SHOOSMITHS

NIS2: Commission Implementing Regulation (EU)

14 October 2024

The European Commission published its draft regulation, the "NIS2 Implementing Regulation" ("N2IR"), for consultation on 27 June 2024. N2IR builds on the Network and Information Systems Directive 2022/2555 ("NIS2"), which was adopted on 16 January 2023 and will begin to apply from 18 October 2024 and beyond.

The N2IR lays down the Commission's proposed cybersecurity standards for so-called "digital providers" regulated by NIS2, as well as the criteria against which those providers must notify incidents to their respective regulators under NIS2. Given that the majority of Member States have yet to publish their proposed legislation for implementing NIS2 into their domestic law, N2IR offers insight into how NIS2 may impact regulated businesses and their supply chains as we move into 2025 and beyond.

This note provides an overview of the key aspects of N2IR, its critical differences with other in-force legislation, namely the General Data Protection Regulation ("**GDPR**") and offers insight on how the draft regulation may shape the rollout of NIS2 across EU Member States.

Background

NIS2 replaces the 2016 NIS Directive ("**NIS 1**") and enhances the scope of the EU's cybersecurity compliance framework. Underpinned by a significantly enhanced enforcement regime, which includes fines of up to €10 million or 2% of global turnover (whichever is greater) for non-compliance and the expectation of personal liability for directors and senior officers, NIS2 imposes stricter requirements on organisations and more than doubles the number of sectors falling within the scope of its regulation.

NIS2 primarily targets organisations that provide key services in vital sectors including energy, transport, banking, financial market infrastructures, healthcare, utilities and digital infrastructure. Additionally, it extends to critical suppliers within these sectors, encompassing both direct providers, such as digital service and cloud computing services, as well as indirect suppliers whose services are integral to the digital infrastructure of those critical sectors.

Entities falling within the scope of NIS2 are further differentiated into two categories: 'essential entities' and 'important entities,' determined by their importance to the EU's critical infrastructure. Both categories are subject to the same requirements, but the supervisory mechanisms and enforcement differ markedly.

As a Directive, much of the underlying detail is left for each EU Member State to determine. This includes, inter alia, which sectors/entities are regulated, the cybersecurity controls required, incident reporting, registration requirements, audit and oversight mechanisms, enforcement powers and

sanctions. Member States must adopt their domestic implementation acts by 17 October 2024, with enforcement starting on 18 October 2024.

The net effect of the new NIS2 framework for newly regulated entities (and those currently regulated under NIS 1) is a significantly increased compliance burden, including implementing cyber resilience policies and supply chain risk management, with stringent incident reporting requirements.

The commission implementing regulation

While the mechanics of NIS2 are left for each Member State to determine, having due regard to the guiding principles set out in NIS2, the Commission retained competence for determining both the cybersecurity controls and incident reporting criteria for entities in these sectors due to the ubiquitous nature of digital infrastructure and services. Note: Member States are still responsible for determining how to monitor and enforce those standards in their respective jurisdictions.

On that basis, under the N2IR, the Commission has set out those standards which will apply to these sector entities. It applies to all digital sector providers, namely: DNS (domain name system) service providers, TLD (top level domain) name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, online search engine providers, social networking services platforms and trust service providers.

Significant incident reporting thresholds

One of the significant aspects of NIS2 is the emphasis on breach reporting, which requires affected entities to promptly report any cybersecurity incidents to the relevant authority without undue delay and **no later than 24 hours after the detection of the incident**, with further detailed reporting at subsequent intervals.

Entities are also required to provide specific details about the incident, including the nature of the breach, its potential impact, and the measures taken or proposed to address the situation. This necessitates having appropriate measures to detect and respond to cybersecurity events promptly with sufficient information.

The N2IR has now provided clarity over what exactly constitutes an “incident” for the purpose of such reporting duties (at least for the digital sectors).

General criteria for significant incidents

For all entities within the digital sectors identified above, the Commission is proposing that an incident will qualify as significant for the purposes of NIS2, and therefore carry incident reporting obligations, if it meets one or more of the following criteria:

- **financial impact**: Causes or is capable of causing financial loss exceeding EUR 500,000 or 5% of the entity’s annual turnover, whichever is lower, based on the latest internal draft seen by a news outlet.

- **reputational damage**: Causes or is capable of causing considerable reputational damage to the entity, based on an assessment of media reporting, complaints from users or critical business relationships, potential inability to meet regulatory requirements and potential loss of customers impacting business.
- **trade secrets**: Causes or is capable of causing the exfiltration of trade secrets as defined in relevant EU law.
- **health and safety**: Causes or is capable of causing the death or considerable damage to the health of a natural person.
- **network security**: Involves suspected malicious and unauthorised access to network and information systems.
- **recurring incidents**: Multiple minor incidents, which are not significant individually under Article 3, are treated as a single significant incident if they have occurred at least twice within six months and share the same apparent cause.

Enhanced criteria for significant incidents

The N2IR sets out a number of additional triggers that are specific to certain categories of digital providers:

Cloud computing service providers (article 7)

- complete unavailability of any service for more than 10 minutes.
- failure affecting either more than 5% of EU users or 1 million users for more than an hour.
- compromise of data integrity, confidentiality, or authenticity impacting more than 5% of EU users.

Data centre service providers (article 8)

- Complete unavailability of any data centre service.
- SLA non-compliance for more than one hour or due to suspected malicious action.
- Compromise of data integrity, confidentiality, or authenticity, or compromised physical access.

Managed service providers and managed security service providers (article 10)

- Complete unavailability of any managed service or security service for more than 10 minutes.
- SLA non-compliance affecting more than 5% of EU users or 1 million EU users for more than one hour.
- Compromise of data integrity, confidentiality, or authenticity impacting more than 5% of EU users.

Cybersecurity risk-management measures

The Annex to the N2IR contains cybersecurity risk-management measures for affected entities in the digital sector. The requirements are set out in considerable detail; in summary, key requirements for covered entities in these sectors include:

Security policies

- requirements for security policies, adequate resourcing and defined roles and responsibilities with regular review. Entities must ensure staff and third-party compliance, with at least one person

reporting directly to management on security matters.

Risk management

- *comprehensive risk management system*: Entities must establish and maintain a system including risk assessments, treatment plans, and management approval of residual risks, with regular review and update. Independent reviews must be reported to management bodies.

Incident handling

- *reporting mechanisms*: Entities must have a simple mechanism for reporting suspicious events, communicated to suppliers and customers, and assess events against specified criteria.
- *monitoring and logging*: Robust monitoring and logging, automated where feasible, with a clear reporting mechanism for suspicious events, reinforced through training.
- *incident assessment*: Incidents must be promptly assessed, classified and managed.
- *communication and response*: Effective communication with stakeholders and incident response teams must be established, along with post-incident reviews to enhance future response.

Business continuity

- *business continuity and disaster recovery plans*: These plans must be based on risk assessments, including roles, communication channels, activation criteria, and recovery sequences, with regular testing and updates.

Supply chain security policy

- *supply chain security policies:* Criteria for supplier selection based on cybersecurity practices, product quality and resilience.
- *appropriate cybersecurity provisions in contracts*: Must specify cybersecurity requirements, incident reporting obligations and audit rights.
- *supplier directories*: Establish directories with contact details.
- *regular reviews*: Policies must be regularly reviewed to address changes in cybersecurity practices and significant incidents.

Acquisition and development

- *risk management*: Manage risks associated with acquiring critical ICT services and products, including security requirements, updates, documenting hardware/software, validating compliance and regular review.
- *secure development*: Rules must cover all phases of system development from design to testing.
- *configuration management*: Robust configuration management, change procedures, security testing policies, network protection and vulnerability management with ongoing updates.

Cyber hygiene and training

- *risk management and awareness programs*: Implement programs covering risk management measures, contact points, and cyber hygiene practices, scheduled, tested and updated regularly.

- *security training*: Required for roles needing security expertise, including secure system operation, threat briefings and response training. Effectiveness must be assessed and periodically updated.

Cryptography

- *cryptographic measures*: Company policy should define measures suitable for asset protection, specify protocols, algorithms, and cryptographic solutions, potentially adopting a cryptographic agility approach. Policies must be regularly reviewed and updated to align with cryptographic advancements and organisational needs.

Human resources security

- *cyber hygiene and administrative roles*: Ensure clarity for employees, suppliers and service providers.
- *background checks*: Carry out checks for employees and service providers where required, with regular reviews and updates, along with post-employment requirements and a structured disciplinary process.

Access control

- *authentication measures*: Strict measures, regularly reviewed and updated in response to operational changes or incidents.
- *access rights management:* Managed according to principles such as least privilege and separation of duties, with special controls for privileged and administrative accounts.
- *removable media policy*: Entities must implement this policy.
- *identity management*: Includes limiting shared identities and implementing state-of-the-art authentication procedures and multi-factor authentication appropriate to the asset being protected.

Asset management

- *classification*: Classify all information and assets within their network and information systems according to sensitivity and business value, based on confidentiality, integrity, authenticity and availability requirements. This classification should guide the level of protection needed and align with business and disaster recovery plans, with regular reviews to ensure classifications remain current.
- *policies*: Establish policies for proper information and asset handling, covering acquisition, use, storage, transportation and disposal.

Environmental security

- *network and information systems protection*: Safeguard against utility failures through facility resilience, redundancy in services like electricity and telecommunications and continuous monitoring. Regular testing and maintenance must be carried out to ensure operational continuity. Reduce physical and environmental threats through risk-based measures and monitoring. Use stringent physical access controls with security perimeters and ongoing monitoring to prevent unauthorised access.

Commentary

The N2IR is notable in several ways. Not only does it set out the specific measures required by digital providers, it will also directly apply to those entities from 18 October 2024, regardless of transposition into Member State law and the maturity of their respective enforcement regimes. This effectively sets cybersecurity standards that will be indirectly enforceable, for example, through contract obligations to comply with applicable law.

Incident reporting and comparisons with NIS 1

First, the thresholds under the old NIS 1 regime are both narrower and considerably less detailed than those proposed under the N2IR. NIS 1 outlines factors for assessing the substantial impact of an incident, such as the number of affected users (particularly those relying on the service for their own operations), the incident's duration, the geographical extent of the affected area, the degree of disruption to the service's functionality and the broader impact on economic and societal activities.

In contrast, the N2IR's proposed thresholds are not only broad and detailed but also include enhanced triggers for those digital sectors perceived to be the most critical, namely data centres, cloud service providers and online marketplace providers.

Given the granular nature of the proposed thresholds, regulated entities are likely to need to change their entire approach to incident classification and management, as, in our experience, the majority of businesses do not classify breaches in such a granular format.

Notification requirements and comparisons with the GDPR

Those familiar with the GDPR's notification requirements will be aware that it only covers personal data breaches that are (or are likely to cause) an impact on the rights and freedoms of individuals, and that such a notification must be made within 72 hours.

NIS2, on the other hand, requires regulated entities to notify the competent authority or Computer Security Incident Response Team ("**CSIRT**") within 24 hours of a significant incident, irrespective of whether the data is personal data or not. In this sense, the NIS2 obligation has been described as an "obligation to seek help" rather than an "obligation to report."

NIS2 represents a significant cultural change for the way regulated businesses handle their incident notification requirements, as well as the personnel involved in that process. A regulated entity's information security team may be sufficiently resourced to ensure it can notify incidents within the 24-hour window, but members of the entity's legal, compliance and risk departments may be concerned about any negative connotations associated with such notification and the resulting impacts on their organisation. The presence of significant financial sanctions (including personal liability) only emphasizes these issues.

Shaping the rollout in member states

Simply put, implementing NIS2 into domestic law is a sizeable task for EU Member States, with many currently lacking a sufficiently robust and resourced national cyber strategy to cater for NIS2. However, given that much of the legwork has already been carried out by the Commission under N2IR, it is easy to see copy-cat type provisions appearing as Member States look to grapple with how they implement the equivalent topics into their own domestic legislation and to potentially use the principles under N2IR to apply to all sector entities.

Next steps

Any potentially affected organisation is advised to:

- assess in more detail whether it is likely to be in scope of NIS2, bearing in mind its size, sector, the nature of its business, and the Member States in which it operates or into which it provides services.
- ensure, considering the Crowdstrike outage of 19 July, that it therefore implements a plan to comply.
- review existing incident handling processes, including incident classification, and consider how that process may need to change in light of the Commission's proposals in N2IR, even if not caught by N2IR.
- consider whether key customers or suppliers are likely to be impacted, and how this should be reflected in key contracts.
- stay aware of the timetable for NIS2 implementation into Member State law.
- if affected by NIS2, implement a roadmap NIS2 compliance plan, starting with the audit of current activities and policies, gap analysis, and familiarisation with registration requirements. For an overview of what that roadmap may look like, please see here.

Further insight and analysis on the full range of cyber resiliency advice can be found on our dedicated website pages Resiliency by Shoosmiths.

Disclaimer