NIS 2 – Frequently Asked Questions

This article is part of a series that Matheson is publishing in advance of transposition and implementation of the second Network and Information Security Directive (EU) 2022/2555 ("**NIS 2**") – the comprehensive new cybersecurity legislation applicable to a wide range of industries across the EU. This legislation will be under the overall supervision of the newly empowered National Cyber Security Centre ("**NCSC**").

For an overview of the legislation and its effects, please see our other articles that we have published including: 'Network and Information Systems 2.0 Directive: New Obligations on Digital Service Providers' and 'NIS2 – Essential and Important Information for Essential and Important Entities.

NIS 2 – Frequently Asked Questions

Matheson

Is NIS 2 going to be implemented in Ireland on time?

On 30 August 2024, the Department of the Environment, Climate and Communications published the highly anticipated General Scheme of the National Cyber Security Bill 2024 (the "**Cyber Security Bill**"), which, once enacted, will transpose NIS 2 into Irish law.

The General Scheme will need to be drafted into a Bill and passed by the Oireachtas (the Irish parliament) before it enters into force. Ireland has not met the implementation deadline of 17 October 2024, and it is possible that implementation may not occur until 2025.

The first NIS Directive, and the European Electronic Communications Code, will continue to apply in Ireland until NIS 2 is fully transposed and enters into force.

What do I need to do in advance of the directive entering full effect?

In-scope entities will need to address compliance with NIS 2 from both a technical and a governance perspective. Cybersecurity is no longer a domain solely for information security and IT professionals, as it now impacts the day to day work carried out by various teams within in-scope entities including, amongst others, Legal, Procurement, HR, and Operations and, crucially, is a top priority for boards.

At the core of NIS 2 is the requirement for all in-scope entities to take "*appropriate and proportional technical, operational and organisational measures*" to manage the risks posed to the security of their systems that are used for operations or for the provision of services (with the aim of preventing or minimising the impact of cybersecurity incidents on those systems and services). These risk management measures are not limited to those focused on mitigating cyber-attacks or, indeed, any specific category of incident. Instead, NIS 2 adopts an "all-hazards approach" which means that the organisation's strategy needs to anticipate risks and incidents holistically. Article 21 of NIS 2 sets out an indicative, non-exhaustive list of measures which should be put in place at a minimum.

In practice, the first step will be identifying the responsible individuals and departments within the organisation which will take responsibility for ensuring overall implementation of cybersecurity risk-management measures. This will depend on the organisation itself, but we expect that such a group will consist of stakeholders from multiple different business functions.

Management bodies (eg, the board of a company) are required to approve and oversee the implementation of cybersecurity risk management measures, and are also required to undertake cybersecurity training to ensure that they have the sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity. This may entail delegating cybersecurity-related functions to an appropriately constituted committee of the board, and ensuring that there are appropriate and effective reporting lines to keep the board fully informed in line with its new statutory obligations.

To prepare for NIS 2 entering into force, in-scope entities should carry out a gap analysis of their existing IT infrastructure / environment, key contractors / service providers / technology vendors, as well as existing cybersecurity controls. As part of this gap analysis, entities should also review their third party supplier contracts and evaluate whether a failure of the counterparties to meet the requirements set out in any such contracts could affect the provision of an in-scope service (and, if so, what contractual protection might be available in such circumstances).

Following completion of the gap analysis, a documented remediation plan to address any identified gaps should be drafted and signed off by the board or an appropriate committee. This should include the adoption of policies addressing risk analysis and information system security, incident handling (including reporting), business continuity (backup management and disaster recovery), use of cryptography and encryption, human resources security (access control policies and asset management), the use of multi-factor authentication or continuous authentication solutions, and secured voice, video and text communications systems. Progress towards completion of a detailed remediation plan will be important for an entity to be able to point to, in the event of a cyber-incident.

In-scope entities should implement a knowledge and training programme addressing cyber threats, including phishing and social engineering techniques, both for the board and ideally for staff as well. A record of the training having been completed should be documented and maintained.

All in-scope entities, whether essential or important, will need to ensure that they have notified themselves to the NCSC in order to be entered on the register of such entities maintained by the NCSC in order to carry out surveillance of ongoing threats.

It is important to note that there will be a range of other steps to be taken depending on the nature and services offered by an in-scope organisation, and the above is only a general guide to the steps that ought to be taken to comply with NIS 2.

NIS 2 – Frequently Asked Questions

Matheson

Do I need to update my contracts with vendors / service providers?

Yes. Essential and important entities should incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers, for example by putting in place, where appropriate, cybersecurity risk-management measures according to Article 21(2) of NIS 2.

This is captured by the requirement under Article 21(2)(c) to ensure supply chain security, including security-related aspects of the relationships between each entity and direct suppliers or service providers and address risks stemming from the supply chain, such as through providers of data storage and processing services or managed security service providers and software.

There is no mandatory list of specific provisions to be included in contracts, as there was in the GDPR or the equivalent of NIS 2 which applies specifically to the financial services sector, the Digital Operational Resilience Act. Essential and important entities should therefore assess and take into account the overall nature and materiality of products and services they receive, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their existing suppliers and service providers, in order to deploy appropriate provisions in the contract.

The current draft of the Cyber Security Bill also grants the NCSC the power to request information from in-scope entities about their technology service providers.

What is the difference between an 'essential' and an 'important' entity?

Both are categories of entities that are within the scope of NIS 2. They are defined based on specific sectors of the economy, and generally will refer to sector-specific legislation which regulates those entities for other purposes (eg, "Healthcare providers" are in-scope by reference to the meaning of that term in Directive 2011/24/EU). Some sectors, such as Wate Management, will only be treated as "important". Others, which are considered "Sectors of High Criticality", will be assessed based on their revenue and size in order to determine whether they are "essential" or "important".

Essential entities are subject to the highest level of supervision, and are subject to ongoing supervision regardless of whether an incident has occurred. Important entities, on the other hand, are subject to a lesser standard of regulatory oversight which will generally apply after an incident has occurred. This does not affect the overall obligation to meet the standards of security that are mandated for all in-scope entities by NIS 2.

Regardless of size or sector, any entity which is designated as 'critical' by the Critical Entities Resilience Directive (Directive (EU) 2022/2557) (which is yet to be transposed) will be deemed an essential entity for the purposes of NIS 2.

Is there any guidance from the Regulator?

The NCSC is the lead competent authority under NIS 2. It is expected to publish updated NIS 2-specific guidance for in-scope entities in advance of the transposition date, which will likely be based on the recently published United States NIST Cyber Security Framework 2.0.

The NCSC has also published a variety of other guidance documents under previous legislation, including Cyber Security Baseline Standards for the original NIS Directive (last revised in November 2022).

In addition, holding internationally recognised cybersecurity certifications such as ISO 27001 is also a good starting point for ensuring NIS 2 compliance for most entities, but will not be a panacea. Much will depend on whether the certification covers the entity's in-scope services and will not cover all of the requirements under NIS 2.

What obligations does NIS 2 place on board members and senior management?

Management bodies must approve and implement the entity's cybersecurity risk-management measures to comply with its obligations under NIS 2. As mitigating risk can be considered a fiduciary duty the directors owe to the entity, there is very limited scope to delegate these obligations.

NIS 2 provides for a suite of new enforcement powers for competent authorities, some of which are significant. This includes the power, in cases of non-compliance with an enforcement order, to apply to the High Court to suspend a chief executive officer from exercising their managerial functions in essential and important entities, unless and until the court is satisfied that the entity meets the requirements set out in the compliance notice.

Similarly, where an entity operates under a licence or permit issued by the relevant competent authority, the High Court may make an order to temporarily suspend the license or authorisation concerning part or all of the relevant services.

In light of these enforcement powers and the potential liability for individuals, we recommend that the board, insofar as cybersecurity is concerned:

- Considers the skills and competencies of the individuals it delegates to;
- Maintains oversight over and, as appropriate, imposes limits on the scope of the delegations;
- Periodically requests updates on significant actions taken / documents executed at board meetings; and
- Requests a review of all delegations of authority on an ongoing basis to ensure they are still required.

NIS 2 – Frequently Asked Questions

Matheson

Is there personal liability for directors or managers under NIS 2?

Yes. There are a number of provisions under the Irish transposing legislation which impose individual liability on members of the management body of in-scope entities. These include failure to comply with supervisory or enforcement orders, and acting negligently where such negligence causes an infringement of NIS 2.

Similarly to other Irish legislation (such as the Criminal Justice (Corruption Offences) Act 2018), where an offence under NIS 2 is committed by a body corporate and is proved to have been committed with the "consent or connivance of, or to be attributable to any wilful neglect" of a director, manager, secretary or other officer, they will be guilty of an offence and are liable to be proceeded against and punished as if they were guilty of the offence. However in our experience, such proceedings against individuals are extremely rare in Ireland.

More novel is the possibility, outlined in question 5 above, of an order being made by the competent authority that a director or CEO be suspended from performing managerial functions until the organisation complies with an enforcement order.

What happens if my organisation suffers a cyber-security incident?

NIS 2 requires "significant incidents" to be reported to the Computer Security Incident Response Team ("**CSIRT**") or competent authority, in addition to notifications of affected service recipients. A serious incident is defined as an incident which:

- causes or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; or
- has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

'Significant incidents' which require reporting are therefore quite broad, as any incident impacting the availability of the service or data could require reporting. This ranges from ransomware or denial of service attacks to a natural disaster affecting the physical infrastructure of the entity leading to a loss of service. Loss or theft of equipment storing information for the entity could also constitute an incident which requires reporting.

The Commission is due to enact further implementing legislation setting out further specific standards for certain types of entity: DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers. This implementing legislation is currently in draft and is available here.

Ultimately, any incident which causes loss of service or data (and not just personal data) could be required to be reported, however there are a number of indicators which would indicate a significant incident, such as the duration of the incident and the number of users that are affected (if relevant).

The reporting obligation involves several reports of increasing detail:

1. Early warning (within 24 hours of becoming aware of the incident)
2. Incident notification (within 72 hours of becoming aware of the incident)
3. Intermediate reports (as requested by the CSIRT / competent authority)
4. Final / Progress report(s) (one month after submission and if the incident is continuing a final report within one month of the incident being handled)

In many cases, these reports will be made to the national CSIRT or competent authority in the Member State where the entity is established, who will act as a 'One Stop Shop' (similar to GDPR). It is important that entities confirm this process, because there are exceptions that may apply. One notable exception to this requirement is for providers of telecommunications services and electronic communications services, which are required to notify in all jurisdictions where they provide services.

What happens if my organisation is in breach of NIS 2 requirements?

Member States have discretion to set out penalties which are "effective, proportionate and dissuasive". As such, the exact penalties will not be known until NIS 2 is transposed into Irish law.

The maximum fines envisaged in NIS 2 include fines for specific breaches of up to €10 million or 2% of total global turnover (whichever is higher). These fines are applicable where an entity infringes Articles 21 or 23 of NIS 2. Senior management can also be obliged to disclose the identity of individual responsible for non-compliance, or to publish details of an infringement.

NIS 2 – Frequently Asked Questions

Will I still have to report incidents to other regulators, such as the DPC or ComReg, under different legal frameworks?

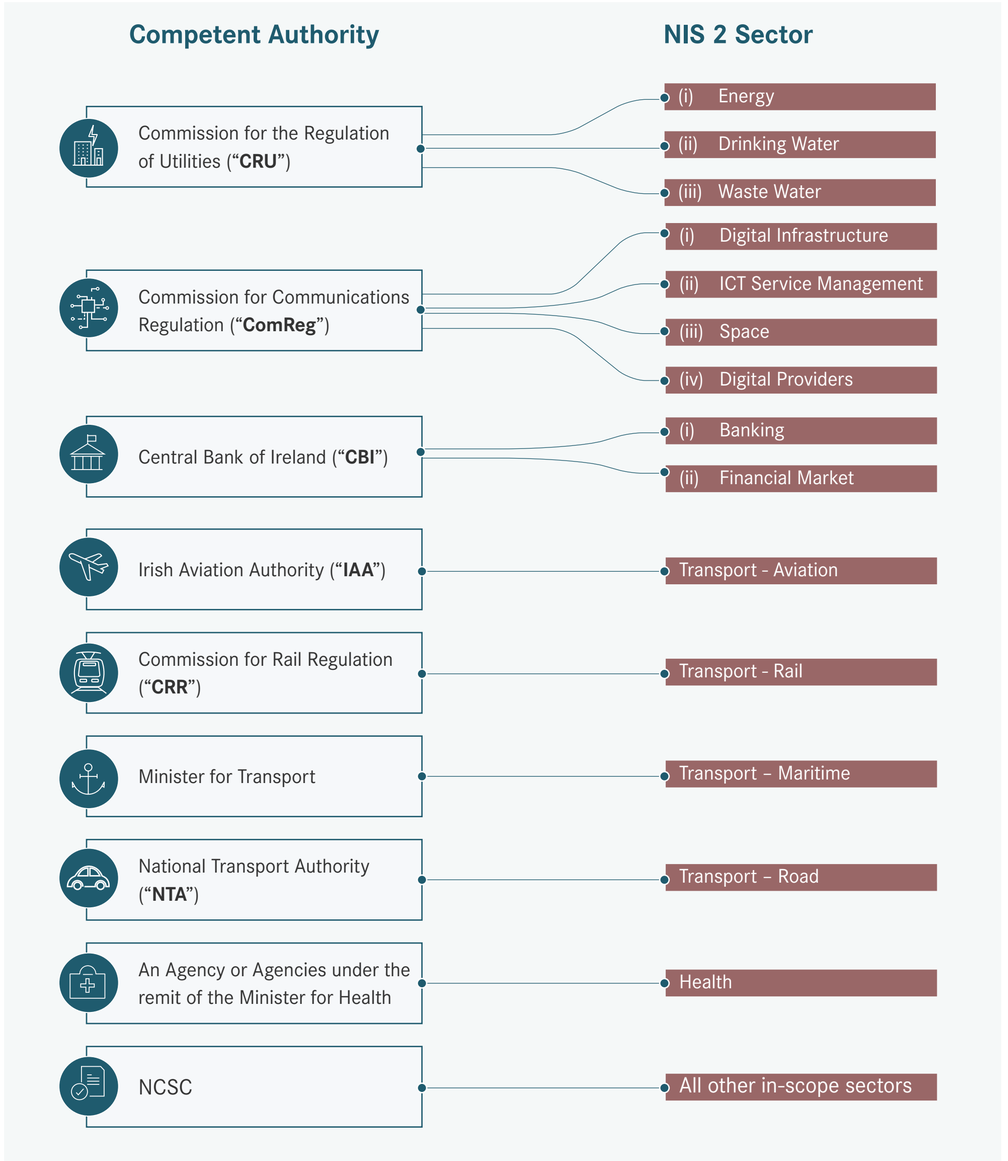
Yes, existing notification requirements under other legislation such as the GDPR will continue to apply.

This depends on the nature of the breach and the sector in which the entity operates in. The requirements for notification of incidents differ under different laws. It is likely that an entity will have to make notifications to the NCSC under NIS 2 and the DPC under the GDPR where personal data is affected by a breach or incident. Lack of access to personal data is itself a reportable breach of the GDPR.

On transposing NIS 2, the requirements of the European Electronic Communications Code will no longer apply.

Who is my regulator?

As signalled, Ireland has opted for a federated regulatory regime for NIS 2. This means that the NCSC shall act as lead competent authority, taking the role of a central coordinator providing advice, guidance and support and development of regulatory frameworks and tools and as the central authority for engagement with European Commission, EU bodies and agencies, and other Member States. The remainder of sectoral competent authorities are proposed as follows:



Your Matheson Contacts

Marie McGinley
Partner
Head of the Technology and Innovation Group
t +353 1 232 3722
e marie.mcginley@matheson.com

Davinia Brennan
Partner
Technology and Innovation Group
t +353 1 232 2700
e davinia.brennan@matheson.com

Deirdre Crowley
Partner
Disputes and Investigations Group
t +353 21 465 8219
e deirdre.crowley@matheson.com

Connor Cassidy
Partner
Disputes and Investigations Group
t +353 1 232 2364
e connor.cassidy@matheson.com

Sarah Jayne Hanna
Partner
Technology and Innovation Group
t +353 1 232 2865
e sarahjayne.hanna@matheson.com