WHITEPAPER

Your ultimate guide to NIS2 compliance

SAI360
RISK FROM EVERY ANGLE

Contents

Executive Summary

The European Commission (EC) is leading initiatives to accelerate the adoption of “advanced technologies”—artificial intelligence, robotics, blockchain technologies, and the like—to further encourage the fusion of physical and digital systems across the collaborative economy. But while increased digitization and interconnectedness open doors for more innovative business models, new processes, and perhaps entirely new industries, it escalates risk for firms. This expansion increases cybersecurity vulnerabilities and heightens the potential for operational disruptions resulting from system failures or data breaches. In the final two months of 2023 alone, there were 178 publicly disclosed security incidents within the European Union (EU), exposing ~150 million records.[1]

The EC recognizes the importance of bolstering the security posture of the Union in tandem. In 2020, the Commission proposed the Network and Information Systems Directive 2022 (NIS2), rectifying long standing criticisms of its predecessor—NIS1—and laying the foundation for a high common level of cybersecurity across the EU.

This whitepaper explores the new requirements in-depth, evaluating the changes compared to NIS1 and highlighting how you can prepare for its transposition across EU Member States.

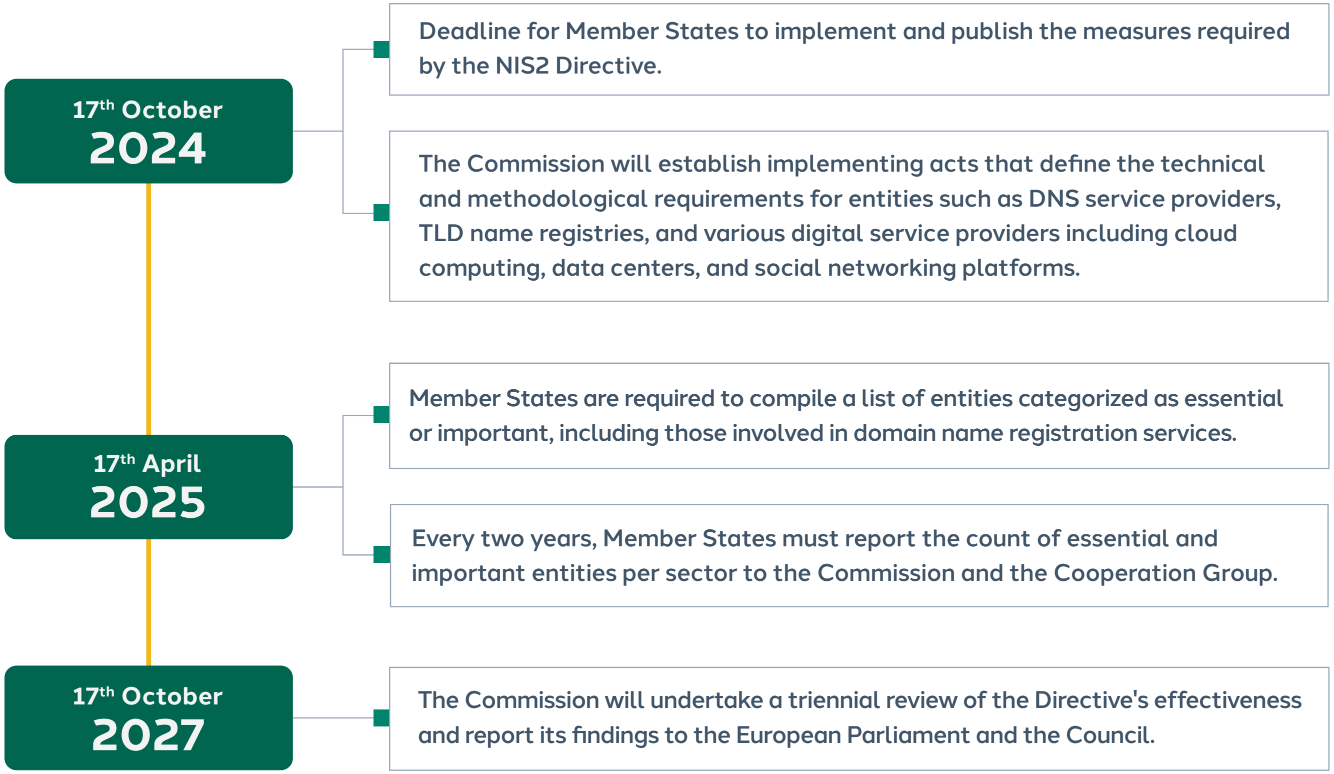
[1] https://www.itgovernance.co.uk/

Scope

The NIS2 Directive expands the scope compared to NIS1 to include a broader range of sectors categorized as either “essential” or “important”. It applies to both public and private large and medium-sized organizations, generally defined as having more than 50 employees and an annual turnover exceeding 10 million euros, with specific inclusions for various IT services providers like online marketplaces, search engines, and cloud computing services, regardless of size. Importantly, the directive also extends to non-EU companies that operate within the EU, ensuring it covers entities outside traditional geographical limitations

Essential Sectors	Important Sectors
Transport	Food
Banking	Postal and Courier Services
Financial Markets	Chemicals
Health	Research Businesses
Drinking Water	Digital Providers
Waste Water	Manufacturing
Digital Infrastructure	
ICT Service Management	
Public Administration	
Space	

.Implementation timeline



17th October 2024

Deadline for Member States to implement and publish the measures required by the NIS2 Directive.

The Commission will establish implementing acts that define the technical and methodological requirements for entities such as DNS service providers, TLD name registries, and various digital service providers including cloud computing, data centers, and social networking platforms.

17th April 2025

Member States are required to compile a list of entities categorized as essential or important, including those involved in domain name registration services.

Every two years, Member States must report the count of essential and important entities per sector to the Commission and the Cooperation Group.

17th October 2027

The Commission will undertake a triennial review of the Directive's effectiveness and report its findings to the European Parliament and the Council.

1. More Sectors Affected

NIS2 covers **15 sectors**, compared to the 7 covered in NIS1

2. Stricter Requirements

NIS2 broadens the requirements to an “all-hazards” approach

3. Enforcements

Heavy fines coupled with extensive non-financial repercurssions present financial and reputational risks.

Key changes compared to NIS1

Senior manager accountability

"Tone from the top" is a term that has been reverberating around the risk and compliance community in recent years after a number of high-profile governance failures. The phrase itself suggests that a firm's board of directors and senior management should embody and not merely dictate compliance and ethical standards. NIS1 was often criticized for being poorly enforced, partly due to a lack of personal liability, an issue directly addressed in the new Directive.

NIS2 places individual accountability at the forefront of impending requirements, declaring it the responsibility of senior management to approve their firm's cybersecurity risk management measures and oversee their implementation. It follows, therefore, that if any infringements ensue, they can be held liable.

Similarly, management bodies of essential and important entities will be required to follow necessary training, and the employees of these organizations will be encouraged to do so too, on a regular basis. This people-first approach recognizes the importance of upskilling the labor force in line with procedural improvements to ensure they gain sufficient knowledge and skill to identify risks and assess broader risk management practices. Without the necessary foundational knowledge of risk, subsequent mitigation measures will likely fail to meet the demands of the modern world.

Cybersecurity risk management framework

NIS2 requires firms to adopt technical, operational, and organizational measures to prevent or minimize the impact of incidents on recipients of their services. Measures must be "appropriate and proportionate" to the risks posed, and this proportionality is to be determined by considering various aspects such as the size of the entity, the likelihood of incident occurrence, and the potential societal and economic impacts.

The probability of preempting a specific hazard impacting your business is difficult, and that's why it's important to consider as many threats and risks as possible. This "all-hazards" approach is reflected in NIS2 and represents a broadening of the risk landscape compared to NIS1. In-scope firms must implement measures designed to address a full range of risks. It's also important to recognize the possibility for a single incident to cascade into multiple. For example, if critical services are delivered either wholly or in part through a third party.

NIS2 lists 10 main areas of information security for which essential and important entities need to have procedures for:

- Policies on risk management and information security: Your approach to understanding and mitigating cybersecurity threats through risk assessments and documented procedures
- Incident handling: Processes to address security incidents, involving rapid detection, evaluation, and efficient communication
- Business continuity: Strategies such as backup management and disaster recovery, and crisis management
- Supply chain continuity: Maintaining secure supply chains through careful vetting of third-party security measures, including aspects concerning the relationships between each entity and its direct suppliers or service providers (fourth parties)
- Secure system acquisition: Processes for securing systems and infrastructure throughout their lifecycle, including vulnerability handling and disclosure
- Assessing the effectiveness of cybersecurity risk-management measures: Including audits and technical testing
- Cyber hygiene practices and cybersecurity training: Implementation of cyber hygiene across the organization, emphasizing secure device use, password management, and anti-phishing practices, complemented by regular staff training
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption to block unauthorized access, including effective management of encryption keys
- Human resources security: Esuring all personnel are aware of and adhere to security responsibilities through stringent recruitment checks, security-focused culture, and access control policies
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

Incident reporting

The NIS2 Directive explicitly describes how firms are to report significant incidents to computer security incident response teams (CSIRTs). Overall, the stricter requirements mean entities must have processes in place for prompt reporting of security incidents with significant impact on their service provision or recipients.

When an incident occurs:

As soon as an incident occurs, firms must determine its criticality by evaluating criteria such as the impact on sensitive data, scope, and scale.

According to supporting Guidelines released by the Commission,[2] severity assessments should consider:

- ***The affected network and information systems. In particular, their importance in the provision of the entity's services.***
- ***The severity and technical characteristics of a cyber threat***
- ***Any underlying vulnerabilities that are being exploited***
- ***The entity's experience with similar incidents***
- ***Indicators such as the extent to which the functioning of the service is affected***
- ***The duration of an incident***
- ***The number of affected recipients of services***

The added emphasis on vendor risk means it's important to have mapped third and fourth parties to critical services to determine the severity of a vendor disruption on different parts of the value chain. As per NIS2, an incident is deemed to be significant if it:

a) has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned, or;

b) has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Within 24 hours of the incident:

Without undue delay, and "in any event within 24 hours" of becoming aware of the significant incident, firms are required to share initial data with CSIRTs and recipients of the disrupted, or potentially disrupted, service:

a) Is the incident suspected of being caused by unlawful or malicious acts?

b) Is it possible the incident will have cross-border implications?

> *In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure their single points of contact are provided in due time with relevant information.*

Within three days of the incident:

Without undue delay and "in any event within 72 hours" of becoming aware of the incident, firms must submit a fuller incident notification to the aforementioned recipients including;

a) any changes to the information reported during the first notification

b) an initial assessment of the significant incident, including severity and, where possible, the indicators of compromise

Finally, and no later than one month after the submission of the second notification, essential and important entities must submit the following;

a) a detailed description of the incident, including its severity and impact

b) the type of threat or root cause that is likely to have triggered the incident

c) the applied and ongoing mitigation measures employed by the firm

d) where applicable, the cross-border impact of the incident

> *It's the responsibility of the CSIRT to be prompt with feedback (within 24 hours of receiving the early warning), guidance and operational advice.*

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023XC0918(01)

Registry of entities

A portion of in-scope entities, such as providers of cloud computing, data center services, content delivery networks, managed services, online marketplaces, search engines, and social networking platforms, will have to supply certain information to competent authorities to enable the European Union Agency for Cybersecurity (ENISA) to keep an up-to-date registry of firms.

Maintaining this registry is crucial for ENISA because it ensures transparency and oversight in the cybersecurity landscape. By having a centralized database of service providers, ENISA can monitor compliance, assess risks more effectively, and coordinate better security measures across the EU. This contributes to a more secure digital environment, benefiting both providers and users by enhancing trust and safety in online services.

Supervision and enforcement

Ultimately, it’s the responsibility of Member States to determine the imposition of “appropriate, proportionate and effective” supervisory and enforcement measures to ensure regulatory adherence. However, the Directive is comprehensive in its prescription of tools and mechanisms through which supervisors can evaluate and penalize non-compliance.

Nowhere to hide - assessing compliance

NIS2 outlines the following tools at supervisors’ disposal to assess compliance for important and essential entities:

- **On-site inspections and off-site supervision:** Including random checks conducted by trained professionals
- **Regular and targeted security audits:** These are to be carried out by an independent body or competent authority, the costs of such an audit are to be paid by the audited entity (unless supervisors decide otherwise)
- **Security scans:** Based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned
- **Information requests:** Including documented cybersecurity policies, as well as data, documents, and any other information necessary to carry out their supervisory tasks
- **Requests for evidence:** For implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence

In addition to the above, essential entities can also be subject to ad hoc audits, including where justified on the ground of a significant incident or an infringement of the Directive.

Enforcement powers

The proposed enforcement measures under NIS2 introduce significant financial, operational, and reputational consequences for non-compliance that could cause an immediate and long-lasting impact on firms.

Administrative fines

For essential entities, infringements of Article 20 (risk management framework) or 21 (incident reporting) could result in a fine of up to €10,000,000 or 2% of the total worldwide annual turnover in the preceding financial year, whichever is higher.

For important entities, infringement of Articles 20 or 21 can result in a fine of up to €7,000,000 or 1.4% of the total worldwide annual turnover in the preceding financial year, whichever is higher.

Loss of business

Competent authorities can order firms to cease the conduct that infringes the directive and never repeat it. This represents a significant threat to firms, potentially leading to immediate and severe disruptions to services and revenue streams.

Hidden costs

Competent authorities can issue binding instructions, such as asking firms to implement necessary measures to prevent or remedy an incident, or to remedy any deficiencies identified during supervision. These can be applied alongside strict time limits for their implementation as well as subsequent reporting detailing their efficacy.

Reputational risk

Competent authorities can mandate those entities:

a) Notify individuals and organizations about significant cyber threats to their services, including advice on protective and remedial actions

b) Publicly disclose details of their regulatory infringements

These enforcement actions under NIS2 requiring entities to disclose significant cyber threats or publicize their compliance infringements carry considerable reputational risks. Firstly, having to inform customers or clients about potential cyber threats can erode trust, as stakeholders may perceive the entity as insecure or unreliable, fearing that their sensitive data could be at risk. Secondly, mandatory public disclosures of infringements highlights the entity's failure to meet regulatory standards and attracts negative media attention and public scrutiny. These actions can damage a firm's reputation, deter potential clients, and negatively impact partnerships and investor relations, ultimately leading to a potential decline in market value. Such transparency, while crucial for public safety and trust, underscores the imperative for robust cybersecurity measures and compliance management to mitigate these risks.

NOTE: Enforcements are issued on a case-by-case basis, depending on a host of factors such as intent or negligence, duration of the incident, or the presentation of false or inaccurate information pertaining to the incumbent risk program. Importantly, firms can reduce the regulatory sanctions **if they are able to demonstrate measures taken to prevent or mitigate the incident.**

Preparing for NIS2

Focus on an integrated approach

NIS2's inclusion of business continuity management (BCM) and third-party risk management (TPRM) demands a more strategic and thorough approach to IT-GRC which extends beyond the traditional bounds of cybersecurity. To think holistically about cybersecurity risk, firms must strive for a more integrated IT-GRC framework, one which consolidates and coordinates disparate IT risk management activities (technology risk, operational risk, IT vendor risk and so on) across the entire organization.

IT-GRC enhances the firm's performance and resilience and embeds a proactive risk-aware culture which significantly outweighs the old compliance-driven frameworks. By integrating risk management into all aspects of business operations, IT-GRC helps organizations improve data quality, ensure disaster preparedness, reduce costs, and maximize operational efficiencies. With a well-defined strategy, thorough assessment, clear communication, and the right technology, IT-GRC equips organizations to not only manage but also capitalize on risks, turning potential vulnerabilities into strategic advantages.

Example

While having multiple specialized solutions across different points of the value chain is beneficial, without a cohesive, integrated view of your risk posture, managing these disparate systems can become disjointed and inefficient.

Different systems often use varying technologies, data formats, and protocols. For instance, an information security management tool might detect a breach using advanced analytics and machine learning, storing data in a certain format, while the incident response tool might use a different format or database structure.

This heterogeneity can make it challenging to automate data sharing and synchronization between systems, leading to delays or errors in data transfer. NIS2 demands an immediate and coordinated response to incidents which includes not only IT staff but also legal, communications, and executive teams to manage the situation. A segregated approach may expose the organization to unnecessary financial, compliance and reputational risk.

Review policies and internal controls

As firms improve their cybersecurity, BCM and TPRM capabilities, the complexity of their operations typically increases. This is largely due to the growing number of systems, processes and external partnerships that must be managed to effectively mitigate risks. As risk management efforts scale, associated policies and internal controls become increasingly valuable:

Structured application of strategies

Policies and controls offer a structured and integrated framework that guides the consistent application of risk management strategies across all organizational levels. It standardizes responses and actions related to risk, which is crucial for maintaining an orderly and predictable management environment amid increasing operational complexities.

Scalable risk management efforts

These elements allow the business to scale its risk management efforts, so as the firm grows, compliance with NIS2 and adjacent regulations can be maintained without proportional increase in risk or management overhead. The infrastructure of policies and controls serves as a blueprint, guiding the organization through growth phases while maintaining tight control over new and emerging risks.

Foster a risk-aware culture

NIS2 places just as much emphasis on senior management accountability and employee competence as it does associate controls and tooling. This dual focus recognizes that while technology and processes are essential for identifying and managing risks, the effectiveness of these solutions hinges on the people who operate them. Employees at every level must be capable of executing risk-related processes and reacting appropriately to the outcomes. By ensuring leadership and staff are well-versed in their responsibilities and competent in their roles, an organization can enhance its overall risk management effectiveness.

SAI360 - an opportunity for holistic IT-GRC

SAI360 can unify disparate elements of an organization's IT-GRC framework into one cohesive platform. This integration is crucial for organizations wrestling with patchwork tech stacks composed of point solutions layered over legacy technology. SAI360 offers a single source of truth, providing senior management with a clear view of all risk factors and compliance statuses. This capability streamlines IT-GRC and improves the reliability of audit trails in tandem.

Unique to SAI360, and particularly beneficial for NIS2 compliance, is the integration of IT security awareness training directly within the GRC management platform. This innovative approach ensures any updates to IT-GRC procedures are immediately reflected in training modules. Additionally, the platform allows for tracking of employee attestations, enabling organizations to assess the effectiveness of the training and directly correlate it with broader risk management metrics.

In essence, SAI360 provides a comprehensive solution that consolidates risk data and integrates cybersecurity awareness into the daily operations of a firm, thereby bridging the gap between strategic IT-GRC management and operational execution.

Regulatory overlap

While the NIS2 requirements are extensive, they should not be considered in isolation. The new rules form part of a broader strategy to mitigate operational and cyber risk across the EU, so understanding the interplay between NIS2 and other standards, directives, and regulations such as ISO standards, GDPR, sector-specific rules like DORA, and even upcoming laws like the Cyber Resilience Act is crucial. Efficient preparation involves identifying overlaps and conflicting obligations among these frameworks to effectively meet multiple requirements and standards within a unified approach.

ISO certification

A growing emphasis on cybersecurity has prompted many large and medium-sized firms to voluntarily bolster their cybersecurity frameworks through securing ISO certifications. ISO 27001, for example, establishes a strong foundation for information security and demonstrates a firm's commitment to cybersecurity more broadly. However, this certification only covers certain aspects of NIS2, and within the framework itself there are deviations in controls which do not leave all ISO-certified firms on an equal footing. For example, ISO 27002, while not a certifiable standard by itself, names specific controls related to information security, physical security and privacy management (e.g. Access controls, restrictions and cryptography). Some of these specific processes are optional for ISO 27001 but become mandatory under NIS2.

Additionally, ISO 22301 and ISO 27036 extend the coverage of ISO 27001 into specific areas like BCM and TPRM, respectively. ISO 22301 assists in establishing comprehensive BCM strategies, enhancing a firm's resilience and aligning with some of NIS2's broader goals. ISO 27036 provides structured approaches to managing third-party risks, addressing areas that ISO 27001 does not explicitly cover. Understanding the scope and limitations of these ISO standards in relation to NIS2's demands allows firms to not only leverage their existing ISO frameworks effectively but will also help them to understand the specific framework components requiring augmentation.

GDPR reporting

The incident reporting obligations under NIS2 and GDPR pose complex and often conflicting compliance challenges for firms, especially given their different focuses and timelines. GDPR mandates that organizations report personal data breaches within 72 hours, whereas NIS2 requires reporting of broader security incidents that impact business continuity within 24 hours, potentially complicating incident prioritization and resource allocation. Moreover, while GDPR specifically targets personal data breaches, NIS2 covers a wider range of security incidents, necessitating a dual assessment approach for incidents that may impact personal data and business operations.

Although NIS2 operates "without prejudice" to GDPR (Article 2(12)), it does not supersede GDPR obligations. Firms must navigate both sets of regulations, which can result in overlapping reports to different regulatory bodies—each with its own specific focus and requirements.

Considerations for the financial services sector

Article 1(2) of DORA provides that, in relation to financial entities covered by NIS2 and its corresponding national transposition rules, DORA constitutes "Lex specialis"[3] i.e. takes precedence.

Consequently, the provisions of DORA relating to ICT risk management, digital operational resilience testing, information sharing, and ICT third-party risk apply instead of those provided for in NIS2. Member States should therefore not apply the provisions of NIS2 on cybersecurity risk-management and reporting obligations, and supervision and enforcement, to financial entities covered by DORA.

An integrated risk management tool is essential for organizations to achieve a holistic security framework under NIS2 and maintain compliance with overlapping standards, GDPR, DORA, and various ISO norms. Such tools facilitate the consolidation and management of various regulatory requirements, ensuring that firms can efficiently prioritize actions and allocate resources. They provide clear visibility into where standards intersect or diverge, helping to identify conflicting obligations and synergize compliance efforts.

By offering an integrated approach, SAI360 enables organizations to leverage a single framework to address multiple requirements simultaneously.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023XC0918(01)

FINAL THOUGHTS

NIS2 intensifies the challenges for organizations operating fragmented technology stacks, with requirements demanding quick, decisive action and comprehensive visibility into compliance and risk, the ability to consolidate and view risks through a singular lens becomes indispensable.

Proactively adapting to these changes will ensure compliance and position your organization ahead of the curve in cybersecurity readiness. Stay informed, stay agile, and leverage integrated risk management solutions to maintain control in a dynamically evolving regulatory landscape.

Interested in learning more about how SAI360 can support your organization's compliance to NIS2?

Request a Demo.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360
RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle. Visit www.sai360.com.