Dignitas Group

The NIS2 blueprint:

From legislation to resilience

Contents

Executive summary 3

Introduction 3

NIS2 beyond the legal text: The compliance obstacle 4

The anatomy of NIS2: The core requirements 5

- Essential and important entities 5
- Management bodies, compliance, liability & accountability: The governance recalibration in NIS2 5
- Risk management re-centred 6
- Incident management & resilience 6
- Third-party and supply-chain assurance: Extending beyond the perimeter 7
- Legislative constellation of NIS2 in EU law 7
- Sub conclusion 9

Operationalising cybersecurity resilience with built-in NIS2 assurance 10

- Limitations 10
- Sub conclusion 11

Conclusion 12

References 13

Executive summary

This whitepaper examines the NIS2 Directive and addresses the central question: which cybersecurity framework can reliably serve as a foundation for demonstrating NIS2 compliance, meeting regulatory expectations, and guiding executive oversight? Six principal findings emerge:

Among NIS2's most consequential innovations is the introduction of personal liability for management. Executives of Essential and Important Entities (EIEs) bear explicit legal accountability for cybersecurity oversight and may be temporarily disqualified or individually sanctioned in cases of misconduct or persistent non-compliance.

The principal challenge facing organisations lies not in awareness of the Directive, but in operationalising its requirements. A significant gap persists between regulatory expectations and organisational capacity for implementation, particularly among small and medium enterprises (SMEs) with limited prior regulatory experience.

Risk management constitutes the foundational imperative of NIS2 implementation. It determines proportionality, informs the prioritisation of mitigating measures, and underpins the demonstrability of compliance with the Directive's requirements.
NIS2 introduces mandatory, time-bound incident reporting obligations: an early warning within 24 hours of awareness, formal notification to the designated CSIRT within 72 hours, and submission of a final report within one month.

NIS2 operates alongside CER, DORA, CRA and GDPR. Whilst these instruments share recurring themes, including governance expectations, incident-reporting obligations and sanctions, their scope and evidencing requirements are not identical. A structured, integrated framework can substantially reduce the burden of concurrent compliance.

ISO/IEC 27001 offers a pragmatic and auditable pathway to NIS2 compliance. It's risk-based, scalable approach operationalises the Directive's obligations within a certifiable management system, whilst simultaneously strengthening supply chain assurance across heterogeneous regulatory environments.

Introduction

The evolving cyber threat landscape within the European Union (EU) has prompted a significant regulatory shift, culminating to the publication of the Network and Information Security Directive (NIS2) in 2022 (Directive (EU) 2022/2555). As the successor to the original NIS Directive, NIS2 was introduced to address modern threats that increasingly target critical infrastructures and essential services across member states. Its core objective is to raise the overall level of cybersecurity and resilience of essential and important entities (EIEs) within the Union by harmonizing expectations, enhancing cross border cooperation, and introducing stricter, more comprehensive security requirements. This paper focuses exclusively on the obligations applicable to EIEs and does not address the obligations of Member States. Earlier approaches allowed organizations to interpret cybersecurity requirements with greater flexibility, whereas NIS2 demands auditable, evidence based compliance. Increase in regulatory rigor also extends to executive leadership. Under NIS2, executives and board level management bear explicit legal accountability for cybersecurity oversight, strategic decision making, and risk mitigation. Despite being mandated to provide informed and active supervision, many leaders still lack the necessary overview, roadmap, and structured framework to understand and carry out their responsibilities. The directive introduces compounding requirements for governance, resilience, supply chain security, monitoring, and incident response, leaving organisations wondering how compliance efforts should be structured. Additional pressure for organisations is introduced to satisfy diverse regulatory contexts and needs. The essential question therefore emerges: Which cybersecurity framework can reliably serve as a foundation for demonstrating NIS2 compliance, meeting regulatory expectations, and guiding executive oversight? Addressing this question is critical to enabling organizations to transform regulatory mandates into practical, sustainable, and auditable cybersecurity practices.

NIS2 beyond the legal text: The compliance obstacle.

The NIS2 Directive significantly expands cybersecurity obligations for organisations designated as Essential and Important Entities (EIEs). While the directive sets out a comprehensive framework aimed at strengthening cyber resilience across the European Union, translating its legal provisions into practical implementation remains a considerable challenge for many organisations. The directive outlines a range of requirements, including risk management measures, incident reporting obligations, governance responsibilities, and supply chain security. However, the legal language in which these obligations are expressed often leaves room for interpretation, making it difficult for organisations to determine what concrete actions are required in practice. At the same time, EIEs operate within an increasingly complex environment. The cybersecurity threat landscape continues to evolve rapidly, regulatory requirements across the European digital framework are becoming more fragmented, and authoritative guidance on implementation remains limited in many jurisdictions. Compounding these challenges is a persistent shortage of qualified cybersecurity professionals capable of supporting organisations in translating regulatory requirements into operational controls. Together, these factors create a significant compliance challenge for EIEs.

For many organisations, the challenge of NIS2 does not lie in awareness of the directive, but in understanding how its legal requirements should be implemented in daily operations. Many leaders navigating NIS2 find they have more questions, challenges and concerns than answers on how to fulfil the Directive's requirements and establish compliance. A significant gap remains between regulatory expectations and organisations' ability to operationalise them. Parlov et al. (2025) argues that cyber resilience is still approached primarily as a compliance exercise rather than as proactive threat mitigation, thereby undermining the Directive's core objective of resilience.

Organisations that recognise they fall within the scope of NIS2 are often uncertain about how to demonstrate compliance, particularly small and medium enterprises (SMEs) with limited prior regulatory experience.

NIS2 imposes significant requirements, especially for smaller organisations with limited resources, both financially and expertise. It may be contended that the NIS2 Directive entails a disproportionate compliance burden for smaller organisations owing to resource constraints and reduced economies of scale (Joswig & Kurz, 2025). Mentzelou et al. (2025) argues that excessive compliance-related costs can divert resources from innovation, thereby discouraging smaller organisations from pursuing compliance-driven cyber resilience. While robust risk management can guide the selection of the most value-accretive investments, SMEs often struggle to develop mature risk-assessment systems (Mentzelou et al., 2025). Many organisations lack budgetary room for substantial investments. Investments are at times discontinued owing to benefits not being readily apparent nor quantified, thereby diminishing the incentive for continued investment. Notwithstanding deteriorating cyber-risk economics, evidenced by elevated breach costs and increasing aggregate losses, the rationale for continued investment is strengthened even as budgets tighten (Mentzelou et al., 2025). This reiterates the need for proportionate interpretation of legal texts to pragmatic guidelines.

SMEs often depend on both their internal IT workforce and external suppliers for cybersecurity decision-making. Divergent priorities and uneven expertise can impede implementation, particularly where in-house knowledge is limited (Joswig & Kurz, 2025). Demand for cybersecurity professionals consistently outstrips supply, and pipeline fulfilment lags as roles typically require formal education, certification and experience (Mentzelou et al., 2025). These challenges could further drive up the cost of compliance. Besides investments, adopting NIS2 requirements will necessitate organisational change; when management prioritises business-as-usual, adoption may be delayed and place additional strain on the workforce (Mentzelou et al., 2025). The Directive seeks to reinforce top-down sponsorship of IT and cybersecurity by mandating training for members of the management body (Vandezande, 2024).

In addition to constrained access to cybersecurity expertise, SMEs frequently do not obtain timely knowledge regarding recent developments in the threat landscape (Joswig & Kurz, 2025). The landscape is increasingly complex and evolving rapidly, extending beyond IT components to encompass organisational, process and human factors. The human element, often overlooked, is frequently the weakest link. Exploitation thrives where security awareness is low and internal structures are weak, producing poor incident reporting, susceptible employees, and ineffective security controls (Parlov et al., 2025).

Although several requirements are precisely articulated with definitions, substantial portions are interpretive, depriving leadership of unambiguous implementation guidance. Besides this, by requiring measures to be appropriate and proportionate without detailing the criteria, the Directive permits substantial interpretive flexibility. Persistent ambiguity around key definitions in the Directive may delay organisations' adoption of NIS2 requirements (Mentzelou et al., 2025; Ruohonen, 2024). Mentzelou et al. (2025) marks the complexity of legal texts as challenging for especially SMEs. Translating requirements into their specific organisational context often leads to uncertainty, resulting in insufficient allocation of resources and a lower priority for compliance activities. As regulatory requirements increasingly overlap and run concurrently, complexity grows, emphasizing the need for a scalable, flexible framework. It remains unclear how supply

chains spanning heterogeneous regulatory regimes will be affected. Simultaneously, as security and privacy concerns intensify, stakeholders increasingly depend on demonstrable regulatory compliance as a source of assurance (Joswig & Kurz, 2025).

NIS2 can be viewed as a baseline that Member States must transpose into national law, potentially introducing divergent requirements and compliance uncertainty. This, in turn, risks undermining its principal objective: harmonising EU-level coordination and achieving comparable security levels. Additionally, transposition of the Directive into national law has been slow and fragmented, with some Member States entering 2026 without national legislation in place. National interpretation of the Directive remains in development across several Member States, leaving expectations uncertain and exposing early adopters to near-term changes. Although the Directive is founded on the principle of proportionality, smaller EIEs may struggle in practice due to contextual constraints and limited guidance and support from competent authorities. Furthermore, the expectations placed upon EIEs, particularly as regards governance, audit, and assurance, remain insufficiently articulated. Implementation efforts may be further dampened by expectations that sector-specific requirements will emerge.

Altogether, the principal challenge lies not merely in recognising NIS2's significance, but in understanding its concrete organisational requirements and overcoming the associated barriers. Accordingly, the next chapter sets out a structured analysis of the Directive's key obligations to support effective implementation.

The anatomy of NIS2: The core requirements

As aforementioned, NIS2 sets requirements across multiple themes to establish a common level of cybersecurity among Member States, with a clear focus on resilience. Its predecessor sought to establish a common level of cybersecurity for essential services, yet Member States articulated markedly divergent requirements (Vandezande, 2024). E.g., an entity may have been designated 'critical' in one Member State, while an identical counterpart in another is not, undermining a level playing field. NIS2 introduces more detailed designation criteria to reduce ambiguity and advance a common level of cybersecurity and resilience. The following sections review the most salient requirements and the interplay between NIS2 and other EU legislation.

Essential and important entities

NIS2 differentiates from essential and important entities, whereas its predecessor was limited to providers of essential services (Vandezande, 2024). The expansion of the scope recognises the potentially protruding effects of disruptions in essential services (Mentzelou et al., 2025). Ruohonen (2024) argues that with the scope expansion, conceptual stretching may occur and the demarcating non-critical entities from critical entities becomes increasingly difficult. While the Directive seeks to exclude smaller organisations, it applies irrespective of size where specified criteria in the Directive are met, c.q., they are marked 'critical'. Per Article 27, entities in scope must notify and register with the competent authorities, enabling oversight and supervision, as well as evidence-based, targeted assistance to entities. Article 28 further provides for the registration of entities' DNS information, recognising its value for analysing and resolving cybercrime. Another material extension of the Directive's scope and applicability is the express inclusion of Operational Technology (OT). The inclusion of OT concurs that downtime of such systems can disturb essential activities. This expansion is especially challenging as OT inherently harbours vulnerabilities and the rapid pace of industry digitalisation is outstripping security controls (Teichmann, 2025).

Management bodies, compliance, liability & accountability: The governance recalibration in NIS2

A substantial change from the predecessor is the expanded responsibility of EIE management bodies, with explicit measures they are required to undertake. Management bodies of EIEs must approve cybersecurity riskmanagement measures, oversee their implementation, and undertake cyberspecific training, thereby ensuring they remain adequately informed and maintain competence.

Among NIS2's most consequential innovations is the introduction of personal liability for management.

Mentzelou et al. (2025) argues that this marks the shift to performance-based accountability. Besides a set of minimum requirements, for risk management and incidentimpact requirements, the principles of appropriateness and proportionality apply. Proportionality should be determined with reference to the entity's size and exposure, applicable European standards, the cost of implementation, and the likelihood and impact of incidents (Ferguson, 2023). Entities may be subject to announced or unannounced information requests, site visits, and security audits or technical scans (Vandezande, 2024). Notably, independent or competent bodies are to carry out audits, with the audited party carrying the financial burden. Given this, entities may benefit from demonstrable compliance and continuous readiness, which reduces the potentiality and cost of audits.

Non-compliance with NIS2 can result in penalties, including financial fines. In short, financial penalties for essential entities may be imposed up to €10 million or 2% of total worldwide annual turnover from the preceding financial year, whichever amount is higher (Article 34(4)), and for important entities may be imposed up to €7 million or 1.4% of total worldwide annual turnover from the preceding financial year, whichever amount is higher (Article 34(5)). Besides monetary penalties, non-monetary penalties may include compliance orders, binding instructions, mandatory security audits, public warnings, notification requirements, and service restrictions. NIS2 permits the temporary disqualification of senior executives from managerial duties where non-compliance persists, until identified deficiencies are corrected and compliance is restored (Singh, 2023). Furthermore, given the provision for personal liability, individuals may be subject to direct fines, temporary bans, public naming, and where gross negligence or wilful misconduct is established: criminal prosecution. This applies to both essential and important entities. Further reputational risk arises from the possibility that competent authorities may require a public statement regarding an infringement, including the naming of responsible persons.

Risk management re-centred

Given the principle of proportionality, robust risk management should be the first substantive step in implementing NIS2, enabling organisations to prioritise effort where it matters most. A risk is defined as "the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident" in NIS2 (Article 6(9)). Ferguson (2023) interprets the risk requirement as "EIEs are required to manage the potential for an incident to cause loss or disruption in the ability of the network and information systems EIEs use for their operations or service provision to resist, at a given level of confidence, any incident". Adequate understanding of the threat landscape is required to achieve sufficient operational readiness (De Valk, 2022). Upon attaining a comprehensive understanding of the organisation's context, including an assessment of internal and external threats, relevant risks are identified. The identified risks should be evaluated using established methods, most commonly done by assigning scores for likelihood of occurrence and the impact of materialisation. Robust risk analysis should consider gross (inherent) and net (residual) risk to distinguish baseline exposure from the effect of controls, thereby enabling prioritisation of treatment and alignment with risk appetite. Risk appetite, defined by International Organization for Standardization (2022) as "amount and type of risk that an organisation is willing to pursue or retain" (clause 3.3.27) should be carefully designed and not confused with risk tolerance, being the "organisation's or interested party's readiness to bear the residual risk in order to achieve its objectives" (clause 3.3.28). In summary, the risk appetite reflects the policy for risk taking. Both risk evaluations and the defined risk appetite should be kept under continual review, reflecting the rapidly evolving threat and business landscape and ensuring accuracy of the established risk framework. For example, Kioskli et al. (2025) explains that Artificial Intelligence (AI) introduces substantial new organisational risks, including enhanced social-engineering capabilities, the automation of intrusion activities, and data leakage arising from irresponsible use. Risks that exceed the organisation's appetite should be treated with mitigating measures to bring exposure within appetite. While NIS2 does not enumerate a single, universal control catalogue, it relies on risk-based management for each organisation to determine a proportionate and appropriate set of mitigating measures. Besides conventional risk management practices, Article 21(2) prescribes an all-hazards approach and requires organisations to consider "supply chain security, so-called cyber hygiene practices, authentication, encryption, human resources security, and even business continuity" (Ruohonen, 2024, p. 10). The all-hazards approach is, in itself, not unprecedented, given that robust risk management is inherently all-hazards. Its novelty lies in its explicit codification as a legislative requirement. Entities should consider any event capable of compromising network and information systems, including hazards arising from the physical environment in which those systems operate; the risk picture therefore extends beyond the digital domain (e.g., climate-related events and insider threats).

Incident management & resilience

While risk management is primarily directed at preventing adverse events, NIS2 equally emphasises incident response and, more broadly, operational resilience. Notably,

EIEs are not explicitly required to prevent incidents; rather, they are obliged to minimise incident impact (Ferguson, 2023).

NIS2 defines an incident as "an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems" in Article 6(6). A principal objective is to ensure the continued provision of essential services during an incident, or, where continuity cannot be maintained, to restore such services without undue delay. Parlov et al. (2025) identifies "three primary forms of data exposure: leakage, unavailability, and manipulation" (p. 17). Considered together, these exposure types highlight the importance of incident management to ensure timely detection, effective containment and orderly recovery.

A widely recognised obligation under the NIS2 Directive is the duty to report incidents to the designated Computer Security Incident Response Teams (CSIRT) (or competent authority). Notification obligations are primarily designed to incentivise compliance and strengthen awareness (Ferrari, 2023). Moreover, such mechanisms support the identification of systemic issues and alert enterprises accordingly; in addition, notification can prompt assistance from the competent authorities.

Prior to NIS2, disclosure of cybersecurity incidents was largely at an organisation's discretion, where under NIS2, incident reporting is made mandatory (Boggini, 2024).

NIS2 introduces timebound mandatory reporting obligations for significant security incidents to authorities (Rehbohm & Moses, 2023). In this context, a 'significant incident' is one where "the company has or will suffer significant financial loss or severe operational disruption, or a natural or legal person could be affected or could be capable of being affected by causing considerable material or non-material damage" (Boddy, 2025, p. 21). These require early warning within 24 hours of awareness, formal notification to CSIRT within 72 hours, and submission of a final report within one month. If an incident constitutes a personaldata breach, the General Data Protection Regulation (GDPR) governs notification, and the CSIRT will notify the relevant Data Protection Authorities (DPAs) accordingly. Antithetically, there is ongoing discourse that the publication of incidents, whether under NIS2 or other legislation may subvert the objectives of protection and resilience since early or overly granular disclosure can expose unresolved vulnerabilities and defensive gaps, invite copycat/followon attacks, and divert scarce response resources while remediation is still underway (Ferrari, 2023). Boggini (2024) establishes how incidents translate into reputational harm and liability risk, with direct consequences for organisational performance. Moreover, contractual penalties and damage to partnerships are listed as indirect effects of disruptions due to a cyber incident (Teichmann, 2025). Insufficient reporting of such incidents may also be detrimental to market position (Mentzelou et al., 2025). Beyond purely commercial impacts, incidents may adversely affect natural persons, including via personaldata compromise and interruptions to critical infrastructure or services, or a combination of the two (e.g., power or hospital services) (Vandezande, 2024). Still, annual incident reporting can benefit organisations by evidencing operational resilience, upholding the rights of individuals, raising awareness across the value chain, and demonstrating compliance with cybersecurity legislation (Boggini, 2024). Besides reporting incidents, organisations are expected to share intelligence on threats and vulnerabilities to aid incident prevention (Vandezande, 2024). NIS2 Article 12 stipulates that this will culminate in the creation of a European vulnerability database, governed by ENISA.

Third-party and supply-chain assurance: extending beyond the perimeter

The NIS2 Directive establishes a persistent through-line concerning supply-chain and third-party risk management across its provisions. Foremost, supply-chain security is integrated into risk-management obligations, e.g., by addressing the vulnerabilities of direct suppliers. The NIS2 Directive is, to an extent, novel in its approach, extending obligations to multiple actors across the supply chain and prescribing the tailoring of measures to an organisation's specific circumstances.

As a consequence of digitalisation, organisations have become increasingly dependent on managed service providers, i.e. defined in NIS2 Article 6(39) as "an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely". Supply chains are becoming more complex through digitalisation, with third and fourthparty dependencies, outstripping governance visibility and control.

A subcontractor with sub-par security within the supply chain can jeopardise, and even bring down, critical infrastructure.

As digital supply chains grow and become more complex, they can advantage threat actors by turning interconnected vendors and service providers into entry points or stepping stones towards larger downstream victims or widespread disruption or both. Furthermore, thirdparty risk is frequently underestimated, with organisations overlooking vendors that process or access sensitive data or deliver critical services resulting in systemic exposure (Parlov et al., 2025). Notwithstanding the exemptions provided for, NIS2 prescribes circumstances in which entities shall be regarded as essential even where an exemption might otherwise apply, including where the entity delivers a critical function, product or service. The NIS2 Directive leaves interpretive latitude regarding the extent of supplychain risk management efforts, as it does not precisely define where the supply chain begins and ends (Van 't Schip, 2024).

By outsourcing services to managed service providers, so-called third parties, organisations may be unaware of the ensuing chain of dependencies upon which their processes depend. Each actor within a chain has vulnerabilities which could pave the way for malicious actors towards their potential victim (Van 't Schip, 2024). Unremedied vulnerabilities and weaknesses that prompt incidents often fail to reveal the underlying root causes, such as security culture and third-party risk management (Parlov et al., 2025). Escalating cascading failures highlight the need to harden the supply chain, with risk management setting insight and priorities. Vigorous cybersecurity strategies and controls are developed in response, with the overarching objective of preventing operational disruption. Harmonised security strategies are increasingly important, as resilience improves when more parties across the chain make mutually beneficial investments, thereby making the benefits of such investments more visible (Van 't Schip, 2024).

Legislative constellation of NIS2 in EU law

Beyond NIS2, organisations may be subject to other EU legislation, creating uncertainty about how the respective requirements align, differ and can be addressed jointly. The

following section reviews the most relevant adjacent EU instruments and their requirements, with particular emphasis on incident-reporting obligations and penalties. It should be noted beforehand that a regulation is a binding act with direct applicability, whereas a directive sets common objectives that Member States must transpose into national law.

Critical entities resilience directive

Complementary to NIS2, the Critical Entities Resilience Directive (CER) (Directive (EU) 2022/2557) entered into force concurrently. Similarly, CER is also to be translated into national legislation. Both directives mandate risk management, incident notification, recovery planning, and business-continuity capability (Boddy, 2024). CER applies to sectors: energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public infrastructure, space and production, processing and distribution of food. Unlike NIS2, the CER Directive focuses on strengthening resilience to non-cyber threats, for example extreme weather (flooding), physical sabotage of substations, or terrorist attacks. Critical entities are designated on the basis of their importance to the economy and the functioning of society. Organisations operating in sectors essential to societal and economic functioning may therefore be classified as critical. Member status are ultimately responsible for identifying critical entities. Organisations may be designated as critical under both NIS2 and the CER Directive, and must comply with both frameworks (Vandezande, 2024). With national laws still pending in several Member States, it is unclear what dual designation (NIS2 and CER) means for affected organisations.
Incidents that (potentially) disrupt the provision of essential services, assessed by the number of users affected, the duration of disruption, and the geographical scope (isolated vs. widespread) are to be reported to appointed authorities (Boddy, 2024). CER also provides incident reporting timelines. An early warning must be submitted to the competent authority within 24 hours of awareness of the incident, yet no 72 hours notification is described.

Within the CER, penalty amounts are not quantified; instead, Article 22 stipulates that sanctions must be “effective, proportionate and dissuasive.”

Digital operations resilience act

Digital Operations Resilience Act (DORA) (Regulation (EU) 2022/2554) is a sector-specific regulation for financial institutions, prescribing specific requirements on resilience and risk management. Both NIS2 and DORA force organisations to consider continuity and risk management (Mentzelou et al., 2025). As with other EU directives and regulations, enforcement, implementation, and supervision are delegated to the competent national authorities. ICT third-party providers are also within DORA’s scope, allowing requirements to cascade through the supply chain. DORA describes reporting obligations of major ICT incidents, being “an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity” (Article 3(10)). Reporting to relevant authorities proceeds in three stages: (i) initial notification, (ii) interim report providing new information, and (iii) final report setting out the root-cause analysis (Bobby, 2024). DORA’s reporting timelines broadly mirror NIS2. An initial notification should be made as early as possible, expected within 4 hours of awareness, and in any case no later than 24 hours. An intermediate report must be submitted within 72 hours (regardless the availability of new information) (AFM, 2022). Lastly, a final report is due within one month of the most recent intermediate report.

DORA does not quantify penalties at EU level; instead, it leaves the determination of fines to the Member States. Criminal sanctions may also be imposed under national law. As in many legal frameworks, national law typically sets fines as a maximum percentage of turnover in the preceding financial year, subject to an absolute monetary cap. Defined fine percentages typically range from 5-10%, with absolute ceilings between €2 million and €20 million; several Member States differentiate these maxima by the nature of the breach or the provisions infringed (D’Ormesson et al., 2025). Similarly to NIS2, personal liability is provisioned under DORA; Article 50 sets out the possibility to administer fines to members of the management body or otherwise responsible persons. D’Ormesson et al. (2025) further shows that certain Member States have set individual fine ceilings ranging from €100,000 to €5 million, in some cases calibrated to the individual’s income.

As with CER, organisations may be subject to both NIS2 and DORA.. DORA shall be treated as the sector-specific lex specialis for financial entities and, accordingly, supersedes the relevant NIS2 provisions insofar as it lays down equivalent requirements for the matters concerned.It should also be noted that DORA sets out more detailed requirements across multiple themes. For requirements prescribed under NIS2 that are not addressed by DORA, entities should implement the relevant NIS2 measures as a complementary layer. AFM (2022) explains that dual incident and threat reporting obligations may occur. Similar to NIS2, DORA requires companies to report relevant cyber threats; however, it remains unclear whether authorities will consolidate such notifications into a single, centralised threat database or maintain separate repositories.

Cyber resilience act

The Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847) focuses on the cybersecurity of products with digital elements, imposing obligations on manufacturers, software developers, importers, distributors, and resellers. In summary: NIS2 fortifies organisational cybersecurity; the CRA integrates security into software and products across their lifecycle. CRA establishes core requirements covering (i) risk assessment and management, (ii) incident handling, (iii) vulnerability management and disclosure, (iv) software and hardware update management, and (v) transparency and documentation (Jara et al., 2024). As for incident notification, Article 14(4) describes that manufacturers must report actively exploited vulnerabilities and severe incidents

affecting the security of products with digital elements: an early warning within 24 hours of awareness, a full notification within 72 hours, and a final report no later than 14 days after a corrective measure is available for actively exploited vulnerabilities and within one month for severe incidents. Notifications are to be made to the CSIRT. The CRA employs the definition of an incident as set out in NIS2. Under Article 64(2) of the CRA, non-compliance may attract administrative fines of up to €15 million or 2.5% of total worldwide annual turnover for the preceding financial year, whichever is higher. With the CRA's prescriptive product requirements and NIS2's organisational controls, dual-in-scope entities can align artefacts and evidence across both regimes, often more straightforwardly than under other legislative combinations. Given the limited contradictions and modest overlaps between the regimes, dual applicability of NIS2 and CRA should not, in itself, pose material challenges to harmonised implementation, beyond the general compliance burden.

General data protection regulation

The GDPR (Regulation (EU) 2016/679) emerged in the same period as NIS2's predecessor; the former provides the EU's legislative framework for personal data protection, while the latter focuses on national-level cybersecurity. The interconnection between the legislation is undeniable, as NIS2 entities also fall under the GDPR and share an obligation to implement appropriate technical and organisational measures. Leaders may run confused to the conflict between GDPR and NIS2, the distinction being: "GDPR holds primary authority over data privacy, NIS2 establishes exclusive authority over cybersecurity and critical infrastructure protection" (Mentzelou et al., 2025, p. 4). Their objectives are unsimilar: NIS2 pursues the continuity of critical products and services, while the GDPR safeguards the right to privacy of natural persons. Understanding the distinctions provides practical guidance on their coexistence. Both regimes require notification of incidents to the competent national authorities. By contrast with NIS2's staged timeline, the GDPR requires that personal-data breaches be reported within 72 hours of becoming aware. Note that this requirement pertains to the initial notification; subsequent submissions, such as the final report (including root-cause analysis and remediation measures) and any notifications to data subjects, are afforded additional time, yet without undue delay. Under the GDPR, notification is required when personal-data is breached, meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed according to Article 4(12). A key difference is that the GDPR requires notification of personal-data breaches to the supervisory authority unless the breach is unlikely to result in a risk to individuals' rights and freedoms, whereas under NIS2 an incident must meet specified markers of 'significance' to trigger notification. Conflicts may arise when a single incident must be reported to two authorities under different frameworks, each prescribing distinct formats, content, and timelines (Ferrari, 2023). The overlap between NIS2 'significant incidents' and GDPR 'personal-data breaches' may not be self-evident: all data breaches are information-security incidents, but not all information-security incidents are data breaches. The interaction of legislative instruments is undergoing progressive tightening as ransomware incidents increasingly involve both the encryption of data and the exfiltration with subsequent disclosure of such data where demands remain unsatisfied (Kioskli et al., 2025). A challenge for entities lie in the need to inform data subjects in a timely manner yet avoid disclosing exploitable security information, whilst remaining within the required reporting timelines (Ferrari, 2023).

Under GDPR Article 83, less serious infringements may attract administrative fines of up to €10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover for the preceding financial year, whichever is higher. For more serious infringements, the maxima rise to €20 million or 4% of the total worldwide annual turnover for the preceding financial year, whichever is higher. Where an incident results in a GDPR infringement and the DPA imposes an administrative fine, the NIS2 competent authority is precluded from imposing a further monetary fine for the same misconduct (Singh, 2023). This arrangement is presumably set up as the GDPR authorises fines exceeding those foreseen under NIS2. Yet, competent authorities may install other non-financial penalties under NIS2, such as publishing details of the incident.

Sub conclusion

In short, NIS2 extends its predecessor by broadening scope, sharpening governance duties, and imposing proportionate, risk-based obligations on EIEs. The regulatory core is consistent: demonstrable risk management, timely incident handling, exercised resilience, and proportionate supply-chain assurance. Management bears explicit accountability for oversight and resourcing, and should anticipate both direct and indirect costs spanning capability uplift, assurance, and third-party due diligence. Also, insight in the interplay between adjacent regimes (CER, CRA, GDPR, DORA) is essential to minimise duplication and to maintain consistent controls, evidence, and reporting.

Organisations often struggle to translate legal requirements, compounded by unclear regulatory and supply-chain expectations, into a sequenced set of practical actions under resource constraints. This underscores the need for an established, field-recognised framework that translates best practice into actionable controls, fulfils legal obligations, and enables harmonised resilience across the supply chain. To address these expectations credibly, organisations ought to adopt a widely recognised governance and control framework that operationalises best practice, ensures auditability, and accommodates multiple compliance objectives.

Operationalising cybersecurity resilience with built-in NIS2 assurance

As digital transformation generates new strategic risks, regulatory frameworks that extend beyond purely technological controls, e.g., NIS2, are increasingly necessary. These risks must be addressed through approaches that integrate organisational, governance, process and human factors. Given SMEs' reliance on vendors and managed service providers, supply-chain risk and resilience must be prioritised. This entails: robust risk management, mapping critical dependencies; setting proportionate security expectations; verifying supplier performance; and planning for disruption and recovery. NIS2 places strong emphasis on the promotion of standards by Member States, encouraging their widespread adoption to support harmonised security practices (Van 't Schip, 2024). To close the implementation gap, organisations should embed assurance that meets the expectations of competent authorities and supply-chain partners. Demonstrable NIS2 readiness, underpinned by structured assurance, is most effectively supported by adopting a recognised framework that translates best practice into operational controls; ISO/IEC 27001 is a prominent example of such an integrated framework. The following chapter sets out a pragmatic, framework-led pathway that delivers measurable reductions in risk and improvements in resilience without unnecessary complexity.

Besides sector specific information security frameworks, ISO/IEC 27001 is the most widely (internationally) recognised, independently certifiable standard.

It mandates a risk based information security management system (ISMS) and, centred on information security, it promotes organisation wide adoption that extends beyond IT operations to safeguard processes and assets across the enterprise. Rehbohm and Moses (2023) argue that an ISMS is vital to implementing NIS2, noting benefits in enhanced security and faster response to incidents and emerging threats. ISO/IEC 27001 emphasises achieving organisational objectives while managing risk to acceptable levels through the selection and operation of controls. ISO/IEC 27001 offers a rigorous, structured approach to designing and operating an ISMS (Parlov et al., 2025). The Deming cycle (PDCA) underpins continual improvement and sits at the core of standards such as ISO/IEC 27001 (Parlov et al., 2025). In practice, this entails: Plan (securing leadership commitment and setting plans to achieve ISMS objectives); Do (operationalising the selected controls); Check (monitoring and evaluating control performance to determine effectiveness and goal attainment while identifying improvement opportunities); and Act (implementing improvements and corrective actions). The cycle then recommences, driving continuous improvement. Moreover, core ISMS requirements include providing aggregated results to the appropriate management levels, thereby ensuring that management satisfies its legal duty to be appropriately informed (Rehbohm & Moses, 2023).

A companioning best practice, ISO/IEC 27002, sets out a comprehensive catalogue of organisational, people, physical and technical controls that can be operationalised to mitigate risks, including supply chain and business continuity risks.

Utilising a common standard across the supply chain delivers multiple benefits. In heterogeneous regulatory environments, parties can anchor their programmes in an ISO framework, enabling harmonised security, a shared control taxonomy and consistent assurance. Besides this, "aligning legislative and ISO requirements can reduce duplication" (Mentzelou et al., 2025, p. 8). Building resilience necessitate investment, which is most efficiently directed through standardisation, specifically the adoption of recognised standards (Van 't Schip, 2024). A shared standard harmonises security across diverse regulatory supply chains, creating a common control language and portable assurance. Well-designed, resilient and collaborative supply chains can serve as a strategic asset for the organisation (Parlov et al., 2025).

From a resilience perspective, ISO/IEC 27001 integrates incident preparedness, response, and recovery with business continuity disciplines, ensuring that detection, escalation, communication, and post-incident learning are governed and tested. Supply-chain exposure is addressed through structured supplier risk management: defining security expectations, due diligence, performance verification, and contingency planning. Thus aligning third-party oversight with NIS2's emphasis on dependency risk and cascading impact. The standard's emphasis on metrics, internal audit, and management review ensures that resilience and supplier assurance are evidenced, evaluated, and improved over time.

Audit and certification should be favoured.Independent certification functions as a credible assurance vehicle for regulators, customers, and partners, materially reducing duplicated evidence requests, on site audits, and bespoke questionnaires.

For EIEs and their vendors, this can lower total compliance costs over time while improving the quality and comparability of assurance artefacts. Where supply chain partners are micro organisations for whom ISO/IEC 27001 is disproportionate, a context appropriate, scaled certification can provide a lighter weight assurance mechanism. For example, the "NIS2 Supply Chain" certification offers three tiers of complexity, calibrated to the risk profile of the organisation concerned. The provision of a certificate may also enables more efficient contractual onboarding and monitoring by providing a recognised baseline against which additional, risk specific requirements can be layered without recreating foundational controls.

Limitations

As with any standardisation effort, deploying ISO/IEC 27001 to meet regulatory and supply-chain needs has limitations. NIS2 contains specific obligations that are not encompassed by ISO/IEC 27001. Nevertheless, the ISMS requires management to determine applicable legal, regulatory and contractual requirements and to treat the resulting risks through appropriate mitigating measures. While ISO/IEC 27001 offers a structured, guided approach, the primary challenge lies in operationalising it in everyday practice instead of defaulting to documentation over practice. Under ISO/IEC 27001, organisations may define the scope of the ISMS, including justified boundaries and exclusions. By contrast, NIS2 prescribes the scope EIEs, leaving no latitude for self-defined exclusions. Furthermore, standardised methodologies commonly address a delineated set of risks and accompanying measures; yet they often lack the impetus to examine interdependencies within the wider supply chain, which is requisite for achieving genuine resilience for most companies today.

Sub conclusion

Deploying ISO/IEC 27001 provides a coherent, risk-based mechanism to satisfy NIS2's regulatory expectations while strengthening assurance across complex supply chains. By structuring governance, risk assessment, control selection, incident management, and continual improvement within a single management system, ISO/IEC 27001 operationalises the obligations placed on EIEs in a manner that is both auditable and proportionate. Crucially, it embeds demonstrable accountability for leadership, establishes repeatable processes for threat-informed decision-making, and links policy intent to verifiable operational controls.

While ISO/IEC 27001 is not a substitute for detailed, sector-specific obligations, its disciplined architecture minimises fragmentation across adjacent regimes and supports coherent control mapping, thereby streamlining compliance portfolios. Implemented with proportionality and supported by certification, ISO/IEC 27001 offers EIEs and their suppliers a pragmatic, defensible path to meet NIS2 expectations, demonstrate due care, and deliver sustained improvements in risk reduction and operational resilience.



Conclusion

The introduction of NIS2 presents a set of practical challenges for organisations; particularly SMEs. Many organisations lack a clear understanding of what the Directive expects in concrete terms; they face constrained budgets and limited capacity; they must contend with technical and organisational complexity; they operate amid a shortage of qualified professionals; and they navigate an uneven, still-maturing regulatory landscape with limited, and sometimes delayed, guidance from competent authorities. In this environment, SME owners are left wondering where to begin. Parsing legal text seldom yields the operational clarity needed to prioritise investments, assign ownership, or identifying tangible activities. Instead, it can amplify uncertainty about scope, sufficiency and evidencing.

Before implementation, and certainly before asserting compliance, the requirements of NIS2 must be properly understood. The most salient notions sit with management obligations and the prospect of personal liability for misconduct, which together elevate accountability from the outset and anchor cybersecurity as a leadership concern rather than a purely technical one.

Risk management is the red thread: it determines proportionality and informs the depth and pace of implementation relative to each organisation's context.

Incident management and resilience form the backbone of the Directive's ultimate aim: sustained continuity of essential functions and the capacity to recover swiftly when disruption occurs. Owing to pervasive digitalisation, third party and supply chain management demand particular care: risks and vulnerabilities cascade over chains of vendors and service providers and can proliferate systemically if left unaddressed. Moreover, NIS2 does not exist in a vacuum. Organisations must consider how it sits alongside adjacent EU instruments, noting both distinctions and points of harmony with frameworks such as CER, CRA, DORA and, perhaps most prominently, GDPR. Across these regimes there are recurring themes: governance expectations, incident reporting obligations and sanctions, yet their scope, object of regulation and evidencing requirements are not identical. In short, organisations require a framework that both guides the journey through NIS2 and supports compliance and assurance across this broader legislative environment.

In practice, many SMEs will look to ISO/IEC 27001 as a widely recognised, risk based standard to operationalise NIS2's requirements. Its logic of proportionality and scalability aligns with SME realities: the ISMS can be calibrated to organisational context; controls can be selected and deepened according to risk; and continuous improvement (through the PDCA cycle) reinforces resilience over time. Just as importantly, the existence of an independently certifiable scheme provides a credible path to assurance: supporting internal confidence, facilitating dialogue with customers and partners, and easing the evidencing burden across multiple regimes by aligning frameworks and audit trails. Used well, ISO/IEC 27001 can serve as the organising backbone for policy, risk assessment, control operation, measurement and improvement, while ISO/IEC 27002 provides a practical control catalogue spanning organisational, people, physical and technical domains, including areas salient to NIS2 such as supplier oversight and continuity.

Nevertheless, limitations should be acknowledged. ISO/IEC 27001 does not, by itself, prescribe every NIS2-specific expectation. E. g., the precise composition and timing of incident notifications, certain governance prescriptions, or the fixed coverage implied where EIEs are in scope. Nor does any single standard fully capture the interdependencies and systemic exposures that can arise across extended supply chains; supplementary procedures, mappings and sector-appropriate playbooks are often required. Even so, these limits are surmountable when ISO/IEC 27001 is used as a foundation and complemented with NIS2-aligned processes (for incident reporting, supplier assurance and management oversight) and, where relevant, with targeted alignments to adjacent legislation.

In sum, the path from uncertainty to demonstrable readiness lies in translating NIS2's intent into a coherent, proportionate programme that SMEs can execute under real world constraints. By grounding efforts in a recognised, risk based framework, treating resilience and incident response as core capabilities rather than secondary tasks, and managing supply chain exposures with the same discipline applied to internal systems, organisations can progress towards predictable compliance and, more importantly, durable resilience.



References

AFM. (2022). DORA notifications. Retrieved March 2, 2026, from https://www.afm.nl/en/sector/themas/belangrijke-europese-wet--en-regelgeving/dora/dora-meldingen

Boddy, S. E. (2024). Case study: The decision-support framework and NIS2, CER, and DORA incident reporting obligations.

Boggini, C. (2024). Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework. Computer Law & Security Review, 53, 105987. https://doi.org/10.1016/j.clsr.2024.105987

D'Ormesson, P., Péligry, S., Metelka, J., Ščerba, T., Rintala, S., Günther, P., Díaz-Jares Amorós, R., Berger, P. E., Rosiglioni Joris Latui, S., Bardelli, E., Ferrari, A., Herkströter, C., Kimmich, S., Brunner-Reumann, U., Vellenzer, C., Hopman, P., Van Weenen, R., Raath, L., Jessup, C., . . . Ossack, D. (2025, November 5). DORA Penalty Regimes: Overview of Divergence Among Member States. DLA Piper. Retrieved March 4, 2026, from https://www.dlapiper.com/en/insights/publications/2025/10/divergence-in-administrative-penalties-under-dora

De Valk, G. (2022). Analytic black holes. National Security and the Future, 23(1), 21–48. https://doi.org/10.37458/nstf.23.1.1

Directive (EU) 2016/1148. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS). https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng

Directive (EU) 2022/2557. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER). https://eur-lex.europa.eu/eli/dir/2022/2557

Directive (EU) 2022/2555. 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 (NIS2). https://eur-lex.europa.eu/eli/dir/2022/2555

Ferguson, D. D. S. (2023). The outcome efficacy of the entity risk management requirements of the NIS 2 Directive. International Cybersecurity Law Review, 4(4), 371–386. https://doi.org/10.1365/s43439-023-00097-8

Ferrari, L. B. (2023). The relationship between the mandatory reporting obligations of NIS2 and GDPR in light of premature public disclosure [Master Thesis, Tilburg University]. https://arno.uvt.nl/show.cgi?fid=163379

International Organization for Standardization. (2022). ISO 31073:2022: Risk management — Vocabulary. In International Organization for Standardization (ISO 31073:2022). https://www.iso.org/standard/79637.html

Jara, A. J., Martinez, I. C., & Sanchez, J. S. (2024, May). CyberSecurity Resilience Act (CRA) in practice for IoT devices: Getting ready for the NIS2. In 2024 IEEE Smart Cities Futures Summit (SCFC) (pp. 56-60). IEEE.

Joswig, T., & Kurz, W. (2025). Empirical Analysis of NIS2 Adoption in EU SMEs: Challenges for Critical Infrastructure in Germany. Journal of Next-Generation Research 5.0.

Kioskli, K., Maglaras, L., Fotis, T., & Varouchas, E. (2025). Human factors and Strategic Approaches in Cybersecurity: Threats for Critical infrastructures in NIS2 domains. AHFE International, 168. https://doi.org/10.54941/ahfe1006136

Mentzelou, K., Chountalas, P. T., Kitsios, F. C., Magoutas, A. I., & Dasaklis, T. K. (2025). Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. Journal Of Cybersecurity And Privacy, 5(4), 97. https://doi.org/10.3390/jcp5040097

Parlov, N., Akrap, G., & Esterhajer, J. (2025). Supply Chain Security and AI Risk Governance Model for Critical Infrastructure under NIS2, CER, and CRA. Applied Cybersecurity & Internet Governance. https://doi.org/10.60097/acig/211823

Regulation (EU) 2024/2847. 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 (CRA). https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

Regulation (EU) 2022/2554. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554

Rehbohm, T., & Moses, F. (2023). Federal Cybersecurity Architecture and Information Security Management - Adoption and diffusion of the NIS-2 requirements. Gesellschaft Für Informatik (GI). https://doi.org/10.18420/rvi2023-006

Ruohonen, J. (2024, 11 december). A Systematic Literature Review on the NIS2 Directive. arXiv.org. https://arxiv.org/abs/2412.08084

Singh, C. (2023). The european approach to cybersecurity in 2023: A review of the changes brought in by the network and information security 2 (nis2) directive 2022/2555. International Company and Commercial Law Review, 5, 251-261.

Teichmann, F. (2025). Cybersecurity risks in mining's operational technology: Implications of OT vulnerabilities and EU NIS2 compliance. The Extractive Industries and Society, 25, 101774. https://doi.org/10.1016/j.exis.2025.101774

Van 't Schip, M. (2024). The regulation of supply chain cybersecurity in the nis2 directive in the context of the internet of things. European Journal of Law and Technology, 15(1).

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, 52, 105890.

Weber, K. (2025, September 18). EU Cyber Resilience Update: NIS2, CRA, and DORA | CSA. Cloud Security Alliance. Retrieved March 2, 2026, from https://cloudsecurityalliance.org/blog/2025/09/18/an-update-on-european-compliance-nis2-cra-dora

Dignitas Group

Dignitas gelooft in de kracht van verbinding en waardering.

+31 30 209 9980

www.dignitas.nl

info@dignitas.nl

Groenekanseweg 70
3732 AG De Bilt