NIS2 implementation: key steps for compliance professionals

TRRI news

Published 05-Aug-2024 by Huw Beverley-Smith, Charlotte Perowne and Emily Evans, Faegre Drinker

Compliance deadlines for the Network and Information Systems Directive (EU) 2022/0383 (NIS2) will apply from October 2024, following its entry into force in January 2023. The directive's focus is on addressing cybersecurity threats and combating the rise of cyber attacks in an increasingly digitalised world. It goes further than its predecessor, NIS1, and covers a wider range of entities, such as social media platforms and medical device manufacturing.

The territorial scope of the NIS2 Directive will stretch to many entities based outside of the EU, which may find themselves subject to the minimum requirements of the NIS2 Directive if they provide certain in-scope services. For those entities which fall within the scope of NIS2, compliance will need to be assured by October to avoid the potentially significant penalties. A step-by-step guide setting out key compliance points ahead of this deadline is set out below.

Scope

As a preliminary step, compliance teams should first assess whether their organisation falls within the territorial scope of NIS2. The relevant questions include whether an entity is:

- Providing services or carrying out activities within the EU.
- Qualified as "important" or "essential" in a relevant sector.
- Defined as either medium (employing 50 or more people or with an annual turnover of 10 million euros) or large (employing 250 or more people or with an annual turnover of 50 million euros). Some entities will be in scope regardless of their size due to specific provisions set out in NIS2, including the possibility of later being brought into scope by individual member states.

The relevant sectors covered in Annexes I and II of NIS2 notably include:

- Banking and financial market infrastructures.
- Digital infrastructure (e.g., DNS services, cloud computing services, and data centre services).
- Digital providers (e.g., online marketplaces, search engines and social networking services platforms).
- ICT business-to-business service management (including security).
- Health.
- Energy.
- Manufacturing in key critical sectors, including medical devices, electronics, machinery and transport.
- Manufacturing, production, and distribution of food and chemicals.
- Drinking and wastewater.
- Transport.
- Space.
- Public administration.
- Postal services.
- Waste management.
- Research organisations.

Additionally, entities providing domain name registration services, critical entities categorised as such under the related Resilience of Critical Entities Directive, and certain public administration entities that provide specific services will also be subject to the regulation. Member states can selectively exclude specific critical entities in areas such as national security, defence or law enforcement.

Non-EU established companies can, therefore, fall in scope by virtue of the sector in which they operate and their relative size and strategic importance, where they are providing services in the EU.

If an organisation is in scope, it should consider whether its operations will mean that it is defined as either an "essential" or an "important" entity. While the base-level obligations will remain the same for all entities, classification, size and risk exposure will be factors in determining the steps required to meet these obligations.

Gap analysis

As a first step, compliance teams should undertake a gap analysis to assess conformity with the relevant requirements under NIS2, with appropriate legal input. At this stage, it also makes sense for the business to identify any critical operational services. Compliance teams may also want to assess the extent to which they are able to access cybersecurity-related funding, which can be used to ensure compliance with NIS2.

Cybersecurity risk assessment and management

One of NIS2's main functions is to create more specific cybersecurity risk management obligations for covered entities. An important compliance step is to regularly assess risks related to network and information systems and implement required policies.

Risk assessments should:

- Identify any potential risks and vulnerabilities within the cybersecurity practices of the organisation.
- Consider and document threats which are specific to the individual business.
- Feed into the determination of appropriate technical, operational and organisational measures.

Continuing systems management should include:

- Integrating multi-factor authentication and encryption measures within networks and systems.
- Continuous monitoring of systems to ensure they are not compromised.
- Implementation of plans and procedures to specifically address any risks uncovered during risk assessments.

NIS2 sets out required policies which should be implemented in a manner that is proportional to the potential impact of any incidents, the organisation's risk exposure and relative size. The policies required under NIS2 include:

- Risk analysis, incident response and business continuity.
- Vulnerability handling and disclosure.
- Use cryptography and encryption.
- Cybersecurity training.
- Supply chain security.

Incident reporting and response

Entities covered by NIS2 will be required to meet strict incident reporting requirements, which will include providing to the competent national authority or computer security incident response team (CSIRT):

- An initial report of a significant incident without undue delay and, in any event, within 24 hours.
- A more detailed incident notification without undue delay and, in any event, within 72 hours.
- A final report within one month.

Significant incidents are defined as those which have either:

- Caused, or can cause, severe operational disruption or financial loss for the entity concerned.
- Affected, or can affect, other natural or legal persons by causing considerable material or non-material damage.

To prepare, entities should ensure that:

- Strong internal and external incident reporting mechanisms are in place, which may require changes to existing reporting lines. Businesses should draw on experiences in other areas, such as responding to personal data breaches.
- Employees are kept informed with clear policies and training on incident reporting.
- Clear and robust crisis management and response plans, including business continuity plans (especially where critical services are affected) and backup and recovery procedures, are in place to deal with any such incidents.

Training and awareness

One of the most important measures that should be undertaken pursuant to NIS2 is to ensure that all staff are cybersecurity-aware and undertake cybersecurity training. It is important to ensure that this includes management.

Crucially, management will be required to approve the cybersecurity risk management measures taken by their organisations, oversee their implementation and can be held personally liable for infringements. It is critical to ensure their involvement at all key stages in the process.

Supply chain security

NIS2 also goes beyond NIS1 to ensure that supply chain security is a relevant consideration for in-scope entities. Organisations should consider:

- Third-party risk management measures, including updating risk assessments, including consideration of specific suppliers' vulnerabilities and the quality of their cybersecurity practices, which is frequently a time-consuming process.
- Updating template contracts to include cybersecurity-related provisions covering different aspects, such as conformity and reporting requirements.
- Where required, re-negotiating existing contracts to ensure adequate cybersecurity provisions so that the entity is protected.
- In some cases, organisations may also consider diversifying their supply chain to ensure that having a sole supplier does not create a single critical point of failure.

Organisations should be aware that member states may also require entities to use certain ICT products, services and processes that are certified under European cybersecurity certification schemes. This may affect non-certified providers, as well as those who are required to use certified products.

Fines and senior management awareness

As businesses look to ensure compliance and weigh up the relative costs and risks, the significant fines and reputational risks under NIS2 should be brought to the attention of the board or other significant decision-makers. Among other enforcement actions, infringements of NIS2 can lead to fines of up to:

- 10 million euros, or 2% of total worldwide annual turnover, whichever is higher (for essential entities).
- 7 million euros, or 1.4% of the total worldwide annual turnover, whichever is higher (for important entities).

Senior management could also be liable for infringements and subject to temporary suspensions from managerial duties.

(Huw Beverley-Smith, partner, Charlotte Perowne, associate, and Emily Evans, trainee solicitor, Faegre Drinker Biddle & Reath, London)

Documents in series

NIS2 implementation: key steps for compliance professionals
05-Aug-2024 | TRRI News

Knowing your providers is key to mitigating ransomware risk, says UK NCA cyber chief
29-Jul-2024 | TRRI News

BOARDROOM BRIEFING: European Commission consults on rules specifying significant incidents under NIS2
10-Jul-2024 | TRRI News

BOARDROOM BRIEFING: Swiss regulator issues guidance on common cyber risk failings
12-Jun-2024 | TRRI News

INTERVIEW: Obsolescence, apathy pose greatest threats to banks, says UK's top cybercrime fighter
02-May-2024 | TRRI News