CYLUS

WHITEPAPER

Comparative Analysis of NIS2 Transposition in EU Member States

Table of Contents

Comparative Analysis of NIS2 Transposition in EU Member States

As Europe raises the bar on cybersecurity, the NIS2 Directive (Directive (EU) 2022/2555) sets a baseline of cybersecurity risk management measures for Essential and Important Entities across the EU. While most Member States adopt the baseline requirements, such as policies, incident response, business continuity, supply chain security, and secure development, many also introduce specific national provisions.

Below, we survey each Member State's NIS2 transposition (or draft), highlighting references to security monitoring (e.g, threat detection, SOC/SIEM, anomaly/intrusion detection, continuous monitoring) and network visibility (e.g., traffic analysis, asset inventory, logging, OT/IT visibility). We note whether these go beyond NIS2's initial text, their mandatory/recommendatory nature, and which entity categories (Essential Entities – EEs, Important Entities – IEs, or other) are impacted. A summary table of notable additional requirements follows the country analyses.

This document reflects the status of NIS2 transpositions across EU Member States as of July 2025. National implementations and interpretations continue to evolve, with some legislative drafts still under discussion or pending formal adoption.

For questions or if you require the most up-to-date information, please contact info@cylus.com.

Overview of National Transpositions

Country	Legislation	Notable Monitoring & Visibility Provisions	Beyond the NIS2 Baseline?
AUSTRIA	Draft Federal Cybersecurity Act (NIS2 transposition)	References a detailed "Risk Management Catalogue" for security measures; requires entities to register their IP addresses with authorities (NIS2 Directive Transposition Tracker - ECSO).	Yes – prescribes additional guidance (catalogue) and data (IP) beyond NIS2.
BELGIUM	Law of 26 April 2024 (NIS2 law, in force 18 Oct 2024)	Requires a coordinated vulnerability disclosure policy for companies (EU NIS2 in Belgium – OpenKRITIS); Art 30 mandates preventive measures to ensure service continuity even under exceptional network failures (NIS2 Compliance: Interpreting 'State-of-the-Art' for Organisations). Baseline NIS2 measures (logging, incident handling, etc.) apply to all in-scope entities.	Yes – adds specific obligations (disclosure policy, continuity measures) beyond NIS2 text, mandatory for Essential Entities (and some for Important Entities).
BULGARIA	Draft amendment to the Cybersecurity Act (submitted 12 Dec 2024; first reading completed; adoption expected Q3 2025)	The draft closely aligns with the NIS2 baseline for transport, including rail. No public provisions mandate enhanced monitoring, SIEM, or continuous logging beyond NIS2 requirements. Technical details—including logging, visibility, and sector-specific guidance—are expected to be specified through secondary legislation once enacted.	No – expected to follow NIS2 baseline; sector-specific controls pending further regulation.

Country	Legislation	Notable Monitoring & Visibility Provisions	Beyond the NIS2 Baseline?
 CROATIA	Cybersecurity Act (Zakon o kibernetičkoj sigurnosti, NN 14/2024, in force 15 Feb 2024)	Explicitly requires incident monitoring and logging: e.g., “Postupanje s incidentima, uključujući njihovo praćenje, evidentiranje i prijavljivanje” – incident handling including their monitoring, recording, and reporting (Art. 30(1)(b)) ([NIS2 Croatia	Članak 30.1.b (logs)
 CYPRUS	Network and Information Systems Security (Amendment) Law 2025 (adopted 25 Apr 2025)	The amendment formally implements NIS2 as of 25 April 2025, expanding the class of Essential and Important Entities to include sectors such as transport (including rail). Rail operators must now comply with standard NIS2 obligations like incident reporting and risk assessment. No sector-specific mandates for continuous monitoring, SIEM, or advanced visibility tools have been announced in secondary regulation as of July 2025.	No – it mirrors NIS2 baseline. No additional rail-specific visibility or monitoring obligations are in force yet.
 CZECHIA	Cybersecurity Act2025 (final draft July2025; expected effective1 Nov2025)	Rail services are explicitly included in the “Strategically Important Services” tier within the transport sector. Operators in this tier must implement ISO-based ISMS, continuous monitoring, control catalogues, redundancy, and supply chain security. These obligations are mandated via implementing decrees accompanying the Cybersecurity Act.	Yes – Czechia exceeds the NIS2 baseline with prescriptive, mandatory monitoring and visibility obligations for rail.
 DENMARK	Sector-specific Cyber & Information Security Acts (bills tabled 6 Feb 2025; staggered entry into force 7 Mar – 1 Jul 2025)	Rail is covered as part of Denmark’s transport-sector approach. The legal texts do not impose statutory monitoring or logging requirements. Future technical obligations, such as visibility or detection mandates, may be introduced by the Centre for Cyber Security (CFCS) via binding guidance.	N/A – legislation follows NIS2 baseline; rail-specific visibility rules not yet defined.
 ESTONIA	Draft pending (minimal progress)	Little information available (The NIS2 directive in the EU: A country-by-country breakdown). Estonia is expected to update its Cybersecurity Act to mirror NIS2’s requirements. No known additional references to continuous monitoring or network visibility beyond the Directive’s list at this stage.	N/A - likely no, will follow baseline obligations.
 FINLAND	Cybersecurity Act (124/2025), adopted Mar 2025; in force Apr 2025	Rail infrastructure operators are treated as Essential or Important Entities and must implement baseline NIS2 controls. No national requirements mandate sector-specific real-time monitoring, audit logging, or visibility technologies. Technical detail is provided through non-binding recommendations from the Finnish Transport and Communications Agency, Traficom.	No – obligations match NIS2 minimum; no added Finnish visibility or monitoring mandates.

Country	Legislation	Notable Monitoring & Visibility Provisions	Beyond the NIS2 Baseline?
FRANCE	Draft NIS2 law (Senate version adopted March 2025)	France's Senate passed a version of the NIS2 transposition law in March 2025. The law is expected to be finalized in the second half of 2025. The implementation is anticipated to integrate NIS2 into existing frameworks (e.g., SecNumCloud and sectoral rules for operators of vital importance), but the final version has not yet clarified whether any enhanced monitoring or network visibility requirements will be imposed beyond thenis 2 directive.	N/A – likely minimal deviations. (France historically enforces strong security for critical operators, so implementation could equal or exceed NIS2, but specifics TBD.)
GERMANY	Draft NIS2-Umsetzungsgesetz (NIS2UmsuCG) – (revised draft publishedJune 2025)	The government's draft, NIS2UmsuCG, was passed to Parliament in July 2024 and remains under review; a revised draft was issued in June 2025. It mandates BSI-powered classification of "essential" and "important" entities, registration within three months of designation, and robust obligations such as incident reporting and log-based monitoring.	Yes – it codifies continuous monitoring, registration duties, and real-time log obligations via BSI guidance and draft law.
GREECE	Law 4577/2024 (published Oct 2024, in force 27 Nov 2024)	Transposition law closely follows NIS2's provisions (covering EEs and IEs). It introduced graded penalties for different levels of offenses (minor, significant, serious), refining the NIS2 sanction regime (NIS2 Directive Transposition Tracker - ECSO). References to security monitoring and network visibility in the text mirror the Directive (e.g., requiring incident handling processes, logging, etc., for in-scope entities) – no evidence of Greece adding new technical mandates beyond the NIS2 baseline.	No (mostly) – aside from stricter penalty structuring, Greece's law stays within NIS2's requirements. All baseline measures (incident monitoring, logging, etc.) are mandatory for Essential/Important entities, as per NIS2.
HUNGARY	Act XXIII of 2023 (Cybersecurity Certification and Cybersecurity Supervision Act, in force 23 May 2023)	Extends NIS2 significantly: All covered "high-risk" and "at-risk" sector organizations must classify their systems into security tiers and implement controls accordingly (Hungary: Cybersecurity Laws – The Saga Continues) (Hungary: Cybersecurity Laws – The Saga Continues). A ministerial decree provides a Threat Catalogue that must be used to identify risks ([NIS2 Directive: The deadline for the registration of entities in Hungary is 30 June 2024	DLA ((Piper)). Bi-annual independent audits are compulsory – entities had to hire an accredited cybersecurity auditor by the end of 2024 and undergo audits every 2 years to prove appropriate measures. ([NIS2 Directive: The deadline for the registration of entities in Hungary was 30 June 2024.
IRELAND	Draft Cybersecurity Act (published Q2 2025; under consultation)	Ireland published its draft NIS2 transposition in mid-2025, assigning supervisory responsibilities to the Department of the Environment, Climate and Communications (DECC). The draft mirrors NIS2's baseline obligations, including mandatory logging, risk management, and incident response procedures. A national register of Essential and Important Entities will be created. No Ireland-specific technical enhancements have been introduced, but entities are expected to follow guidance issued by the National Cyber Security Centre (NCSC-IE).	No – Ireland follows NIS2's structure with minimal national additions; further obligations may follow in sectoral guidance.

Country	Legislation	Notable Monitoring & Visibility Provisions	Beyond the NIS2 Baseline?
 ITALY	Legislative Decree No. 138/2024 (4 Sept 2024, in force 16 Oct 2024)	Italy's decree largely mirrors NIS2 requirements. It repeals the old NIS1 law and imposes NIS2's measures on a broadened set of entities (Direttiva NIS2: le novità del decreto di recepimento in GU - DB). Key obligations like risk analysis policies, incident handling (with detection and reporting), and logging are included as per NIS2. Italy did not introduce new technical controls beyond the directive, but it did refine enforcement: e.g., tiered fine levels for different severities and specific liability for management (aligning with NIS2's governance provisions) (NIS2 Directive Transposition Tracker - ECSO). No explicit mention of SOC or network monitoring beyond what NIS2 prescribes (though Italian guidance may encourage alignment with national cybersecurity framework standards).	No significant additions – Italy's transposition is faithful to NIS2's text. All NIS2 baseline security measures are mandatory for Essential/Important entities. (Financial sector entities are mostly handled via DORA, not NIS2 (NIS2 Directive Transposition Tracker - ECSO).)
 LATVIA	National Cyber Security Law (adopted June 2024, in force Sept 2024)	Goes beyond NIS2 in organizational measures: entities must appoint a Cyber Security Manager by October 2025 and submit an annual self-assessment report on cyber risks by that date (Summary of Latvia's New National Cyber Security Law).	The law enforces "minimum cybersecurity requirements" (detailed in regulations) for all in-scope organizations.
 LITHUANIA	Law on Cyber Security (amended 2024)	The amended Lithuanian Cybersecurity Act closely follows NIS2's content (What Does the Lithuanian Cybersecurity Act Require? - Advisera) ([Key Implications of the EU's NIS 2 Directive Insights - Skadden)	It maintains the same scope criteria and risk-based approach. Core requirements – e.g., conducting risk assessments, implementing security measures (including network traffic monitoring, logging, etc.), and incident reporting – are adopted essentially verbatim from NIS2 (Lithuania - NIS2 Implementation in the EU - Lex Mundi). One notable addition: senior management liability is emphasized (as in NIS2) and possibly extended to public-sector entities. However, no unique national technical controls (such as specific tools or monitoring systems) were introduced; Lithuania opted to mirror the directive's main points.

Country	Legislation	Notable Monitoring & Visibility Provisions	Beyond the NIS2 Baseline?
 LUXEMBOURG	Draft law (public consultation mid-2024)	Luxembourg's draft NIS2 law was under discussion in 2024; as of mid-2025, the law remains unenacted. It generally aligns with NIS2 but is considered unique enforcement tweaks – e.g., extending fines to public bodies (applying GDPR-like penalty concepts to government agencies) (NIS2 Directive Transposition Tracker - ECSO). On security measures, the draft text did not add new obligations for monitoring or visibility; it sticks to the directive's list (risk management, incident detection and response, logging, etc.). The national cyber authority will likely issue guidance, but the law itself is expected to mirror NIS2's requirements for continuous monitoring and network security at a high level.	No - apart from enforcement nuances. All NIS2 baseline measures will be mandatory for Essential/Important entities in Luxembourg once adopted, but no evidence of extra technical requirements in the draft.
 MALTA	Draft pending (Minimal progress by Oct 2024)	Malta had not published a NIS2 transposition law by the deadline (The NIS2 directive in the EU: A country-by-country breakdown). It is anticipated that Malta will transpose the directive largely as-is. There's no indication of additional Maltese requirements regarding security monitoring or network visibility at this time. (Malta's small size and reliance on EU directive text suggest a direct transposition approach.)	N/A – Likely no deviations. Standard NIS2 obligations (including monitoring/logging as part of risk management) will become mandatory when enacted.
 NETHERLANDS	Amendment to Wbni (adopted June 2025)	In June 2025, the Netherlands adopted its Wbni amendment to implement NIS2. While baselining NIS2 log, detection, and reporting obligations, the law empowers sectoral regulators (e.g., NCSC-NL) to issue binding technical guidance (released July2025).	No significant additions. NIS2 baseline (monitoring, anomaly detection, logging obligations) will apply as mandatory minimums for Dutch Essential and Important entities, with details possibly handled via secondary legislation or guidance.
 POLAND	Draft Act to amend the National Cybersecurity System Act (published 2024; expected adoption 2025)	Poland's draft is considered the strictest in the EU (NIS2 implementation January 2025). It goes far beyond NIS2: notably, it empowers authorities to exclude "High-Risk ICT Vendors" from supply chains across 18 sectors, extending the EU 5G Toolbox principles to other critical sectors (NIS2 implementation January 2025). This affects network visibility indirectly – entities must have insight into their network components and suppliers to comply. The draft also proposes more stringent requirements for certain sectors (telecom, energy, etc.), potentially including enhanced monitoring obligations (though details are under inter-ministerial review). Standard NIS2 controls (incident monitoring, logging, etc.) are all mandatory, and Poland may add to them: e.g., its existing law already requires operators to implement continuous monitoring and have 24/7 incident response capabilities. The new draft continues that spirit of proactive threat detection.	Yes – Poland is innovative and strict in its approach, using NIS2 as a floor and adding supply-chain monitoring and other sector-specific controls. All these would be mandatory; the government justifies this rigor by Poland's status as one of the most cyber-attacked EU countries (NIS2 implementation January 2025).

Country	Legislation	Notable Monitoring & Visibility Provisions	Beyond the NIS2 Baseline?
 PORTUGAL	Regime Jurídico da Cibersegurança (NIS2 transposition; proposal approved Feb 2025)	In February 2025, Portugal's Cabinet approved the draft law for public consultation, expanding the cybersecurity regime, increasing CNCS supervisory powers, and adjusting obligations by organisational size and criticality. Continuous monitoring and incident-reporting obligations are tiered and proportionate; major fines and restrictions on high-risk suppliers are also included.	Yes – Portugal introduced proportional, tiered reporting and monitoring based on criticality, adding extended enforcement mechanisms.
 ROMANIA	GEO No. 155/2024 (Government Emergency Ordinance, adopted 31 Dec 2024)	Romania's NIS2 transposition introduces strict governance and oversight obligations for Essential and Important Entities. Organizations must conduct and submit annual cybersecurity self-assessments evaluating risk-management maturity to the National Cybersecurity Directorate (DNSC), and implement DNSC-approved risk management measures, which will likely include requirements for continuous monitoring, log analysis, and network oversight once finalized in 2025. Entities must appoint a dedicated NIS Officer responsible for network and information systems security, while management bodies are explicitly accountable for approving and supervising cybersecurity measures. Regular security audits are mandated, and board members are required to complete accredited cybersecurity training—ensuring that both technical controls and governance practices are strictly implemented and monitored.	Yes – Romania imposes strict procedural obligations beyond NIS2 (self-assessment reports, named security officers, mandatory training). These are mandatory for all Essential/Important entities. The actual security measures (monitoring, etc.) will be further detailed by DNSC secondary regulations in 2025 (Transposition of the NIS2 Directive in Romania), likely making robust threat detection and network visibility a clear expectation.
 SLOVAKIA	Act on Cybersecurity (amended, adopted 28 Nov 2024, in force Jan 2025)	Slovakia managed to pass its NIS2 law by late 2024 (NIS2 implementation January 2025). The law updates the existing Cybersecurity Act with NIS2 terms. It stays largely within the directive's scope but introduces some timing and oversight tweaks. For example, entities must register within a short period and implement measures within one year of registration (EU NIS2 in the Czech Republic – OpenKRITIS). There is an emphasis on continuous compliance: supervised entities can be subject to audits and are expected to maintain evidence of risk management (which implies keeping logs and monitoring records for ex-post review). The law itself does not list new security measures beyond NIS2's list, but Slovakia's National Security Authority may issue guidelines. No unique provisions on SOCs or network mapping have been reported.	No major additions – aside from administrative differences (deadlines, etc.), Slovakia's requirements on monitoring and visibility match NIS2's baseline (and are mandatory for EEs/IEs).

Country	Legislation	Notable Monitoring & Visibility Provisions	Beyond the NIS2 Baseline?
 SLOVENIA	Cybersecurity Act (adopted Q1 2025; in force July 2025)	The act transposes NIS2 into Slovenia's legal framework. Obliged entities must conduct risk assessments, maintain structured logging, implement incident response capabilities, register via a new self-registration portal, and submit incident reports to the Information Security Administration (URSIV). It expands the scope to include approximately 6,000–8,000 essential entities, with penalties prescribed for non-compliance.	Yes – the act extends oversight with mandatory self-registration, expansive entity coverage, and formal administrative enforcement through URSIV.
 SPAIN	Draft law under parliamentary review (Council approval Jan2025)	Spain's draft NIS2 transposition introduces structural enhancements beyond the directive. On 14 January 2025, Spain's Council of Ministers approved the Draft Law on Cybersecurity Coordination and Governance to urgently transpose NIS2 into national legislation. The law establishes a centralized National Cybersecurity Center (CNCS), which will coordinate national-level cyber defense and act as the single point of contact with EU authorities. Under the draft, entities must classify themselves as Essential or Important and register with the CNCS. It also mandates centralized incident reporting via a new National Cyber Incident Notification and Monitoring Platform, which will integrate with existing systems such as INCIBE-CERT and CCN-CERT. Essential Entities are expected to implement continuous monitoring, undergo periodic external certifications, and meet enhanced reporting obligations aligned with Spain's National Security Framework (ENS). Although the final legal text is still under parliamentary review, it is expected to formalize logging and network surveillance requirements. Though the final language is pending.	Yes – the draft law expands oversight by creating a central authority (CNCS), requiring structured reporting mechanisms, and imposing certification and monitoring expectations consistent with Spain's existing ENS.
 SWEDEN	Draft law (published 2024; expected in force mid-2025)	The Swedish draft transposition law largely adopts NIS2 but with some deviations tending toward stricter implementation (NIS2 implementation January 2025). Concerns raised include the burden on single businesses of being subject to many sectoral authorities and clarity on board liability. Sweden is likely to enforce board accountability firmly (potentially making it an explicit legal obligation for directors to ensure cyber monitoring is in place, although NIS2 already implies this). No specific new technical controls are detailed in public summaries of the draft. However, Sweden's approach to incident reporting is already strict, and we can expect that the law will not leave much "open to interpretation" – e.g., requiring systematic logging and prompt detection mechanisms as a clear legal duty. The implementation timeline is short, pushing companies to quickly achieve visibility over their IT/OT networks.	Possibly – Sweden's transposition seems to tighten compliance timeframes and oversight, rather than add new types of measures. All NIS2 baseline measures (monitoring, etc.) will be mandatory, and the law's strict tone suggests minimal flexibility (in practice, entities should treat continuous monitoring and thorough logging as required).

Key Differences and Noteworthy Approaches

Despite NIS2's goal of harmonization, national implementations show meaningful differences in how they address security monitoring and network visibility:

- **Additional Internal Compliance Duties:** Some Member States require entities to formally assess and document their cybersecurity posture on an ongoing basis. For example, Romania and Latvia mandate annual self-assessment reports of cybersecurity readiness, going beyond the NIS2 Directive's general risk management framework (COBALT, DNCS Romania). In addition, Latvia and Belgium require the appointment of designated cybersecurity officers or managers, another step not explicitly mandated by NIS2 but aligned with its governance principles. These national obligations reinforce the importance of regular internal oversight and may indirectly drive greater investment in continuous monitoring and visibility, as organizations must evaluate and report on their cyber maturity more systematically.

- **Mandatory Audits and Certifications:** Hungary took a pioneering route by requiring bi-annual external audits by certified experts. Likewise, the Hungarian law enforces a formal classification and a catalogue of threats to be addressed, essentially prescribing in detail what to monitor and protect against. This approach is significantly stricter than NIS2's general "take appropriate measures" language, and it hardcodes continuous improvement (auditors must even alert the regulator if they discover serious threats mid-audit. These audits are obligatory for all covered entities in Hungary (both high-risk and normal sectors). No other country has yet made third-party audits a blanket requirement – most others allow some form of self-assessment or are silent on audit frequency.

- **Technical Standards and Catalogues:** Austria and Czechia both reference detailed technical guidance as part of their transposition. Austria's draft mentions a "Risk Management Catalogue", implying that the authority will publish a compendium of security controls (potentially including logging, IDS, etc.) that entities must follow. Czechia has gone even further – issuing decrees with comprehensive lists of security measures for different tiers of entities. For instance, Czech regulations explicitly require an ISMS, extensive supply chain risk rules, and specific availability targets for critical services. This level of specificity effectively translates NIS2's broad requirements into checklists; it exceeds NIS2 by leaving less room for interpretation. These measures are mandatory and enforceable by the respective authorities (e.g., NÚKIB in Czechia).

- **Security Monitoring and SOC Requirements:** While no country's law outright forces companies to set up a SOC or use a SIEM by name, some implicitly require 24/7 monitoring. Poland's existing regime (even pre-NIS2) and its draft push the envelope here – by planning to ban untrusted vendors and heavily regulating ICT supply chains, Poland is indirectly compelling organizations to gain deep visibility into their networks and equipment (you can't exclude "high-risk" tech if you don't know what's in your network). We can expect Poland to also enforce robust logging and perhaps require critical operators to integrate with national monitoring systems. Spain's anticipated law will likewise likely reference the National Security Framework, which already calls for continuous surveillance and anomaly detection in government systems; if extended to the private sector, Spain would be embedding continuous monitoring as a de facto obligation. Germany, in the absence of a law, uses BSI guidance: for example, BSI's KRITIS guidelines demand real-time log correlation and alerting – essentially a SOC function. Once Germany's law is passed, these "state-of-the-art" expectations may become binding through technical standards empowered by the law. In summary, many states leverage soft law or standards to insist on SOC-like capabilities without explicitly writing "SOC" in legislation.

- **Logging and Network Visibility:** All transposition laws require incident logging to some extent, as this is part of "incident handling" in NIS2. Croatia stands out for explicitly writing "monitoring and recording (logging) of incidents" into law. This clear phrasing, absent in the EU directive text, ensures no ambiguity that organizations must have systems to detect incidents, record event data, and report them. Other countries rely on the general phrasing of NIS2, but then enforce logging via secondary rules. For example, France and Italy are likely to rely on existing national standards (France's SecNumCloud, Italy's framework for critical infrastructure, etc.), which include extensive log retention and analysis requirements. Lithuania and Slovakia essentially copy NIS2's

language, which means logging is required as part of risk management (implicitly), but not elaborated. We see a split: some nations explicitly spell out logging/monitoring in legal text, others assume it under general clauses, and plan to issue guidance.

- **Entity Categorization and Scope:** A few countries diverged from NIS2's two-category model. Germany and Portugal propose a three-tier system, and Czechia added a special label for "strategically important" services on top of essential/important. These additional tiers often come with graduated obligations – e.g., lighter measures for the lower tier or extra measures for the top tier. For monitoring, this means the most critical entities might be required to do more (e.g., Czechia's "strategic" entities must meet higher availability criteria, implying more robust network monitoring to preempt downtime). Conversely, some countries chose not to differentiate between Essential and Important at all for security measures: Finland explicitly makes the same measures apply to both, only supervision differs. This is a strict approach for Important Entities, who under NIS2 could arguably have a lighter touch – in Finland (and similarly Latvia and Hungary), even smaller in-scope entities must implement full controls (continuous monitoring, etc.) rather than it being just recommended. This increases the compliance burden but raises the overall security baseline.

- **Innovative Supply Chain and Vendor Controls:** Poland's plan to use the 5G Toolbox mechanism across sectors is particularly innovative. It effectively extends network visibility requirements into the supply chain – companies will need to know and possibly report what hardware/software they use and ensure none is from banned vendors. This is beyond NIS2, which only generally addressed supply-chain risk analysis. Similarly, Romania and Hungary force contractual clauses on suppliers: Hungary's Act obliges entities to have their IT service providers commit to the Hungarian cyber law's requirements. Such clauses mean an organization must have visibility not just into its network, but also ensure its outsourcers are performing monitoring and protection (since any incident on outsourced systems still implicates the entity). These measures are strict but aim to plug visibility gaps in complex ICT ecosystems.

- **Management Accountability and Training:** Many transpositions underscore NIS2's theme that cybersecurity is a board-level issue. Romania and Latvia go as far as requiring management training and certification in cybersecurity. Sweden's draft and Germany's discussions highlight director liability for non-compliance. While not directly about technical monitoring, this focus ensures that corporate leadership must actively support continuous monitoring and visibility improvements (or face penalties). It shifts the culture to make ongoing cyber monitoring a governance priority, which in turn likely leads to more investment in SOCs, logging systems, and asset management.

In conclusion, most Member States stick to NIS2's baseline of security monitoring and network visibility measures, making them mandatory for in-scope entities, but several countries have augmented these requirements with their twists. Nations like Hungary, Romania, Latvia, Czechia, Poland, and Belgium have particularly strict or specific provisions – whether it's regular audits, self-assessments, named officers, detailed control catalogues, or third-party vendor restrictions – all of which either directly or indirectly demand a higher level of monitoring and visibility than the original NIS2 text. On the other hand, a few states (e.g., Finland, Lithuania, Italy) have chosen a near verbatim transposition, adding little in terms of new obligations (focusing mainly on implementing the required measures and not expanding them).

Even if national regulations don't explicitly mention terms like "anomaly detection" or "SIEM," the intent of NIS2 across member states is unmistakable: organizations are expected to maintain continuous threat monitoring and comprehensive logging capabilities. The differences lie in how explicit or forceful the national laws are about these practices. Companies operating in the EU should therefore pay attention to the specific transposition in each relevant country: some will allow more flexibility in how to meet the NIS2 requirements, while others will impose concrete steps and shorter deadlines. Particularly innovative/strict approaches (like Poland's vendor bans or Hungary's audit scheme) could become models for other EU states if they prove effective, potentially influencing future EU-wide standards or guidance.

References Cited in Comparative NIS2 Analysis

1. La loi NIS2 | CCB Safeonweb – https://ccb.belgium.be/fr/la-loi-nis2
2. NIS2 Compliance: Interpreting 'State-of-the-Art' for Organisations – https://www.openkritis.de/en/insights/nis2-compliance-interpreting-state-of-the-art-for-organisations/
3. NIS2 Croatia | Članak 30.1.b (logs) – https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_240.html
4. NIS2 Directive: The deadline for the registration of entities in Hungary is 30 June 2024 | DLA Piper – https://www.dlapiper.com/en-hu/insights/publications/2024/02/nis2-directive-the-deadline-for-the-registration-of-entities-in-hungary-is-30-june-2024
5. Hungary: Cybersecurity Laws – The Saga Continues – https://www.dlapiper.com/en-hu/insights/publications/2023/12/hungary-cybersecurity-laws-the-saga-continues
6. Transposition of the NIS2 Directive in Romania – https://dnsc.ro/citeste/ordin-de-transpunere-nis2
7. Summary of Latvia's New National Cyber Security Law | COBALT – https://www.cobalt.legal/publications/summary-of-latvias-new-national-cyber-security-law
8. NIS2 Implementation January 2025 – https://www.osborneclarke.com/insights/nis2-directive-transposition-eu-member-states-where-are-we-now
9. EU NIS2 in the Czech Republic – OpenKRITIS – https://www.openkritis.de/en/insights/nis2-in-the-czech-republic/
10. NIS2 Directive Transposition Tracker – ECSO – https://ecs-org.eu/newsroom/nis2-transposition-tracker
11. What Does the Lithuanian Cybersecurity Act Require? – Advisera – https://advisera.com/27001academy/blog/2024/04/15/lithuania-cybersecurity-act-nis2/
12. Key Implications of the EU's NIS 2 Directive Insights – Skadden – https://www.skadden.com/insights/publications/2024/02/key-implications-of-the-eu-nis-2-directive
13. Lithuania – NIS2 Implementation in the EU – Lex Mundi – https://www.lexmundi.com/lexsearch/nis2-directive-lithuania/
14. ECSO, ENISA, and other legal commentary sources – https://www.enisa.europa.eu/publications/nis2-directive