instituDE

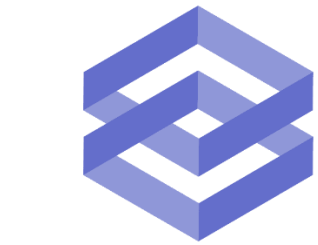
NAVIGATING SUPPLY-CHAIN SECURITY: NIS2 AND BEYOND

instituDE Report

March 2026

Dr. Yasir Gökce Thomas Krüger Stefan Hartmann

instituDE REPORTS



instituDE

First Published in 2026 by instituDE
Version 1.0
ISBN: 978-625-00-2301-4

Recommended citation: Gökce, Y., Krüger, T., & Hartmann, S. (March 2026). *Navigating Supply Chain Security: NIS2 and Beyond*. Brussels: instituDE.

instituDE | INSTITUTE FOR DIPLOMACY AND ECONOMY
Schuman Roundabout 2-4, Level 6, 1040 Brussels
www.instituDE.org | info@institude.org | @institude_org

Table of Contents

PREAMBLE

Modern digital infrastructures are increasingly dependent on complex and highly interconnected supply chains. Organizations rely on numerous external providers for software components, cloud infrastructure, IT services, and operational technologies. While these dependencies enable efficiency and innovation, they also significantly expand the cybersecurity risk landscape. A vulnerability, misconfiguration, or compromise at any point in the supply chain can propagate across multiple organizations, potentially affecting critical services and sensitive data far beyond the initially compromised entity.

Supply chain attacks have therefore become a prominent threat vector in recent years. Instead of directly targeting well-protected organizations, attackers frequently exploit weaker links such as software dependencies, service providers, or third-party vendors. Incidents involving compromised software packages, breached IT providers, or poorly managed vendor relationships illustrate how attackers can leverage trusted relationships to gain unauthorized access and scale the impact of cyberattacks.

In response to these systemic risks, the European Union introduced the NIS2 Directive, which significantly strengthens cybersecurity obligations for operators of essential and important services. The directive places particular emphasis on cybersecurity risk management and explicitly requires organizations to address risks arising from supply chain dependencies. By integrating supply chain security into a multilayered governance framework that includes Union-level coordination, national supervision, and entity-level risk management, NIS2 aims to improve the overall resilience of critical sectors.

This report provides a structured analysis of supply chain security within the context of the NIS2 framework and related international standards. It examines the legal and normative foundations of supply chain security, compares national implementation approaches across EU Member States, and highlights key patterns and differences in regulatory practice. By analyzing selected real-world cyber incidents, the report also illustrates how supply chain vulnerabilities manifest in practice and how supply chain security measures under NIS2 could influence their course and impact. Through this comprehensive examination, the report aims to contribute to a deeper understanding of supply chain cybersecurity risks and governance in the European regulatory landscape. I warmly invite you to explore the following pages and engage with the insights and analyses presented in this report.

Johannes Schmidt
Chief Information Security Officer (CISO)
DB InfraGO AG

EXECUTIVE SUMMARY

- Supply chain security is a central pillar of modern cybersecurity and operational resilience. Increasing reliance on cloud providers, software components, managed services, and complex ICT ecosystems has expanded organisational dependencies beyond traditional boundaries. As recent incidents demonstrate, cyberattacks targeting trusted third parties can propagate rapidly across sectors, affecting critical infrastructure, sensitive data, and public trust.
- The NIS2 (Network and Information Security 2) Directive embeds supply chain security within a comprehensive, all-hazards risk management framework. It establishes a three-tier governance model based on EU-level coordinated risk assessments, national risk assessments, and entity-level obligations.
- The comparative analysis of national NIS2 transpositions reveals substantial heterogeneity across Member States. There is strong convergence on foundational measures such as supplier risk assessments, incident and vulnerability reporting, supplier inventories, and contractual security clauses. However, advanced lifecycle and assurance requirements—including end-of-service management, structured supplier lifecycle governance, mandatory acceptance testing, audit rights, and long-term resilience controls—are unevenly addressed. Many national frameworks prioritise risk identification over sustained, enforceable risk control.
- The report concludes that effective supply chain cybersecurity requires alignment across three complementary dimensions: product-centric, supplier lifecycle-centric, and organisation-centric controls. Fragmentation between Member States and overlaps between EU instruments increase compliance complexity and reduce legal certainty. Clearer operational guidance, stronger lifecycle governance, enhanced transparency of third-party dependencies, and better alignment between regulatory frameworks are necessary to strengthen resilience across the Single Market.
- At EU level, stronger harmonisation, clearer operational guidance under the NIS2 Directive, closer alignment with the Cyber Resilience Act, and mechanisms addressing dominant suppliers would enhance effectiveness. At Member State level, consistent operationalisation and alignment across NIS2, Cyber Resilience Act (CRA), General Data Protection Regulation (GDPR) and Digital Operational Resilience Act (DORA) are key. At entity level, organisations should implement structured controls, ensure transparency of third-party dependencies, conduct robust risk assessments, and manage suppliers across their full lifecycle.
- Supply chain security is no longer a peripheral compliance issue. It is a strategic resilience imperative for critical services, digital markets, and public trust in the EU. A coordinated, risk-based, and lifecycle-oriented approach across institutions, Member States, and entities is essential to achieve robust, end-to-end cybersecurity across Europe's interconnected digital ecosystem.

1. INTRODUCTION

Supply chain security has emerged as a critical component of broader cybersecurity and operational resilience. In today's interconnected digital ecosystem, organisations depend on a complex network of suppliers, service providers, and embedded components, making the integrity of the entire supply chain essential for maintaining secure and reliable operations. Cyber threats, operational disruptions, and vulnerabilities can propagate across upstream and downstream partners, meaning that a weakness in one supplier or component can have significant cascading effects. Effective supply chain security is therefore not a standalone concern but an integral part of an organisation's overall risk management strategy, combining technical, operational, and organisational measures.

The European Union has addressed these challenges through the NIS2 Directive, which establishes an "all-hazards" approach to cybersecurity.[1] NIS2 integrates supply chain security into entity-level risk management while linking national and EU-level coordinated risk assessments. Essential and important entities are required to implement proportionate cybersecurity measures, assess supplier vulnerabilities, and maintain transparency regarding third-party products and services.[2] Complementary frameworks, such as CRA, DORA, and GDPR, extend responsibilities across product lifecycles, financial ICT services, and data processing chains. Together with international ISO standards, these instruments create a layered and multidimensional approach, encompassing product-centric, supplier lifecycle-centric, and organisation-centric security.

Despite this comprehensive framework, implementation across Member States varies significantly. While baseline risk assessments, supplier inventories, and incident reporting channels are largely harmonised, advanced lifecycle controls, resilience measures, and upstream supply chain oversight remain inconsistent. National innovations in several countries demonstrate that higher levels of supply-chain security are achievable, yet gaps persist, highlighting the need for clearer guidance, alignment between regulations, and more structured operationalisation of requirements at EU, national, and entity levels.

This report provides a structured analysis of supply chain security under NIS2 and related frameworks. Section 2 outlines the legal and normative landscape, including EU-level, national-level, and entity-level risk assessment obligations, and examines how NIS2 interacts with CRA, GDPR, DORA, and relevant ISO standards. Section 3 presents a comparative analysis of national transpositions, identifying coverage patterns, regulatory gaps, and innovative implementation practices across Member States. Section 4 analyses selected cyber incidents to illustrate how supply-chain security regulation influences real-world resilience outcomes. Section 5 develops policy implications and

[1] Article 21, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Document 02022L2555-20221227

[2] Article 20 & 21, NIS 2 Directive

recommendations at the EU, Member State, and entity levels, offering actionable guidance to enhance consistency, operational effectiveness, and risk-informed supply chain resilience. Finally, Section 6 concludes the report by summarising the key findings and consolidating the main recommendations.

2. LEGAL AND NORMATIVE FRAMEWORK

2.1 Core NIS2 Supply Chain Security Provisions within Multilayered Risk Governance

The NIS2 Directive embeds supply chain security within a broader, holistic framework of risk management. Rather than addressing supplier-related risks in isolation, the Directive positions them within a comprehensive "all-hazards" approach to cybersecurity and operational resilience. This approach requires the consideration of both technical and non-technical threats, including systemic dependencies, physical vulnerabilities, geopolitical influences, and potential disruptions throughout the entire lifecycle of ICT systems, services and products.[3] As a result, supply chain security is not treated as a standalone obligation but as an integrated and continuous component of overall risk assessment and mitigation across the Union.

NIS2 structures supply chain security within a multilayered risk-assessment framework conducted at three levels: EU-level coordinated risk assessments, national-level risk assessments carried out by Member States, and entity-level risk assessments performed by essential and important entities.[4] Together, these three levels create a coherent governance structure in which EU-wide strategic insights inform national priorities, while entity-level assessments operationalize those priorities within individual organisations.

2.1.1 UNION LEVEL COORDINATED RISK ASSESSMENTS

The coordinated Union-level risk assessment is defined in Article 22 as a process through which the Cooperation Group, together with the Commission and ENISA, evaluates the security of specific critical ICT services, systems or products. Its purpose is to identify sector-relevant threats, vulnerabilities, systemic dependencies and potential single points of failure across the Union, thereby supporting essential and important entities in managing their supply chain risks.

> **Article 22**
> **Union level coordinated security risk assessments of critical supply chains**
> 1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.

[3] Ruohonen, Jukka. "A systematic literature review on the NIS2 Directive." *arXiv preprint arXiv:2412.08084* (2024).

[4] Katko, Peter, and Joanna Ostrowska (Gałajda). *"How Will NIS2 Affect the Supply Chain Security Approach?" EY*, 6 June 2023

> 2. The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1.

These assessments are carried out to address cross-border and structural risks that no Member State can fully assess alone. Drawing on the model developed for the EU-wide 5G cybersecurity risk assessment, they aim to avoid fragmented national approaches and promote a harmonised understanding of common dependencies and emerging risks.[5]

The actors involved include the Cooperation Group, which coordinates the process, the Commission, which ensures its policy coherence and determines the ICT components to be assessed, and ENISA, which provides technical expertise. Where relevant, industry stakeholders and technical experts may also be consulted to ensure that the assessment reflects real-world operational and market conditions.

The scope of each assessment is defined by the Commission and may include any critical ICT service, system or product. Both technical and non-technical risks are examined, including structural market dependencies, governance models of suppliers, and potential undue influence from third countries or systemic disruptions caused by technological lock-in.

Preamble 91 specifies the criteria used to select supply chains for coordinated assessment: the degree of reliance by essential and important entities, the criticality of supported functions, the availability of alternatives, lifecycle resilience, and the potential future importance of emerging technologies. Based on this analysis, the assessments produce recommendations, mitigation measures and best practices to strengthen supply chain resilience across the EU.[6]

> **[*Preamble*] (91)** The coordinated security risk assessments of critical supply chains, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU coordinated risk assessment of the cybersecurity of 5G networks and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group.
> To identify the supply chains that should be subject to a coordinated security risk assessment, the following criteria should be taken into account:
> **(i)** the extent to which essential and important entities use and rely on specific critical ICT services, ICT systems or ICT products;

[5] Radu, Roxana, and Cedric Amon. "The governance of 5G infrastructure: between path dependency and risk-based approaches." *Journal of Cybersecurity* 7.1 (2021): tyab017.
[6] Ferguson, Donald David Stewart. "The outcome efficacy of the entity risk management requirements of the NIS 2 Directive." *International Cybersecurity Law Review* 4.4 (2023): 371-386.

(ii) the relevance of specific critical ICT services, ICT systems or ICT products for performing critical or sensitive functions, including the processing of personal data;
(iii) the availability of alternative ICT services, ICT systems or ICT products;
(iv) the resilience of the overall supply chain of ICT services, ICT systems or ICT products throughout their lifecycle against disruptive events; and
(v) for emerging ICT services, ICT systems or ICT products, their potential future significance for the entities' activities.
Furthermore, particular emphasis should be placed on ICT services, ICT systems or ICT products that are subject to specific requirements stemming from third countries.

2.1.2 NATIONAL-LEVEL RISK ASSESSMENTS

Member States are responsible for conducting national cybersecurity risk assessments that reflect the specific threat landscape, sectoral dependencies, and national critical infrastructure within their territory. These assessments inform national cybersecurity strategies and guide national authorities in implementing supervisory measures, incident handling procedures and sector-specific security requirements. They also serve as a bridge between EU-level assessments and the operational measures required from entities at domestic level.

The method of a national risk assessment involves assessing the potential impact of service disruption on public safety, public security, public health, the economy and the resilience of interdependent sectors, drawing on the criteria set out in Article 2(2). The scope of this assessment includes identifying entities that are sole providers of essential services; entities whose disruption could cause significant societal or economic harm; entities whose failure could generate systemic or cross-border risks; and entities whose functions are of specific national or regional importance. Through this structured evaluation, Member States determine which operators are critical within the national context and ensure that corresponding supervisory and security requirements are appropriately applied.[7]

Article 2
Scope
...2. Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where: ...
(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;
(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

[7] Aude Steen, Fabian, and Daniel Assani Shabani. "A NIS2 pan-European registry for identifying and classifying essential and important entities." *arXiv e-prints* (2025): arXiv-2508.

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State ...

2.1.3 ENTITY-LEVEL RISK ASSESSMENTS

An entity-level or internal risk assessment under NIS2 is an internal, organisation-specific evaluation conducted by each essential and important entity to identify and manage risks affecting its network and information systems, including those arising from its physical environment and supply chain. Carried out by the entity itself as part of its mandatory cybersecurity risk-management measures under Article 21, it follows an all-hazards approach and must incorporate policies on risk analysis, information system security and supplier-related security considerations.[8]

Article 21
Cybersecurity risk-management measures
... 2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:
(a) policies on risk analysis and information system security...
(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers...
3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

In determining appropriate measures, entities must assess vulnerabilities specific to each direct supplier or service provider, the overall quality and cybersecurity practices of the products and services they rely on, and the secure development processes of their providers.[9] They are also required to take into account the outcomes of EU-level

[8] Ruohonen, *A Systematic Literature Review on the NIS2 Directive*.
[9] *Ibid*

coordinated supply chain risk assessments.[10] Through this structured evaluation, entities ensure that their internal controls, procurement choices and contractual arrangements adequately address both technical and non-technical risks within their operational and supply ecosystems, consistent with the emphasis in Preamble 85 on assessing the quality, resilience and cybersecurity practices embedded in third-party products and services.

> **[*Preamble*] (85)** Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

2.1.4 ENTITIES RESPONSIBLE FOR INTERNAL RISK ASSESSMENTS

Essential and important entities, as defined in Article 3 of NIS2, are organisations operating in sectors critical to societal and economic stability—such as energy, transport, health, drinking water, digital infrastructure, ICT service management, public administration, manufacturing of key products, and certain digital services. Essential entities represent operators whose disruption would have the most significant impact, while important entities cover those whose services are also critical but with comparatively lower systemic impact.[11]

The scope of suppliers that essential and important entities are required to consider for supply chain security under NIS2 is relatively narrow, focusing primarily on direct suppliers and service providers, as specified in Section 5.1.1 of the Annex to the Commission Implementing Regulation laying down rules for the application of Directive

[10] Article 21(3), NIS 2 Directive

[11] European Union Agency for Cybersecurity (ENISA). *Technical Implementation Guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 Laying Down Rules for the Application of the NIS2 Directive as Regards Technical and Methodological Requirements of Cybersecurity Risk-Management Measures*. Version 1.0, June 2025, European Union,

(EU) 2022/2555.[12] Consequently, entity-level risk assessments are expected to address risks arising from these immediate relationships. However, the Directive appears to overlook further upstream or downstream actors, whose activities can nonetheless have a significant impact on the overall supply chain security of essential and important entities.[13]

> **5.1.1.** For the purpose of Article 21(2), point (d) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the relevant entities shall identify their role in the supply chain and communicate it to their direct suppliers and service providers.

Similarly, being classified as an essential or important entity does not necessarily imply that the organisation holds the most influence or leverage within its supply chain. In some cases, a supplier's dominant position or an entity's high dependency on that supplier may shift the balance of power, limiting the ability of essential or important entities to enforce supply chain security measures effectively.[14] In other words, relying solely on an organisation's ability to impose security measures on its suppliers may weaken overall supply chain security. One potential approach NIS2 could have adopted to address this limitation would be to classify suppliers as essential or important entities by virtue of their proximity to critical operators, thereby strengthening the incentive and authority to manage supply chain risks effectively. Complementing this approach with mechanisms that extend security requirements downstream to an entity's customers would engage multiple actors across the supply chain and strengthen overall supply chain security.

2.1.5 CYBERSECURITY RISK-MANAGEMENT MEASURES

Under Article 21 of NIS2, essential and important entities are required to implement appropriate and proportionate technical, operational, and organisational measures to manage risks to the security of their network and information systems, including those arising from their supply chains. The Directive identifies key domains of action, which include risk analysis policies, incident handling, business continuity and crisis

---

[12] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers, C/2024/7151.

[13] Czulak, Piotr, et al. *"NIS2 Directive Explained: Part 3 – Supply Chain Security." JD Supra*, 12 Dec. 2025

[14] van 't Schip, M. *The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things*. *European Journal of Law and Technology*, vol. 15, no. 1, 2024

management, secure acquisition, development and maintenance of ICT systems, and supply chain security measures addressing direct suppliers and service providers (Article 21(2)). Entities must assess supplier vulnerabilities, evaluate the quality and security practices of their suppliers—including secure development procedures—and integrate findings from coordinated EU-level risk assessments of critical supply chains (Article 21(3) and Article 22).[15]

Operationally, entities are expected to formalise supply chain security requirements in contracts with suppliers and service providers,[16] covering cybersecurity obligations, employee awareness and training, incident reporting, vulnerability handling, subcontracting rules, audit rights, and obligations at contract termination. Entities must also maintain an up-to-date registry of direct suppliers and service providers including the ICT products and services provided,[17] and periodically monitor, evaluate, and update security practices in response to changes in operations, risks, or significant incidents.[18]

From a technical perspective, NIS2 requires that entities implement secure development life cycle processes for in-house and outsourced network and information systems.[19] These processes must cover all phases of development, including specification, design, coding, implementation, testing, and validation. Entities are expected to apply secure coding principles, cybersecurity-by-design approaches, zero-trust architectures, and appropriate management of test data, including sanitisation and anonymisation.

Acquisition of ICT services and products is another critical technical measure.[20] Entities must set and enforce security requirements throughout the lifecycle of ICT products and services, including documentation of hardware and software components, cybersecurity functions, secure configurations, validation of compliance, and ongoing updates or replacements. Regular review of acquisition and development processes ensures that technical, operational, and organisational measures remain effective and proportionate to evolving risks.

Collectively, these technical, operational, and organisational measures provide a structured framework for managing supply chain risks, ensuring that essential and important entities influence the security behavior of their suppliers and maintain secure supplier relationships.

[15] ENISA, *Technical Implementation Guidance on Commission Implementing Regulation*
[16] Annex - Article 5.1.4, Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555
[17] *Ibid,* § 5.2
[18] *Ibid,* § 5.1.6
[19] *Ibid,* § 6.2
[20] *Ibid,* § 6.1

2.2 Relationship with other EU legislation

This section examines how the NIS2 Directive interacts with other EU regulatory frameworks to address supply chain security across different contexts. It compares NIS2 with the Cyber Resilience Act (CRA), highlighting product-level obligations for manufacturers, importers, and distributors; with the General Data Protection Regulation (GDPR), focusing on responsibilities of data controllers and processors across the processing chain; and with the Digital Operational Resilience Act (DORA), which establishes direct obligations for critical ICT third-party service providers in the financial sector. Together, these comparisons illustrate how supply chain security is regulated at the product, data, and operational levels, identifying complementarities and gaps relative to the entity-focused approach of NIS2.

2.2.1. Cyber Resilience Act and NIS2 Directive

The Cyber Resilience Act (CRA, EU 2024/2847) regulates cybersecurity across the entire lifecycle of products with digital elements by assigning obligations to clearly defined actors within the supply chain. It conceptualises this chain as a sequence beginning with upstream suppliers and extending through manufacturers, importers, and distributors before reaching the end consumer. Manufacturers bear the primary responsibility for ensuring secure-by-design development, lifecycle vulnerability management, and overall product conformity. [21] Importers and distributors serve as verification and due-care actors who must ensure that only compliant, CE-marked products enter and circulate in the EU market.[22] Suppliers, though not directly regulated by the CRA, are indirectly bound by the manufacturer's obligation to ensure that all integrated components and software meet security requirements.[23] Consumers themselves have no compliance obligations but benefit from receiving secure products and long-term security support.

Suppliers
│ (components, software modules)
▼
Manufacturer
│ (secure-by-design, conformity assessment, CE marking)
▼
Importer
│ (verify compliance before placing on EU market)
▼
Distributor
│ (due care, ensure compliant products reach consumers)
▼
Consumer

[21] Articles 7–9, Annex I & Articles 6.1–6.2, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), PE/100/2023/REV/1.
[22] Articles 17–20, Cyber Resilience Act.
[23] Articles 7–8, Annex I, Cyber Resilience Act.

(receives secure products; no obligations)

Under the Cyber Resilience Act, products with digital elements are grouped into three risk-based categories: baseline products, important products, and critical products.[24] This categorisation primarily reflects the cybersecurity function and systemic impact of a product—particularly the harm that could result if it were compromised.[25] While supply chain security is not the direct basis for assigning a product to a higher category, it plays an important underlying role. Products that serve as foundational components across many systems, or whose compromise could propagate vulnerabilities widely through downstream supply chains, are more likely to be designated as important or critical.[26]

The NIS2 Directive and the CRA address supply chain security from complementary perspectives across the digital ecosystem.[27] The CRA focuses on products with digital elements—software, hardware, and firmware—placing obligations on manufacturers, importers, and distributors. It does not regulate end users or operators of critical services directly, beyond ensuring they receive secure products, nor does it explicitly impose formal contractual obligations or verification with suppliers beyond product security.[28] NIS2, by contrast, targets essential and important entities, requiring risk management, supply chain assessment, incident reporting, and organisational measures, including contractual obligations with direct suppliers.[29] However, unlike the CRA, NIS2 does not regulate upstream manufacturers or the development of the digital products themselves. Together, the two frameworks create a complementary system that covers both product-level and entity-level supply chain security, though certain gaps remain in bridging upstream and downstream responsibilities.

2.2.2. GDPR AND NIS2 DIRECTIVE

The General Data Protection Regulation (GDPR, EU 2016/679) addresses supply chain security primarily through the relationship between data controllers and processors. Data controllers retain ultimate responsibility for ensuring that personal data is processed securely, even when handled by third parties, and must conduct due diligence on processors to verify that they implement appropriate technical and organizational measures.[30] Controllers are also required to formalize these obligations through written

[24] Annex III and Annex IV, Cyber Resilience Act.
[25] Articles 7 and 8, Cyber Resilience Act.
[26] Articles 8, Cyber Resilience Act.
[27] *"Cyber Resilience Act." Shaping Europe's Digital Future*, European Commission, 3 Dec. 2025,
[28] *Ibid*
[29] Article 21, NIS 2 Directive; Art. 5.1.4–5.1.6 of Annex to Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555
[30] Articles 24, 28(1), Recital 81, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016*.

contracts specifying the scope of processing, security requirements, and responsibilities toward data subjects.[31]

Data processors, in turn, must process personal data only under the controller's instructions and implement appropriate security measures.[32] They may only engage sub-processors with the controller's prior authorization, ensuring that contractual and security obligations flow downstream.[33] Processors are also required to notify controllers without undue delay in the event of a personal data breach.[34]

Unlike NIS2, which primarily considers direct suppliers when imposing supply chain security obligations, GDPR explicitly acknowledges sub-processors along the processing chain, extending accountability beyond the immediate service provider. This allows data controllers to enforce security measures further downstream. However, a limitation of GDPR is that it only applies when personal data is being processed. Supply chain components that do not handle personal data fall outside its scope, leaving potential security risks unaddressed.[35]

2.2.3. DORA AND NIS2 DIRECTIVE

The Digital Operational Resilience Act (DORA, EU 2022/2554) establishes a comprehensive framework to strengthen the operational resilience of financial entities across the European Union.[36] Its scope covers a wide range of financial institutions, including banks, insurers, investment firms, and payment service providers,[37] and extends to the ICT third-party service providers upon which these entities rely.[38] DORA aims to ensure that financial services remain secure, stable, and resilient in the face of ICT disruptions, cyberattacks, or other operational incidents.[39]

Financial entities under DORA are responsible for managing ICT risks throughout their supply chain, which includes conducting due diligence on suppliers, establishing contractual security obligations, and monitoring provider performance. Unlike NIS2, which envisions an all-hazards approach at the entity level, financial entities under DORA must perform a preliminary assessment of ICT concentration risk before engaging ICT providers, identifying potential single points of failure and dependencies that could

[31] *Ibid*, Article 28(3)
[32] *Ibid*, Articles 28(3), 32
[33] *Ibid,* Articles 28(2)–(4)
[34] *Ibid,* Article 33
[35] Dasgupta, Avirup, Asif Qumer Gill, and Farookh Hussain. "A review of general data protection regulation for supply chain ecosystem." *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. Cham: Springer International Publishing, 2019.
[36] Articles 1–3 & 5, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act), PE/41/2022/INIT
[37] Articles 2–3, Digital Operational Resilience Act
[38] *Ibid*, Articles 28–31
[39] *Ibid*, Articles 5, 6, 28

materially affect operations.[40] ICT providers identified as critical, based on criteria such as systemic importance, substitutability, and the number of financial entities relying on them, are subject to heightened regulatory oversight and additional obligations.[41]

As discussed under Section 3.1.4, NIS2 relies on essential or important entities to enforce supply chain security, but high dependency on dominant suppliers can limit their influence, weakening overall security. DORA addresses this gap by imposing direct obligations on critical ICT third-party service providers.[42] These providers are required to implement robust ICT risk management and security measures, ensure operational continuity, report incidents promptly to financial entities, facilitate audits and independent testing, and maintain transparency regarding subcontracting arrangements. To safeguard the financial supply chain, critical providers and financial entities must adopt a risk-based approach, including contractual obligations, continuous monitoring, vulnerability management, and contingency planning. Additionally, they must establish exit strategies and fallback arrangements to mitigate the consequences of provider failures, ensuring that critical services remain operational and resilient. By assigning responsibilities directly to critical providers, DORA strengthens incentives and authority to manage supply chain risks effectively, complementing the entity-focused approach of NIS2.

[40] *Ibid*, Article 29
[41] *Ibid*, Articles 28–29
[42] *Ibid*, Articles 28–31

2.3 Supply Chain Security stipulated in International ISO-Norms

This section examines supply chain security from both a regulatory and standards perspective. The first subsection presents a set of key supply-chain security requirements and maps them to relevant provisions in the NIS2 Directive and key ISO standards—namely ISO/IEC 27001, which defines requirements for an information security management system (ISMS);[43] ISO/IEC 27002, which provides guidelines and best-practice controls for information security;[44] ISO/IEC 27036-1, which offers guidance on managing information security in supplier relationships;[45] and ISO 28000:2022, which specifies requirements for security management systems within supply-chain environments. [46] The second subsection discusses how these frameworks address supply chain security across three complementary dimensions: product-centric, supplier lifecycle-centric, and organisation-centric.

2.3.1 Comparative Mapping of Supply Chain Security under NIS2 and ISO Standards

The European Union Agency for Cybersecurity (ENISA), which provides expert guidance and supports the development of EU-wide cybersecurity best practices, has published several reports on good practices for supply chain security. [47] Based on these publications, a set of outstanding supply-chain security requirements was identified. These requirements were then mapped against the principal regulatory and standardisation frameworks relevant to supply-chain cybersecurity—namely the NIS2 Directive, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27036-1 and ISO 28000:2022. The resulting table specifies the exact articles or clauses in which each requirement is regulated or covered, without assessing the depth or extent of that coverage.

[43] International Organization for Standardization, International Electrotechnical Commission. *ISO/IEC 27001:2022 — Information technology — Security techniques — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO, 2022

[44] International Organization for Standardization & International Electrotechnical Commission. *ISO/IEC 27002:2022 — Information technology — Security techniques — Code of practice for information security controls*. ISO/IEC, 2022

[45] International Organization for Standardization & International Electrotechnical Commission. *ISO/IEC 27036-1:2014 — Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*. ISO/IEC, 2014.

[46] International Organization for Standardization. *ISO 28000:2022 — Security and resilience — Security management systems for the supply chain — Requirements*. ISO, 2022.

[47] ENISA, Raising Awareness (Campaigns), Network and Information Systems Directive 2 (NIS2); Papaphilippou, Maria, Konstantinos Moulinos, and Marianthi Theocharidou. *Good Practices for Supply Chain Cybersecurity*. European Union Agency for Cybersecurity (ENISA), June 2023

	Supply Chain Security Requirements	NIS2 Directive	ISO/IEC 27001 / ISO/IEC 27002	ISO/IEC 27036-1	ISO 28000:2022
1	**Dedicated supply-chain security policy**	Art 5.1 of Annex[48]	A.5.19	Clause 5	-
2	**Defined responsibilities and authorities for supply-chain security**	Article 21, Art. 1.2 of Annex	A.5.19	Clause 5	Clause 5.3
3	**Inventory of third-party entities and third-party products**	Art. 5.2, Art. 6.1.2(c), and Art 12.4.2 of Annex	A.5.19 (a); A.5.21(d)	Clause 6	Clause 8.1 / 8.2
4	**Supply-chain risk assessment process**	Article 21, Art. 2 of Annex	A.5.19	Clause 7	Clause 6.1 / 6.2 & Clause 8
5	**Supplier lifecycle management process**	Art. 6.1.2 of Annex	A.5.19	Clause 6	-
6	**Supplier selection and qualification procedures**	Art. 5.1.5 and 5.1.6 of Annex	A.5.21	Clause 6.2	-
7	**Information-security requirements integrated into supplier contracts**	Art. 5.1.4 of Annex	A.5.20	Clause 8	Clause 8.3
8	**Rules governing subcontracting and prevention of cascading risks**	Art. 5.1.4(g) of Annex	A.5.21(b), (c)	Clause 8	-
9	**Agreed service-continuity and service-level parameters (SLAs)**	Art. 5.1.4 of Annex	A.5.23	Clause 8	Clause 8.4 / 8.5
10	**Acceptance testing to verify product authenticity, compatibility, and security**	Art. 6.1.2 of Annex	A.5.21	Clause 9	-

[48] The same annex is referenced throughout the table to avoid repeating its full title "Annex to Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555"

11	**Security scanning and awareness for supplier personnel**	Art. 5.1.4(b) & (c), Art. 8 & 10 of Annex	A.5.19(k), (n)	Clause 10	Clause 7.2
12	**Communication channels for reporting security vulnerabilities and incidents**	Art. 5.1.4(d), Art. 4.3.2(a) and Art. 6.10.2 of Annex	A.5.19 (i)	Clause 10	Clause 8.13
13	**Change management for supplier relationships and third-party components**	Art. 5.1.7(d) of Annex	A.5.22(c)	Clause 10 & 11	Clause 8.6
14	**Supplier business-continuity requirements**	Art. 4.3 of Annex	A.5.19(j)	Clause 10	Clause 8.4 / 8.5
15	**Procedures for managing end-of-service and end-of-support situations**	Art. 6.1.2 of Annex	A.5.20(z), A.5.21(m)	Clause 6.3 & 11	-
16	**Processes for supplier monitoring, review, and audit**	Art. 5.1.6, Art. 5.1.7 of Annex	A.5.22	Clause 10 & 11	Clause 9.1–9.2

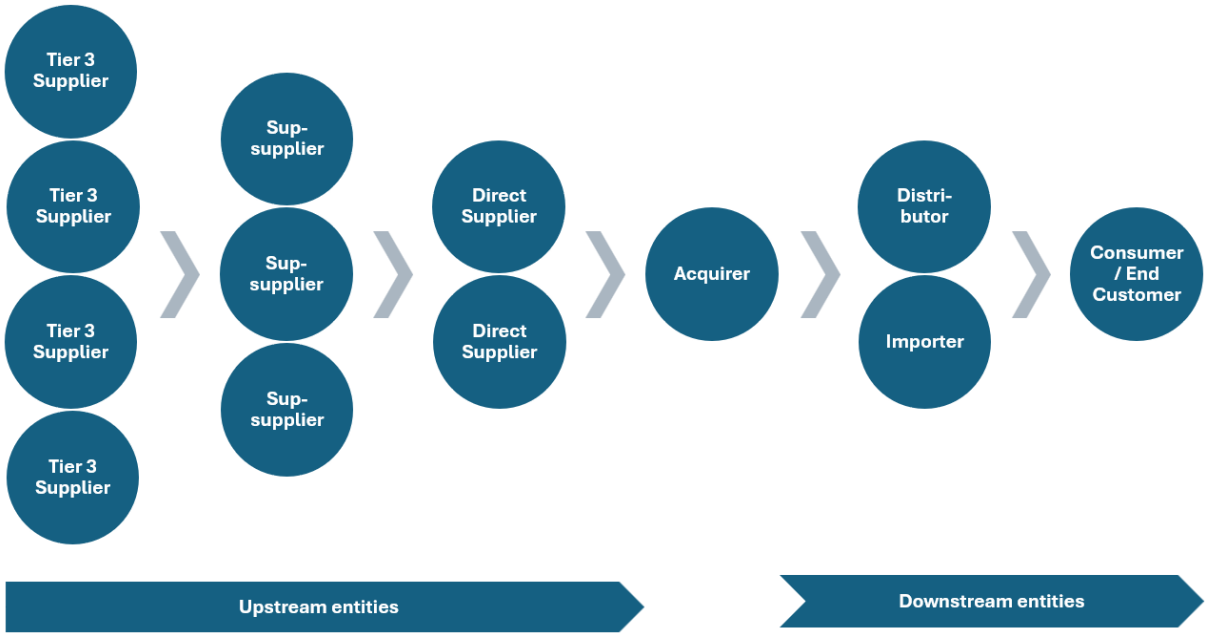
Comparative Mapping-Table of ENISA-derived Supply Chain Security under NIS2 and ISO-Standards

The ENISA-derived supply chain security requirements summarized in the table above will be used throughout the following sections as reference criteria. They serve to assess the extent to which individual EU member states have implemented and transposed the supply chain security obligations from the NIS2 Directive, allowing for an evaluation of whether these requirements have been fully, partially, or not yet addressed at the national level.

2.3.2 Three Dimensions of Supply Chain Security in leading ISO Standards

For the purposes of this analysis, supply chain security can be structured across three complementary dimensions:

- **Product-centric supply chain security** – focuses on securing a product or service throughout its entire supply chain, with the acquirer at the center, interacting with upstream suppliers and sub-suppliers as well as downstream entities such as importers, distributors, retailers, and end customers. According to ISO/IEC 27036-1:2021, an ICT supply chain is a set of organizations with linked resources and processes that form successive supplier relationships.[49] A product or service may be composed of components and services sourced from multiple suppliers, where each organization acts as an acquirer to its upstream supplier and a supplier to its downstream customer, with the end customer typically having limited influence over upstream security requirements. Consequently, information security risks can propagate throughout the supply chain, and effective product-centric security requires consideration of both upstream and downstream dependencies.[50]



Graphic: Product-centric supply chain structure

- **Supplier lifecycle-centric supply chain security** – focuses on managing individual suppliers throughout the supplier-relationship lifecycle. ISO/IEC 27036-1:2021 describes processes that effectively span the lifecycle of a supplier relationship, including: selection and evaluation, establishment of agreements and security requirements, operation and management (monitoring,

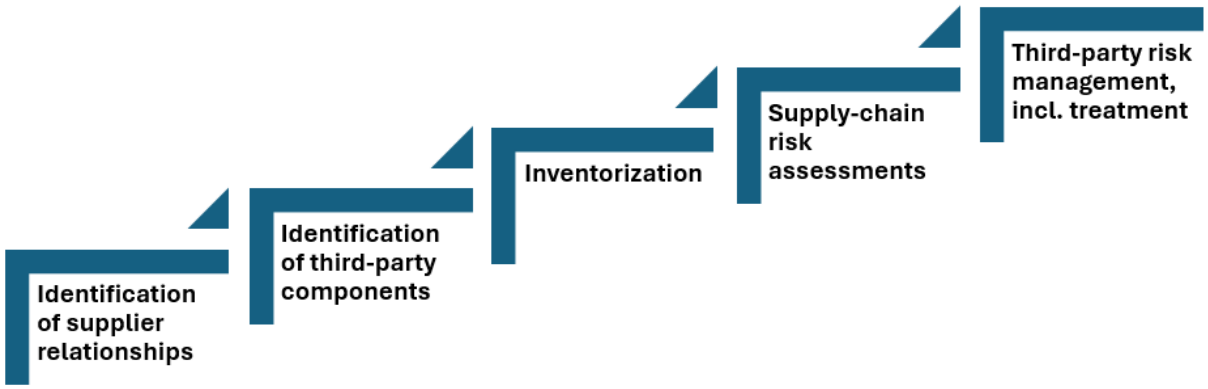
[49] Sec. 5.2.3, ISO/IEC 27036-1:2021

[50] Li, X., & Xu, Y. (2024). *Cybersecurity investments in supply chains with two-stage risk propagation*. *Computers & Industrial Engineering*, 110519

performance, incident handling), and termination. [51] ISO/IEC 27036-2:2022 provides detailed requirements and controls for managing these processes. This dimension ensures that risks associated with each supplier are identified, mitigated, and continuously managed.

Graphic: Supplier lifecycle -centric supply chain structure

- **Organization-centric supply chain security** – considers the organisation's responsibilities in managing risks arising from third-party involvement. This includes performing supply-chain risk assessments, maintaining inventories of supplier relationships and third-party components, and implementing structured third-party risk-management processes. ISO/IEC 27001 and ISO/IEC 27002 primarily support this dimension through requirements and controls for third-party risk management, supplier monitoring, and contractual security obligations.[52]



Graphic: Organization-centric supply chain structure

A comprehensive approach to supply chain security requires integrating all three dimensions. They complement each other: product-centric security addresses the propagation of risk through the supply chain, supplier lifecycle-centric security ensures rigorous governance of individual supplier relationships, and organization-centric security provides the internal processes and controls to oversee and manage the broader network of suppliers and components.

Under the three supply chain security dimensions, the NIS2 Directive and the Cyber Resilience Act (CRA) take complementary approaches. NIS2 primarily addresses the organization-centric dimension, requiring essential and important entities to implement risk management measures, including assessing and mitigating risks from third-party dependencies, maintaining supplier inventories, and enforcing security requirements in

[51] Part 1: Overview and concepts, ISO/IEC 27036-1:2021.
[52] A.5.19-A.5.23, ISO/IEC 27001 and ISO/IEC 27002.

procurement. It also partially covers the supplier lifecycle-centric dimension, obliging organisations to evaluate suppliers' cybersecurity practices and include relevant obligations in contracts. The CRA, by contrast, focuses on the product-centric dimension, imposing cybersecurity requirements on products with digital elements throughout their lifecycle, from design and development to maintenance and end-of-life, which in turn influences supplier practices and organizational risk management. Together, these regulatory frameworks provide a layered approach to securing the supply chain across products, suppliers, and organizational processes.

3. COMPARATIVE ANALYSIS OF NATIONAL SUPPLY-CHAIN SECURITY IMPLEMENTATION UNDER NIS2

This section examines how EU Member States have integrated supply-chain security requirements into their national transposition of the NIS2 Directive. It first analyses the extent to which core supply-chain controls—derived from ENISA guidance and relevant standards[53]—are reflected in national laws, before identifying broader patterns, gaps, and emerging innovations in implementation. Together, these subsections provide a structured view of the current regulatory landscape and the varying levels of maturity across Member States.

3.1 Coverage Analysis of Supply-Chain Security Requirements in National Transpositions

The good practices for supply chain security, as derived under Subsection 2.3 from ENISA best practice reports and a range of regulatory and standardization frameworks—including the NIS2 Directive, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27036-1, and ISO 28000:2022—were considered core supply chain security requirements. An evaluation was then conducted to determine the extent to which these requirements are reflected in national legislation transposing the NIS2 Directive. The results of this evaluation are presented in the coverage table below.

Coverage is determined through a structured review that maps each identified requirement to explicit provisions in respective national legislation implementing NIS2, capturing the relevant articles/sections as evidence. “Covered” means the requirement is fully and clearly addressed by binding legal obligations. “Not covered” means the requirement is absent or only mentioned tangentially without enforceable clauses. “Partially covered” means the law addresses some aspects of the requirement (e.g., high-level intent, limited scope, or implicit coverage) but lacks specificity, completeness, or enforceable detail for all elements. The analysis deliberately considers only primary national legislation; secondary instruments such as internal regulations, implementing by-laws, technical decrees, or other subordinate normative acts that may further operationalize these obligations were not taken into account.

Several national laws transposing the NIS2 Directive are not yet in force; some remain subject to parliamentary approval while others are in various internal ratification phases.[54] The coverage table is therefore a status-driven snapshot: it maps requirements against the most current draft or known status of each national instrument at the time of assessment, regardless of formal enactment or entry into force, and is intended to support gap analysis rather than to certify binding compliance. The national legislation taken into account as the basis for this assessment can also be found below.

[53] Section 2.3.1 of this report

[54] *See* Table of National NIS2-Laws

Last but not the least, the United Kingdom was included in the scope of this assessment, although it is no longer subject to the NIS2 Directive as a non-EU state, because it had previously transposed the original NIS Directive through the NIS Regulations 2018 and is currently in the process of revising its national cybersecurity framework through a new Cyber Security and Resilience legislative package in line with NIS2 requirements.[55]

[55] *Cyber Security and Resilience (Network and Information Systems) Bill*. UK Parliament, Bill 329, 59th Parliament, Session 2025–26

	Supply Chain Security Requirements / EU States	1 Dedicated supply-chain security policy	2 Defined responsibilities and authorities for supply-chain security	3 Inventory of third-party entities and third-party products	4 Supply-chain risk assessment process	5 Supplier lifecycle management process	6 Supplier selection and qualification procedures	7 Information-security requirements integrated into supplier contracts	8 Rules governing subcontracting and prevention of cascading risks	9 Agreed service-continuity and service-level parameters (SLAs)	10 Acceptance testing to verify product authenticity, compatibility, and security	11 Security scanning and awareness for supplier personnel	12 Communication channels for reporting security vulnerabilities and incidents	13 Change management for supplier relationships and third-party components	14 Supplier business-continuity requirements	15 Procedures for managing end-of-service and end-of-support situations	16 Processes for supplier monitoring, review, and audit
1	Austria	!	!	!	✓	✗	✗	✓	✗	✗	✗	!	✓	✗	✗	✗	!
2	Belgium	✓	!	✗	✓	✗	✗	!	!	!	✗	✗	✓	✗	!	✗	!
3	Bulgarian	!	!	✗	✓	✗	!	!	!	!	✗	!	!	!	!	✗	!
4	Croatia	!	!	✗	✓	✗	!	!	✗	!	✗	✗	✓	✗	!	✗	!
5	Cyprus	!	!	✗	✓	✗	!	✓	!	!	✗	✗	✓	✗	!	✗	✗
6	Czech Republic	!	!	✓	✓	!	!	✓	!	!	!	✓	✓	✓	!	✗	!
7	Denmark	!	!	✓	✓	!	!	✓	!	!	✗	✗	✓	✓	!	✗	!
8	Estonia	✓	!	✓	✓	!	✓	✓	!	✓	✗	!	✓	!	!	✗	✓
9	Finland	!	!	✗	!	✗	✗	✗	✗	!	✗	✗	!	✗	!	✗	!
10	France	✓	!	✓	✓	!	!	✓	!	✓	✗	!	✓	!	!	✗	!
11	Germany	!	!	!	✓	!	!	✓	!	!	!	!	!	!	!	!	✓
12	Greece	!	!	✗	✓	✗	!	!	✗	!	✗	!	✓	✗	!	✗	!
13	Hungary	✗	✗	✗	!	✗	✗	!	✗	✗	!	✗	✓	✗	✗	✗	✓
14	Ireland	!	!	✗	✓	✗	!	!	✗	!	✗	!	✓	!	!	✗	!
15	Italy	!	!	!	✓	✗	!	!	!	!	✗	!	✓	!	!	✗	!
16	Latvia	✗	!	✗	!	✗	✗	✗	✗	!	✗	✗	!	✗	!	✗	!
17	Lithuania	!	!	✗	!	✗	✗	✗	✗	!	✗	!	✓	✗	!	✗	!
18	Luxembourg	!	!	✗	✓	!	✗	!	!	!	✗	✓	✓	!	✓	✗	✓
19	Malta	!	✓	!	✓	!	!	!	!	!	!	!	✓	!	!	✓	!
20	Netherlands	!	!	✗	✓	!	✗	!	!	!	✗	!	✓	!	!	✗	!
21	Poland	✗	!	!	!	✗	✗	!	✗	!	✗	!	✓	✗	!	✗	!
22	Portugal	!	✓	✗	✓	!	!	!	✗	✓	✗	!	✓	!	!	✓	✓
23	Romania	✗	✗	!	✓	✗	✗	✗	✗	!	✗	✗	✓	✗	!	✗	!
24	Slovakia	✓	✓	!	✓	!	!	✓	!	✓	!	!	✓	!	✓	!	✓
25	Slovenia	!	!	✓	✓	✗	!	✓	!	!	!	!	✓	!	!	!	✓
26	Spain	!	!	✓	✓	!	✓	✓	!	!	✗	!	✓	!	✗	✗	!
27	Sweden	!	✓	✗	✓	!	✗	✗	!	✗	✗	!	✓	✗	!	✗	✓
28	United Kingdom	✗	✓	!	!	!	!	!	!	!	!	✗	!	!	!	✗	✓

✓ covered ! partially covered ✗ not covered

Coverage Table

	EU-Zone	Domestic Legislation transposing NIS2
1	Austria	Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen
2	Belgium	Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique
3	Bulgarian	Законопроект за изменение и допълнение на Закона за киберсигурност
4	Croatia	Cybersecurity Act
5	Cyprus	ΝΟΜΟΣ ΠΟΥ ΤΡΟΠΟΠΟΙΕΙ ΤΟΝ ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΝΟΜΟ ΤΟΥ 2020
6	Czech Republic	Act of 2024, on Cybersecurity
7	Denmark	Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven)
8	Estonia	Küberturvalisuse seaduse ja teiste seaduste muutmise seadus (küberturvalisuse 2. direktiivi ülevõtmine)
9	Finland	Kyberturvallisuuslaki
10	France	Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité
11	Germany	Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
12	Greece	Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 του Ευ-ρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψη-λό κοινό επίπεδο κυβερνοασφάλειας σε ολόκλη-ρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδη-γία NIS 2) και άλλες διατάξεις
13	Hungary	2024. évi LXIX. törvény Magyarország kiberbiztonságáról
14	Ireland	The National Cyber Security Bill 2024
15	Italy	DECRETO LEGISLATIVO 4 settembre 2024, n. 138 Recepimento della direttiva (UE) 2022/2555
16	Latvia	Nacionālās kiberdrošības likums
17	Lithuania	LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMAS
18	Luxembourg	Projet de loi concernant des mesures destinées à assurer un niveau élevé de cybersécurité
19	Malta	EUROPEAN UNION ACT (CAP. 460) Measures for a High Common Level of Cybersecurity across the European Union (Malta) Order, 2025
20	Netherlands	Cyberbeveiligingswet
21	Poland	Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw
22	Portugal	proposta de lei visa autorizar o Governo a aprovar o Regime Jurídico da Cibersegurança, transpondo a Diretiva (UE) 2022/2555
23	Romania	ORDONANȚĂ DE URGENȚĂ privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil
24	Slovakia	Z Á K O N z 28. novembra 2024, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony
25	Slovenia	Zakon o informacijski varnosti (ZInfV-1)
26	Spain	Anteproyecto De Ley De Protección Y Resiliencia De Entidades Críticas
27	Sweden	Cybersäkerhetslagen (CSL)
28	United Kingdom	Cyber Security and Resilience (Network and Information Systems) Bill

Table of National NIS2 Laws

3.2 Patterns, Gaps, and Innovations in National Supply-Chain Security Implementation

Building on the methodology described above, the coverage table reveals substantial heterogeneity in how core supply chain security requirements are transposed into national NIS2 measures. Basic governance controls — notably inventories of third-party entities and products, supplier risk assessments, and the incorporation of information-security clauses into supplier contracts — appear with greater frequency and clarity. Elements that are comparatively well addressed tend to be those that map directly to existing risk-management and procurement practices, making them easier to codify into law. At the same time, several intermediate requirements (for example, documented supplier selection procedures and some aspects of supplier risk scoring) are present in law but often with caveats or limited scope, producing a mix of "covered" and "partially covered" designations across Member States.

The coverage map also shows a high degree of regulatory convergence in the areas of supply-chain risk assessment and communication channels for reporting security vulnerabilities and incidents. Across Member States, transposition laws consistently require organisations to integrate third-party and supplier risks into their overarching cybersecurity risk assessment frameworks, typically through periodic self-assessments, supervisory reviews, or mandatory audits. This reflects a common understanding that supply-chain risks are inseparable from core operational risk management. Similarly, strong convergence is observed in incident and vulnerability reporting mechanisms: national laws uniformly establish formal communication channels with competent authorities and CSIRTs, prescribe strict notification timelines, and increasingly extend reporting beyond incidents to include significant threats, vulnerabilities, and near-misses. Together, these two areas appear to represent the most harmonised elements of NIS2 supply-chain implementation.

On the other hand, procedures for managing end-of-service and end-of-support are the least covered requirement in national NIS2 implementation acts because the NIS2 Directive itself addresses this topic only indirectly through general lifecycle and patch-management obligations. [56] Most Member States therefore prioritised operationally enforceable controls such as risk assessments, incident reporting, and supplier audits, rather than product termination scenarios, which are traditionally regulated through procurement law, contracts, or sector-specific regulation. In addition, the technology- and vendor-specific nature of this requirement makes it difficult to codify in cross-sector cybersecurity legislation, leading to its systematic underrepresentation in national transposition laws.

Similarly, deeper operational controls and lifecycle assurances are less consistently enacted. The table shows limited legal coverage for comprehensive supplier lifecycle management, mandatory acceptance testing of supplier products, and formalized change-management regimes for supplier relationships. Equally notable are gaps in

[56] Annex, Section 6.1.1 & 6.1.2(b), Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555

requirements that underpin resilience over time: explicit duties for suppliers to support business-continuity planning, obligations around end-of-service/end-of-support handling, and mandated security awareness and vetting for supplier personnel. Provisions enabling structured monitoring, independent audit rights, and clear two-way incident-notification channels with suppliers are also uneven.

These coverage patterns carry important analytical implications for the interpretation of the table. The uneven transposition of requirements reflects differing national regulatory priorities, legislative drafting approaches, and levels of institutional maturity in addressing supply chain cyber risk. The concentration of legal detail around baseline risk management, coupled with the relative absence of enforceable provisions for advanced lifecycle, assurance, and resilience controls, suggests that many national frameworks currently emphasize risk identification over sustained risk control. At the same time, since the analysis is based exclusively on primary legislation and does not take into account secondary instruments such as by-laws or technical implementing acts, some of the observed gaps may still be addressed outside the scope of this review. Although most national laws are now close to their final form, the remaining differences suggest that the regulatory landscape is still in a transitional phase, with further convergence toward more detailed and operationally prescriptive supply chain obligations still underway.

Several Member States have introduced notable enhancements in their national NIS2 transposition acts that go beyond the minimum requirements of the Directive. Romania's Emergency Ordinance strengthens supervisory visibility by introducing registration duties that require organisations to document third-party dependencies for the national CSIRT.[57] Slovakia's Cyber Security Act goes further by obliging organisations to report not only incidents, but also significant threats, identified vulnerabilities, and near-misses through its Unified CSIRT, with the option for anonymous reporting.[58] Belgium's NIS2 implementation framework also improves reporting quality by operationalising early-warning and 72-hour notification procedures and requiring structured information fields that explicitly capture supplier involvement.[59] Austria and the Czech Republic follow a similar approach by defining clear communication channels and requiring supplier-related indicators in incident notifications, thereby transforming vulnerability sharing into a formal legal obligation.[60]

[57] Article 11(9), *Ordonanța de Urgență nr. 155/2024 privind măsurile de punere în aplicare a Directivei (UE) 2022/2555 (NIS2).* Monitorul Oficial al României, 2024

[58] Article 1, *Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov, novelizovaný zákonom č. 366/2024 Z. z*. Slovak Republic, 1 Jan. 2025

[59] Articles 34-37, *Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*. Moniteur Belge, 26 Apr. 2024,

[60] Article 16, *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG);* Article 15, 18, 45, 46, *Government Proposal Act No. 181/2014 Coll., on Cybersecurity, as amended 2024. Ministry of the Interior of the Czech Republic, 7 Nov. 2024*.

Some countries have also adopted strict supervisory and audit mechanisms that give supply-chain security greater enforceability. Hungary's Act on Cybersecurity introduces mandatory external audits and sector-specific supervisory rules that require organisations to demonstrate effective supplier controls, including oversight and monitoring of third-party providers.[61] Spain's Draft Bill on the Protection and Resilience of Critical Entities sets out detailed baseline requirements for supplier selection and qualification, providing organisations with clearer expectations for managing external partners.[62]

Furthermore, several Member States have translated supply-chain risk assessment into binding, auditable duties. Belgium's NIS2 implementation framework requires entities to incorporate supplier and third-party risks into their ISMS and to document these dependencies as part of registration and reporting obligations.[63] Germany's BSI-Gesetz integrates the Article 21 security measures into national law and extends risk-assessment obligations to a wider group of essential and important entities, effectively making supplier risk assessment a statutory compliance requirement.[64] France's draft transposition legislation similarly embeds supplier-related risk assessment duties within its critical infrastructure and national resilience framework, linking them directly to registration and supervisory review processes.[65] Together, these national measures turn supply-chain risk assessment from general guidance into a concrete, reviewable obligation enforced by national authorities.

Overall, the comparative analysis demonstrates that Member States are converging on foundational elements of supply-chain cybersecurity—particularly risk assessment, supplier-related incident reporting, and baseline governance controls—while diverging considerably on more advanced lifecycle and assurance requirements. The presence of national innovations in several countries shows that higher levels of supply-chain security are attainable within the NIS2 framework, yet such examples remain exceptions rather than the norm. As the legislative landscape continues to evolve, further alignment is likely to emerge through secondary legislation, implementing acts, and supervisory practice.

[61] Article 4, *2024. évi LXIX. törvény a Magyarország kiberbiztonságáról.* Nemzeti Jogszabálytár, 1 Jan. 2025
[62] Articles 25-26, *Anteproyecto de Ley de protección y resiliencia de entidades críticas*. Ministerio del Interior, 30 May 2025
[63] Article 30, *Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*
[64] Article 30 & 38, *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)*
[65] Articles L.1332-3 & L.1332-4, *Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité*, NOR : PRMD2412608L/Bleue-1, Conseil des ministres, 15 Oct. 2024.

4. HOW NIS2 COULD HAVE ALTERED THE COURSE OF PAST CYBER INCIDENTS

Supply chain attacks and third-party security failures continue to pose significant risks to organizations across critical infrastructure, software development, and telecommunications. These incidents demonstrate how threat actors can exploit trusted partners, from IT service providers to software dependencies, to gain unauthorized access to sensitive data and operational systems. The following case studies—FS Italiane Group, Shai-Hulud 2.0, and UScellular—highlight diverse attack vectors, including supplier compromises, malicious software packages, and failures to properly terminate vendor access. Together, they underscore the importance of robust supply chain security practices, continuous monitoring, and adherence to regulatory frameworks such as NIS2 to mitigate cascading risks.

4.1 Software Supply-Chain Compromise — FS Italiane Group

A significant cyber incident affected Italy's national railway operator, the FS Italiane Group, as a result of a breach at its IT services provider, Almaviva. Rather than attacking the railway operator directly, the threat actor targeted Almaviva, a major Italian technology and digital services company that provides IT, cloud, CRM, and outsourcing services to both public and private sector clients, including FS Group. [66] This makes the incident a classic supply-chain cyberattack, where a trusted third party is compromised to gain access to a larger or more sensitive organization.

Attacker: The breach is attributed to a threat actor using the alias "0xCrypton," who claimed responsibility on a hacking forum and alleged the theft of approximately 2.3 terabytes of data.[67] While the attacker's identity and affiliations have not been publicly verified, they released samples intended to demonstrate the scale and authenticity of the stolen information. The size of the dataset and the nature of the documents suggest the attackers had prolonged and privileged access to Almaviva's internal systems.

Vulnerabilities: The vulnerabilities exploited in the attack have not yet been publicly disclosed in detail. However, available analysis indicates unauthorized access to Almaviva's internal infrastructure, followed by large-scale data extraction. This suggests weaknesses in access controls, monitoring, or segmentation within the provider's environment, highlighting the broader risks associated with third-party IT dependencies, especially when they support critical national infrastructure.

Impact: Through this access, the attackers reportedly exfiltrated a wide range of highly sensitive data linked to FS Group and its subsidiaries, such as Trenitalia and Rete Ferroviaria Italiana. The leaked materials allegedly include long-term strategic and industrial planning documents extending to 2035, confidential contracts with government entities such as the Italian Ministry of Defense and the Air Force, financial

[66] Toulas, Brian. "Hacker Claims to Steal 2.3 TB Data from Italian Rail Group, Almaviva." *Bleeping Computer*, 20 Nov. 2025.
[67] Draghetti, Andrea. "Presunta compromissione di Almaviva e del Gruppo FS" *LinkedIn*, 2025.

records, technical project documentation, and internal communications. In addition, there are reports that personnel data—such as employee records, salaries, and contact details—were compromised, and that some passenger-related information, including passport details, may also be included in the stolen dataset.

The impact of the breach appears potentially to be severe. FS Group faces risks related to exposure of strategic plans, intellectual property, and confidential commercial agreements, which could have long-term competitive and national security implications. Employees and possibly passengers face privacy risks due to the exposure of personal data, raising concerns around identity theft and regulatory compliance under data protection laws. Despite the seriousness of the breach, there has been no indication that railway operations or passenger services were disrupted, and train services reportedly continued as normal.

Response: In response to the incident, Almaviva confirmed that it had suffered a cyberattack and stated that it immediately activated its incident response and cybersecurity procedures. The company reported isolating affected systems while keeping core services operational. Relevant authorities, including Italian cybersecurity agencies, law enforcement, and data protection regulators, were notified, and investigations remain ongoing. [68] At the time of reporting, there was no public confirmation of ransom demands, payments, or a detailed technical disclosure of the attack methods.

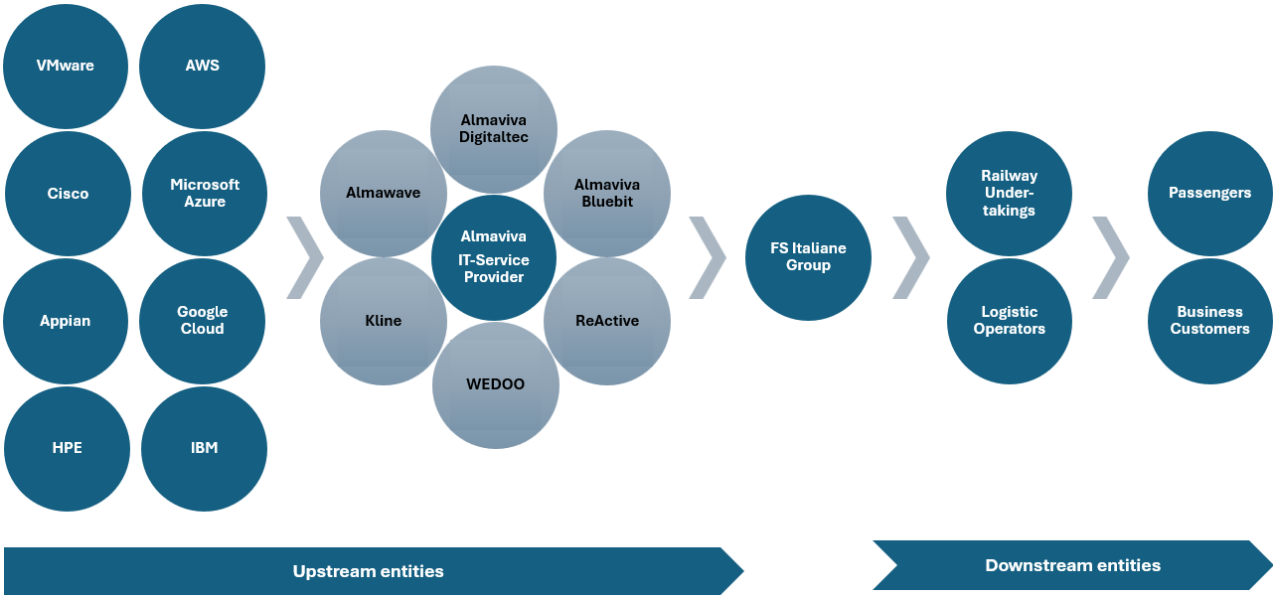
Third-Party Involvement and Risk Context: Almaviva and the FS Italiane Group maintain a strategic partnership focused on digital transformation in transport and mobility. Almaviva acts as a key technology partner, supporting FS Group with the design, development, and operation of complex IT systems such as digital mobility platforms, traffic and infrastructure management solutions, ticketing, data analytics, and cloud-based services. The collaboration has evolved from a traditional supplier relationship into a structured, long-term cooperation, including joint initiatives and shared development of digital solutions that are critical to FS Group's core operations.[69]

Services rendered by Almaviva rely on major third-party providers including AWS, Microsoft Azure, Google Cloud, Oracle, IBM, VMware, Cisco, Dell Technologies, HPE, Adobe, and Appian for cloud infrastructure, enterprise systems, networking, security, and application development. Delivery is further supported by Almaviva group companies—Almaviva Digitaltec, Almaviva Bluebit, Almawave, Kline, ReActive, WEDOO, and the Tecnau Transport Division—which provide specialized capabilities across digital engineering, data, AI, and transport technologies.[70]

[68] "Nota su attacco cyber" *AlmavivA*, 20 Nov. 2025,

[69] *Sustainable mobility: FS Italiane and Almaviva sign agreement on digital solutions*. FS Italiane press release, Dec. 14, 2023

[70] *Partnerships* – *Almaviva Group,* Almaviva official website



Supply-Chain Security Structure of FS Italiane Group

The multi-layered and highly interconnected supply chain depicted above concentrates risk across shared platforms, integrations, and trust relationships: a vulnerability, misconfiguration, or compromise at any upstream provider or Almaviva group entity contains the potential to propagate laterally through shared services or vertically into FS Italiane Group's operational environments. The dependency on major cloud and infrastructure providers introduces exposure to third-party outages, credential compromise, and software supply-chain attacks, while intra-group dependencies increase the risk of cascading impact across multiple services if segmentation and access controls are insufficient. Given the downstream reach to railway undertakings, logistics operators, passengers, and business customers, a cyber incident affecting this supply chain materially impacts operational resilience, safety-critical services, and the protection of personal or business data.

Resilience Through Supply Chain Security: In line with the NIS2 Directive requirements for risk management and supply-chain security, FS Italiane Group likely had baseline third-party governance measures in place prior to the incident, including supplier selection and qualification procedures, contractual information-security obligations, supplier business-continuity and resilience requirements, defined service levels and continuity parameters (SLAs), and established communication channels for incident reporting. As an operator of essential services, FS Group would reasonably be expected to maintain inventories of critical suppliers, clearly defined responsibilities for third-party management, and supplier lifecycle controls consistent with Article 21(2)(d) of NIS2, which explicitly addresses risks arising from supply-chain dependencies.

However, the propagation of the incident through the supply chain—encompassing Almaviva's internal group entities and its upstream technology providers—suggests that third-party security controls were not sufficiently granular or continuously enforced to prevent lateral impact. Limited visibility into subcontractors and third-party components may have delayed the identification of compromised systems within the service provider's environment, allowing unauthorized access and data exposure to persist.

Stronger NIS2-driven measures, such as comprehensive inventories of supplier components, enforceable rules governing subcontracting, and continuous monitoring and audit of supplier systems, could have enabled earlier detection, restricted attacker movement, and reduced the scale of data compromise. More robust implementation of these controls would have strengthened FS Italiane Group's ability to pre-empt, rapidly detect, and contain a cyber incident originating within the multi-tier supplier ecosystem supporting Almaviva.

4.2 Transparency via Software Bill of Materials (SBOM) — Shai-Hulud 2.0 Supply Chain Attack

The Shai-Hulud 2.0 attack is a large-scale software supply chain attack that significantly impacted organizations relying on JavaScript ecosystems and CI/CD automation, including Postman, PostHog, and Zapier. The attackers compromised hundreds of publicly available npm packages in order to obtain credentials and configuration secrets of CI/CD pipelines, developer environments and cloud environments.[71]

Attacker: The identity of the attacker is not publicly known. Analyses of the attack describe the tactics, techniques, and processes used, but do not attribute it to a specific nation, hacker group, or state actor. However, the choice of platforms such as Postman, PostHog and Zapier suggests that the goal is to maximize the exposure of downstream processes by targeting organizations whose tools are widely used in customer environments.[72]

Vulnerabilities: The initial compromise at Postman, PostHog, and Zapier occurred through access to maintainer accounts and the theft of GitHub personal access tokens. These were used to create manipulated versions of legitimate npm packages and publish them in the npm registry.

The manipulated npm packages contained a malicious preinstall script. This installed the Bun runtime environment if it did not already exist and used it to execute a malicious script. This created a new GitHub repository and a runner agent. Additional files including a tool for scanning repositories for secrets were downloaded and executed to query keys and cloud credentials. The stolen credentials were posted to the newly created GitHub repository.[73]

Impact: Due to the compromise of the npm packages, the primary risk to users was the exposure of sensitive credentials, potentially enabling secondary attacks such as

[71] Microsoft Defender Security Research Team. "Shai-Hulud 2.0: Guidance for Detecting, Investigating, and Defending Against the Supply Chain Attack." *Microsoft Security Blog*, 9 Dec. 2025
[72] *Ibid*.
[73] Berkovich, Shay, and Rami McCarthy. "*Shai-Hulud 2.0 Aftermath: Trends, Victimology and Impact*." *Wiz Blog*, 1 Dec. 2025

unauthorized cloud access, repository manipulation, or lateral movement into production environments.

Response: Since the exfiltration of credentials is carried out across multiple victims, this poses a significant challenge for companies trying to determine whether they have been affected, as they would need access to the entire set of leaked data. Various measures have been taken for potentially affected credentials and systems to limit the consequences of Shai-Hulud 2.0, including the removal of unnecessary roles and permissions in CI/CD pipelines, and the isolation of potentially affected CI/CD agents and workspaces.

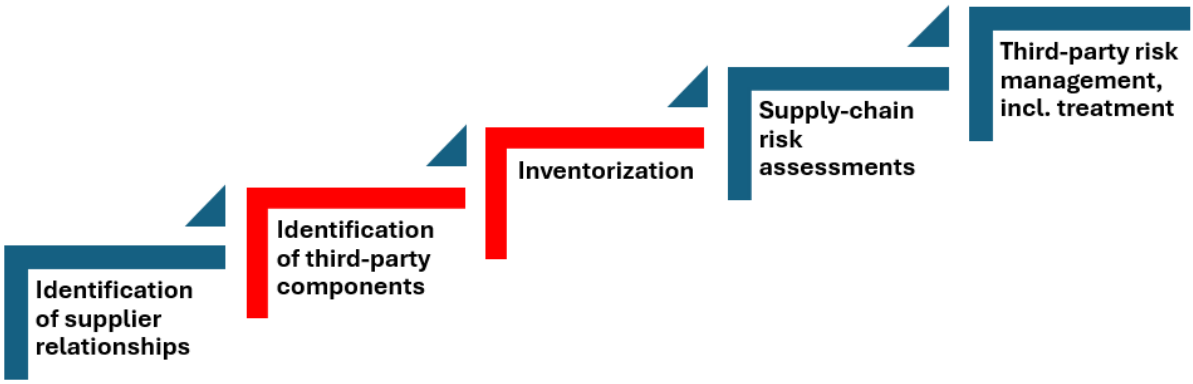
Postman's security team confirmed that several of its public npm packages were infected and promptly unpublished all compromised versions, working with npm support to remove those that couldn't be directly unpublished from its org, and clarified that its core application and production services remained secure. PostHog quickly identified the unauthorized releases of its SDKs and related packages, deleted the malicious versions, revoked the tokens used to publish them, and began issuing clean "known-good" releases while overhauling its CI/CD workflows and adopting a more secure publishing model to prevent similar future breaches. Zapier engineering teams also removed affected npm package versions, advised developers to update to the latest safe releases, and communicated that its core customer-facing services were unaffected, focusing its response on dependency cleanup and credential rotation for developer environments.[74]

Third-Party Involvement and Risk Context: The Shai-Hulud 2.0 attack illustrates how legitimate third-party providers that have themselves been compromised can pose a direct information security risk to their consuming parties.

Packets that lose their integrity as a result of the attack may appear legitimate and thus also compromise the system of the party using them.

The attack makes it clear that dependencies on third-party packages and components must be managed and subjected to risk assessment during the development process. Appropriate security controls must be applied to reduce the risks to an acceptable level.

[74] Eriksen, Charlie. "*Shai Hulud 2.0 Strikes Again: Malware Supply-Chain Attack Hits Zapier & ENS Domains.*" *Aikido.dev Blog*, 24 Nov. 2025



Graphic highlighting the vulnerable phases within the organisation-centric supply chain structure of the victims

Resilience Through Supply Chain Security: In the event of a supply chain attack involving a worm or other self-propagating malware—such as Shai-Hulud 2.0—organizations must be able to conduct rapid impact assessments and initiate targeted incident response measures without delay. A foundational requirement is maintaining a clear inventory of all third-party components used within the environment, enabling swift identification of exposure when otherwise trusted dependencies are compromised. Software Bills of Materials (SBOMs) play a critical role in supporting timely analysis, testing, and remediation—particularly in fast-moving, self-propagating attack scenarios. Adopting an organization-centric supply chain security approach—one that maintains comprehensive inventories of supplier relationships and third-party components in alignment with NIS-2 requirements—would significantly strengthen resilience against such supply chain attacks and improve the ability to detect, assess, and respond to them effectively.

4.3 Failure to Sever a Former Vendor — UScellular 2023 Data Exposure

UScellular reported that in early January 2023, unauthorized actors accessed a misconfigured server operated by a former third-party vendor, exposing data from approximately 52,000 customers, including names, phone numbers, and service-related account information. Samples of the stolen data appeared on a dark web forum prior to the company's announcement.[75]

Attacker: It is not known who carried out the attack or which company was targeted. All that is known is that the targeted company was a former service provider for UScellular whose business relationship ended several years ago.[76]

Vulnerabilities: The misconfiguration allowed the unknown attacker to steal stored data from UScellular customers. The exact misconfiguration is unknown. UScellular's own systems were not affected.

Impact: The data breach affected data from around 52,000 customers. The breached data included customer names, phone numbers and details about mobile phone

[75] Schappert, Stefanie. "*UScellular Breach: New Details Revealed*" *Cybernews*, 28 Mar. 2023
[76] *Ibid*.

services such as tariff types, device types and monthly invoice amounts, which together are referred to as customer proprietary network information (CPNI). UScellular stated that highly sensitive data, such as social security numbers or credit card information, was not among the breached data.[77]

Response: According to UScellular, immediate action was taken to prevent such incidents in the future. The former third-party vendor is cooperating with law enforcement agencies to identify those responsible for the attack, and all information has been removed from the internet. In addition, UScellular reported the incident to law enforcement agencies in accordance with Federal Communications Commission requirements. Affected customers were advised to remain aware of phishing attempts, consider resetting their account passwords and security PINs, and monitor their other accounts for unusual activity.[78]

Third-Party Involvement and Risk Context: This breach highlights how third-party vendors can pose significant security risks even after a contract has ended. The compromised system was linked to a vendor that no longer provided services to UScellular, but whose misconfigured server remained connected and accessible which illustrates a classic supply chain security issue.

Information security risks in this context primarily arise from failing to revoke third-party vendor access to internal organizational resources and to ensure the deletion of data that should no longer be retained by the vendor. Additionally, unaddressed vulnerabilities within the vendor's environment can increase the likelihood of a data breach. In the case of UScellular, insufficient vendor management and limited audit oversight appear to have significantly expanded the organization's risk exposure.

Graphic highlighting the termination phase as a critical weakness within UScellular's supplier lifecycle-centric supply chain structure

Resilience Through Supply Chain Security: Terminating a business relationship at the appropriate time, with due consideration of information security risks, might have mitigated or even prevented the data breach at UScellular.

A supplier lifecycle–centric approach to supply chain security identifies the formal termination of a supplier relationship as its final stage. At a minimum, this stage should be governed by contractual provisions that clearly define the legally compliant retention and deletion of data, the return or secure transfer of information assets, and the proper decommissioning of interfaces, system integrations, network connections, and process dependencies between the third-party vendor and the organization.

[77] UScellular. "*Notice of Data Breach*" *UScellular Newsroom*, 8 Mar. 2023
[78] *Ibid*.

5. POLICY IMPLICATIONS & RECOMMENDATIONS

The effective implementation of NIS2 and related EU cybersecurity frameworks requires coordinated action across institutions, Member States, and individual entities. While EU-level legislation sets common objectives, differences in national implementation, sectoral dependencies, and operational contexts create challenges for consistent supply-chain security. The following sections provide targeted recommendations for EU institutions, Member States, and entities, focusing on enhancing coherence, reducing duplication, and translating strategic requirements into practical, actionable measures across the supply chain.

5.1 EU Level Recommendations

The comparative analysis (Section 3) points to several areas where EU-level action could enhance the effectiveness and coherence of supply-chain cybersecurity. While NIS2 establishes a strong regulatory foundation, differences in national implementation, evolving legislative overlaps, and persistent market fragmentation create challenges for both regulated entities and ICT suppliers.

The following recommendations aim to promote greater consistency, clarify responsibilities across the supply chain, reduce unnecessary compliance burdens, and support a more integrated cybersecurity framework across the Single Market.

Enhancing Operational Guidance for Supply-Chain Cybersecurity: As highlighted in the Coverage Analysis (Section 3.1), Member States are aligning on foundational elements of supply-chain cybersecurity—such as risk assessment, supplier-related incident reporting, and baseline governance controls—yet significant divergence persists in more advanced lifecycle and assurance requirements. This heterogeneity highlights the need for clearer operational guidance at EU level. The EU should further specify high-level NIS2 obligations and support their consistent translation into comprehensive, end-to-end supply-chain cybersecurity controls.

Strengthening supply-chain accountability beyond essential entities: Under NIS2, supply-chain security largely relies on essential and important entities to impose cybersecurity requirements on their suppliers. However, this approach does not always reflect actual power dynamics within supply chains: high dependency on dominant suppliers may limit an entity's ability to enforce adequate security measures, potentially weakening overall resilience. The EU should consider mechanisms to bring strategically significant suppliers closer to the NIS2 regulatory perimeter—for example, by designating certain high-impact suppliers as essential or important entities or by introducing direct cybersecurity obligations for critical providers. The DORA offers a useful reference point, as it assigns explicit risk management, incident reporting, audit, and transparency obligations to critical ICT third-party service providers. Adopting a similar approach, where appropriate, would strengthen incentives, clarify responsibilities, and enhance the effective management of supply-chain risks across sectors.

Aligning requirements between NIS2 and the CRA: ICT vendors in the EU face significant administrative overhead due to fragmented cybersecurity requirements across Member States and sectors. With the entry into force of the Cyber Resilience Act, many vendors will be subject to both CRA and NIS2 obligations, particularly when operating in or supplying NIS-regulated sectors. To prevent duplicative compliance burdens and enhance legal certainty, the EU should prioritize the alignment of the two frameworks. This includes harmonizing security requirements and streamlining vulnerability handling and incident reporting processes wherever possible, ensuring a coherent and efficient regulatory environment for ICT vendors.

Developing a common EU cybersecurity procurement framework: Divergent cybersecurity requirements in public and private procurement create administrative burdens for vendors and risk fragmenting the Single Market. The EU should mandate ENISA to develop a European Supply Chain Security and Procurement Cybersecurity Framework, establishing baseline security requirements and a unified due-diligence methodology. Such a framework would support buyers in securing their supply chains, reduce compliance overhead for suppliers serving multiple customers, and streamline procurement processes across the EU.[79]

5.2 Member State Level Recommendations

The effective implementation of NIS2 requires more than formal transposition; it calls for structured refinement, operational alignment, and coherent integration with related EU instruments. As national frameworks mature, the focus should shift from establishing baseline obligations to ensuring depth, consistency, and practical enforceability across sectors. In this context, Member States play a pivotal role in strengthening supply-chain security, translating strategic risk intelligence into operational requirements, and reducing fragmentation across overlapping regulatory regimes.

Deepening Supply-Chain Controls through Secondary Instruments: As highlighted in the Coverage Analysis (Section 3.1), national transposition of NIS2 places strong emphasis on foundational risk-management measures—such as risk assessments, incident reporting, and supplier audits—while more advanced lifecycle and assurance requirements remain unevenly addressed. End-of-service and end-of-support procedures, comprehensive supplier lifecycle management, structured change management, independent audit rights, and explicit business continuity support obligations are frequently underrepresented in primary legislation. This pattern suggests that many national frameworks currently prioritise risk identification over sustained, long-term risk control. Member States should therefore pursue further alignment and depth through secondary legislation, implementing acts, regulatory guidance, and consistent supervisory practice.

[79] Sciacovelli, Annita Larissa, et al. *ENISA Advisory Group Opinion Paper on NIS2 Post-Implementation*. European Union Agency for Cybersecurity (ENISA), June 2025

Bridging EU-Level Risk Assessments and Entity-Level Implementation: Member States should strengthen their role as an operational bridge between EU-level cybersecurity risk assessments and entity-level risk management. While EU assessments provide strategic and cross-border insights, they are often abstract and complex.

Building on their responsibility to conduct national risk assessments—evaluating the potential impact of service disruption on public safety, public security, public health, the economy and the resilience of interdependent sectors—Member States should use this structured methodology to derive sector-specific security requirements. In particular, by identifying sole providers of essential services, entities whose disruption could cause significant societal or economic harm, entities whose failure could generate systemic or cross-border risks, and entities of specific national or regional importance, national authorities can determine which operators are critical within their national context and tailor corresponding supervisory and security obligations accordingly.

National authorities should therefore translate EU-level findings into clear, sector-specific guidance, supervisory expectations, and practical risk scenarios that reflect both the outcomes of EU assessments and the results of their national criticality analyses.[80] By converting high-level EU risk analyses into actionable national measures—through guidance, implementing acts, and supervisory practice—and aligning them with the identified national risk landscape, Member States can ensure that strategic intelligence is effectively embedded in operational cybersecurity requirements at entity level, thereby enhancing coherence, proportionality, and resilience across the EU.

Streamlining Supply-Chain Controls Across EU Instruments: Member States should seek to streamline and align supply-chain cybersecurity controls derived from different EU instruments—particularly NIS2, the CRA, GDPR, and, where applicable, DORA—by structuring national implementation and guidance along the three complementary dimensions of supply chain security: product-centric, supplier lifecycle-centric, and organization-centric (Section 2.3.2). Mapping legal obligations against these three structures would enhance clarity, avoid duplication, and make compliance more predictable for regulated entities.

In practice, product-related obligations stemming from the CRA should be clearly distinguished from organization-centric risk management duties under NIS2, while supplier lifecycle requirements—such as due diligence, contractual clauses, monitoring, and termination procedures—should be consolidated into coherent national guidance applicable across sectors. By presenting requirements through a unified conceptual framework, Member States can reduce administrative complexity, facilitate supervisory consistency, and support entities in implementing comprehensive, end-to-end supply-chain security controls without unnecessary regulatory overlap.

[80] *Ibid*.

5.3 Entity Level Recommendation

Effectively managing supply-chain cybersecurity requires entities to navigate a complex landscape of overlapping EU regulations and standards. To do so, organisations need a structured approach that clarifies which frameworks apply to them, integrates obligations into a coherent internal requirements framework, and maps controls across product-centric, supplier lifecycle-centric, and organization-centric supply chain structures. By increasing transparency of third-party relationships and conducting comprehensive, entity-level risk assessments, entities can ensure that security measures are proportionate, consistent, and aligned with regulatory expectations, actual operational dependencies und business needs.

Assess Applicability of NIS2 and Related EU Frameworks: Entities should conduct a structured assessment to determine whether, and to what extent, they fall within the scope of the NIS2 Directive and other relevant EU cybersecurity frameworks, such as the Cyber Resilience Act, GDPR, or, where applicable, DORA. This assessment should consider their sector, size, role in the supply chain (e.g. operator, manufacturer, supplier, or service provider), and the nature of the products or services they provide. Clarifying regulatory applicability at an early stage enables entities to identify overlapping obligations, allocate responsibilities internally, and design a coherent compliance strategy that avoids duplication and ensures consistent implementation of supply-chain cybersecurity controls.

Develop an Integrated Requirements and Controls Framework: Entities should establish an internal cybersecurity requirements framework that maps and consolidates obligations stemming from applicable EU regulations, national laws, implementing acts, and relevant standards. By systematically aligning and cross-referencing requirements—rather than addressing each instrument in isolation—organisations can identify overlaps, eliminate duplication, and leverage the strongest elements of each legal and normative framework. Such an integrated approach enhances clarity, improves efficiency in compliance efforts, and supports the consistent implementation of robust, end-to-end supply-chain security controls.

Structure Internal Controls Along the Three Supply-Chain Security Dimensions: Entities should organise their internal policies and processes in line with the three complementary dimensions of supply-chain security: product-centric, supplier lifecycle-centric, and organisation-centric. Security controls derived from applicable regulatory and normative frameworks should be mapped against these structures to ensure comprehensive and coherent implementation. This approach enables organisations to address product-level risks, manage supplier relationships throughout their lifecycle, and maintain robust internal governance of third-party dependencies, thereby strengthening end-to-end supply-chain cybersecurity while avoiding fragmented or ad hoc controls.

Increase Transparency of Third-Party and Component Dependencies: Entities should systematically identify, document, and contextualise third-party involvement in their business processes, as well as third-party components embedded in their products and

services. By mapping these dependencies and clarifying their role, criticality, and associated risks, organisations can gain a transparent and structured understanding of their supply chain. This visibility is essential for informed risk assessment, effective contractual management, and the implementation of proportionate security controls across both operational processes and product architectures.

Conduct Comprehensive Entity-Level Risk Assessments: Entities should conduct structured, organisation-specific risk assessments under Article 21 NIS2, building on a clear and documented understanding of their third-party relationships and embedded components. Applying an all-hazards approach, these assessments should cover risks to network and information systems arising from operations, the physical environment, and the supply chain. Based on transparent mapping of suppliers, service providers, and third-party components, entities should evaluate supplier-specific vulnerabilities, the cybersecurity quality and resilience of products and services used, and the secure development practices of providers, while taking into account relevant EU- and state-level coordinated risk assessments.[81] This integrated approach ensures that internal controls, procurement decisions, and contractual arrangements are proportionate, risk-based, and aligned with the entity's actual dependency landscape.

[81] *Ibid*.

6. CONCLUSION

The NIS2 Directive establishes a comprehensive framework for supply-chain security, embedding risk management into a multi-level governance structure that spans EU-level coordinated assessments, national risk evaluations, and entity-level controls. By integrating technical, operational, and organisational measures, NIS2 positions essential and important entities to manage risks across direct suppliers and service providers, while the Cyber Resilience Act, GDPR, and DORA provide complementary protections at the product, data, and operational levels. Comparative analysis of national transpositions highlights both convergence on foundational controls—such as supplier inventories, risk assessments, and incident reporting—and divergence in advanced lifecycle, assurance, and resilience measures, reflecting differing regulatory priorities and institutional maturity.

To strengthen EU supply-chain security, a coordinated, multi-stakeholder approach is essential. At the EU level, enhanced operational guidance, alignment across frameworks, and a unified cybersecurity procurement methodology will improve consistency and reduce administrative burden. Member States should translate EU strategic risk intelligence into actionable, sector-specific requirements, deepening lifecycle and assurance controls while aligning supervisory practices across instruments. Entities themselves must assess regulatory applicability, integrate obligations into a consolidated internal framework, map security controls across product-, supplier-, and organisation-centric dimensions, increase transparency of third-party and component dependencies, and conduct robust, all-hazards risk assessments.

Together, these measures create a layered, resilient approach that aligns strategic objectives with operational implementation, promotes consistency across the Single Market, and strengthens end-to-end cybersecurity across EU supply chains, supporting both regulatory compliance and real-world operational resilience.

AUTHORS

Thomas Krüger is an experienced information security professional specializing in governance, risk, and audit within critical infrastructure environments. Since 2019, he has served as an expert at DB InfraGO AG, where he focuses on developing ISMS frameworks, aligning policies with ISO 27001 standards, and advancing centralized security service concepts. His work includes refining security processes and strengthening organizational resilience—key elements in supply chain security.

Previously, Mr. Krüger contributed to security consulting and large-scale project reviews, as well as the design of security lifecycle models for complex systems. His background in IT security management includes incident response, reporting, and SOC process development. He began his career at EY in forensic data analytics, building automated solutions and supporting investigations. Mr. Krüger holds a Master's degree in Mathematics and multiple certifications, including CISM and CISA.

Stefan Hartmann is a dedicated professional at the intersection of business, information technology, and law. He currently serves as Referent for Information Security at DB InfraGO AG, where he applies his interdisciplinary expertise to address complex challenges in cybersecurity and compliance.

Mr. Hartmann's academic journey began with a Bachelor's degree in Business Administration from Fachhochschule Düsseldorf, followed by a Master's in Business Informatics from Hochschule Niederrhein. Currently, he is pursuing a Bachelor of Laws at Fernuniversität Hagen, further expanding his ability to integrate legal perspectives into technical and organizational contexts.

As a certified ISO 27001 Lead Auditor, Stefan combines his technical and legal knowledge to enhance security governance and risk management. His professional experience includes developing security training programs, conducting threat analyses, and supporting compliance initiatives. His multilingual skills and certifications in ITIL v4 and SAFe 5 Agilist reflect his commitment to excellence in a rapidly evolving field.

Dr. iur. Yasir Gökçe is a senior information security and legal professional with extensive experience in governance, risk, audit, and regulatory compliance, currently serving as Director at instituDE and Senior Expert in Information Security at DB InfraGO AG. He has a proven track record in leading ISO/IEC 27001 and BSI-based audits, conducting risk assessments, and advising on mitigation strategies across complex infrastructures.

With a multidisciplinary background spanning cybersecurity, law, and public policy, Mr. Gökçe has held roles in consulting, legal advisory, and government, contributing to the development of information security strategies and ISMS frameworks. His work supports alignment with evolving regulations, including the NIS2 Directive, with a focus on strengthening supply chain security.

He holds a PhD in international law applicable to cyberspace, earned advanced degrees from Harvard Kennedy School and other leading institutions, and maintains professional certifications including CISSP, CISM, CISA, and ISO/IEC 27001 Lead Implementer/Auditor.