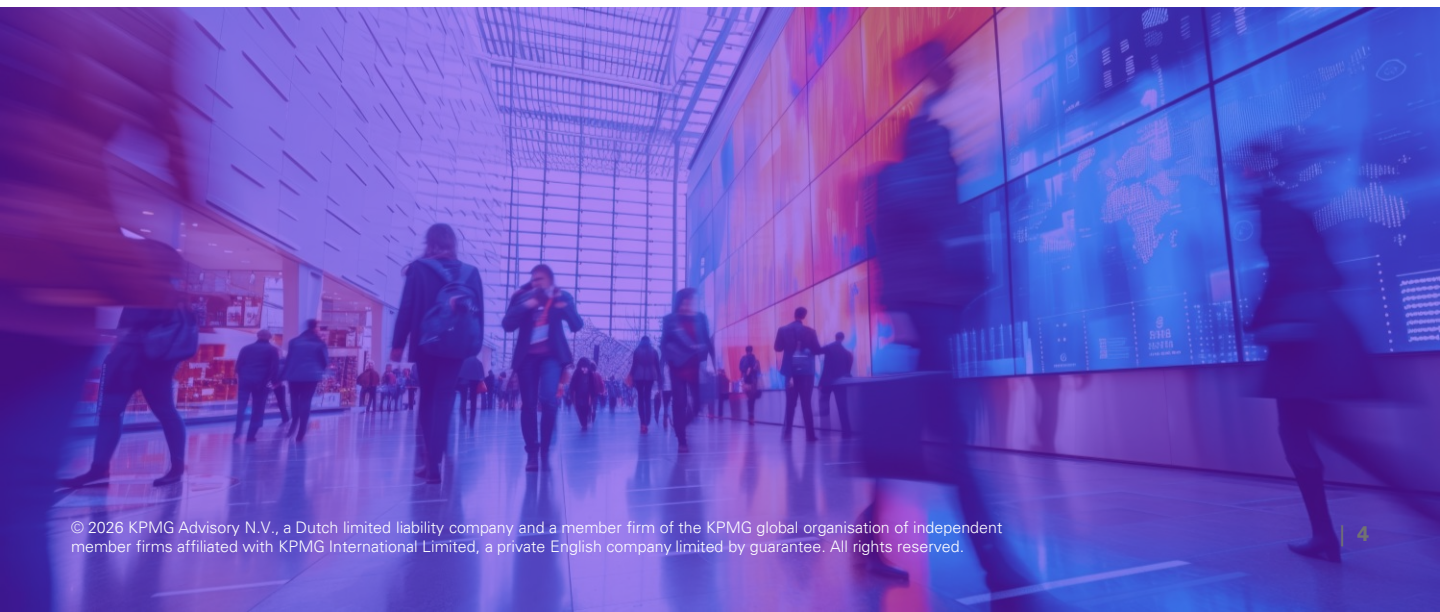
In 2026, this discussion has become both more concrete and more nuanced. The dividing line between governance models is not always clear. In some organisations, accountability is concentrated at the executive board level. In others, accountability is blurred across the Board of Management, group functions, local entity management, and line management, with supervisory bodies providing oversight. This raises practical questions around who is formally accountable under NIS2 and whether supervisory boards, while not accountable, may still face liability if oversight proves insufficient.

Under NIS2, the Board of Management has a clear role in approving cybersecurity risk-management measures, overseeing implementation and ensuring that the right structures, resources and reporting are in place. In two-tier models, however, the Supervisory Board becomes an important discussion point. It does not execute the NIS2 programme, but may be relevant from an oversight perspective by challenging management, requiring evidence-based reporting and ensuring that oversight actions are documented.

Line management adds another layer to this accountability discussion. While not necessarily part of the statutory management body, it is often where cyber risk decisions become operational. This means organisations need to clearly define how accountability flows across the different layers of governance: from approval and oversight to execution, escalation and evidence.

Training is only the starting point

A common misconception is that this accountability challenge can be addressed through a one-off management body training session. Training is important, but it does not resolve the underlying governance question. The practical lesson is that NIS2 accountability is becoming less about awareness alone and more about demonstrable governance across organisational types.



4. Incident reporting still raises operational questions

The formal NIS2 incident reporting timelines – 24-hour early warning, 72-hour notification and one-month final report – are only part of the challenge. In practice, organisations often struggle less with the existence of these deadlines and more with the operational questions that sit behind them:

- When does an incident qualify as "significant"?
- If an organisation's risk appetite is higher than the defined NIS2 incident reporting threshold, can it adjust the threshold?
- When has the organisation "become aware" of a significant incident?

These questions become more complex where incidents have cross-border impact or affect international supply chains. Organisations may need to determine where the incident occurred, which services are affected, whether those services are in scope of NIS2, whether there is cross-border impact and whether national or sector-specific rules apply.

Incidents with cross-border impact often require coordination across multiple national authorities and CSIRTs. While EU-level cooperation mechanisms exist, including the CSIRTs Network and EU-CyCLONe supported by ENISA, organisations still need to manage the practical reporting implications during the incident itself. This may include identifying which national obligations apply, aligning internal decision-making, preparing consistent information for different authorities and managing potentially differing reporting channels, timelines and information requirements.

There is no one-size-fits-all approach to addressing these operational questions. However, in our experience, organisations are better positioned when they define these decisions in advance and embed them into their incident response process. In practice, the following can help:

Because NIS2 is risk-based, organisations are defining and documenting their own thresholds for determining 'significance', provided these remain aligned with legal reporting criteria and are reasonable, consistently applied and supported by documented decision-making.

- Significance should not be assessed by incident size alone. Under NIS2, context matters: the affected service, its role in society, the potential impact on continuity and the effect on other parties may all be relevant. For example, a short disruption at an energy company may still be NIS2-relevant if it affects, or could affect, the continuity of an essential service, even where the organisation recovers quickly.
- Organisations should define and document when they consider themselves to have "become aware" of a NIS2-relevant significant incident. This is often not every technical alert, but the point at which the organisation has sufficient information to reasonably determine that the incident may meet the applicable NIS2 reporting threshold.

5. Country-specific deviations that still matter

Despite efforts to harmonise NIS2 at EU level, implementation still differs significantly across Member States. The Directive provides a common baseline, but national laws vary in their timing, registration obligations, supervisory approach, reporting channels and the level of detail already available to organisations.

For organisations falling under the Dutch implementation of NIS2, the Cbw, the focus is now shifting from preparing for forthcoming obligations to ensuring readiness for obligations that will soon formally apply. In April 2026, the House of Representatives approved the Cbw alongside the Wet weerbaarheid kritieke entiteiten (Wwke), which complements the Cbw by addressing the broader resilience of critical entities, including physical and other non-cyber disruptions. On 7 July 2026, the Senate adopted both bills, confirming the final step in the legislative process. The Cbw and Wwke will enter into force on 15 August 2026. Dutch authorities have also made clear that organisations should not wait for the formal start date, but should already be preparing.

In other Member States, supervisory expectations are already more concrete. Belgium is a clear example of evidence-based ex-ante supervision: essential entities were required to submit information and supporting evidence by 18 April 2026, allowing the CCB to verify their cybersecurity posture before incidents occur. Germany illustrates another implementation pattern, where core obligations applied immediately upon entry into force and in-scope entities had to register with the BSI within three months.

The practical implication is that organisations should treat country-specific implementation as an active part of their NIS2 programme, not as a legal follow-up exercise. A group-level NIS2 baseline can provide consistency, but it needs to be supplemented with country-level monitoring, local ownership and jurisdiction-specific decisions on scope, registration, reporting and evidence requirements. This helps organisations maintain consistency at group level while still responding to the supervisory expectations that apply in each Member State.

How KPMG can help

We approach NIS2 as a practical, cross-functional implementation challenge, helping organisations navigate legal scoping, national requirements, IT and OT environments, supply-chain dependencies and management oversight. The aim is not just to understand the rules, but to translate them into an approach that works in daily operations and demonstrates control. This is where KPMG adds value.

Scoping and applicability

We help organisations determine which legal entities, services, activities and dependencies are in scope of NIS2. This includes Annex I and II interpretation, national implementation requirements, cross-border considerations and supply chain dependencies.

The aim is to develop a scope position that is legally sound, explainable and maintainable as requirements and business operations evolve.

End-to-end NIS2 delivery

We support the full NIS2 implementation journey, from scoping and readiness to remediation, implementation and embedding into business-as-usual operations. This includes implementation roadmaps, governance and ownership, policy and control uplift, incident reporting, supply chain security, IT/OT considerations and management oversight.

Independent third-party assessment of NIS2 programmes

We provide independent assessments of NIS2 programmes to help organisations understand whether their approach is sufficiently complete, coherent and demonstrable. This can include reviewing the design and implementation of the NIS2 programme, assessing alignment with applicable requirements, and identifying areas where further evidence, control maturity or governance clarity may be needed.

An independent assessment can support management and board-level assurance by providing an objective view on progress, key residual risks and the extent to which NIS2 readiness can be evidenced. This is particularly relevant where organisations have already started implementation and want to validate whether their programme is on track before moving further into BAU.

NIS2 Board Training Sessions

We deliver tailored NIS2 board training sessions to help management bodies understand their responsibilities, key decision points and oversight role under NIS2. Sessions can be adapted to the organisation's sector, operating model and maturity, and typically cover board accountability, cyber risk governance, incident reporting, supply chain dependencies, OT considerations and practical scenarios relevant to the organisation.

NIS2 is now moving from interpretation to execution. As national laws take effect and supervisory expectations become more concrete, organisations should focus on building a NIS2 approach that is not only compliant on paper, but operationally embedded, evidence-based and adaptable across jurisdictions. This means maintaining a clear view of scope, critical services, dependencies, incident reporting obligations and management accountability, while ensuring that decisions and controls can be demonstrated in practice.

Our experts

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

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