SLAUGHTER AND MAY/

ARE YOU READY FOR NIS2?

New cyber law applies from 18 October

New European cyber law NIS2 must be implemented at local member state level by 18 October 2024. Do you know if you are in scope, and if you are, what you need to do to comply? This briefing will help you understand who is in scope, what new rules NIS2 imposes, how it differs from the regime it is replacing and what steps organisations should take now to comply.

Cyber continues to be a key risk for countries and organisations alike as the world becomes more digital, and threat actors evolve. NIS2 (otherwise known as Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union) is the EU's latest attempt to improve the resilience of network and information systems across the Union.

It has been in force since 16 January 2023, and will apply from 18th October 2024, replacing the original 2016 NIS Directive. Member States therefore have until 17 October 2024 to adopt and publish the national measures required to transpose the directive into their local law, although it looks like some will miss this deadline.

In this briefing, we will highlight some of the key aspects of NIS2 for organisations, and provide some actions you can take to comply, focusing on the following five questions:

In addition to its obligations for organisations, NIS2 imposes various obligations on the Member States themselves regarding their cyber capabilities. These are beyond the scope of this briefing.

As NIS2 is an EU Directive requiring Member States to pass a national implementing law, it is always important to identify your key European jurisdictions. We help clients do this, and check the detail of their relevant national law(s) which may differ slightly from the text of the Directive.

For more information on Member State implementation, see our tracker here.

1. WHAT ARE THE KEY DIFFERENCES BETWEEN NIS AND NIS2?

NIS2 provides legal measures to boost the overall level of cybersecurity in the EU. It builds on the first NIS Directive, which aimed to improve the resilience of network and information systems in the EU against cybersecurity risks, focusing on essential services in key sectors and certain digital service providers.

Following a review of the NIS Directive in 2020, the Commission concluded that it had helped improve the cybersecurity capabilities in Member States but failed fully to address current and emerging cybersecurity challenges. There were also significant divergences in the implementation of the original NIS Directive across Member States.

As a result, the Commission proposed a revised directive, NIS2, which aims to improve on the existing cybersecurity regime. For example, it:

- Expands the scope – NIS2 adds new sectors based on their degree of digitalisation and interconnectedness and how crucial they are for the economy and society. It introduces a clear size threshold rule meaning all medium and large companies in the selected sectors will be in scope. There is also discretion for Member States to bring smaller entities with a high security risk profile in scope.
- Removes the distinction between operators of essential services and digital service providers. Instead entities will be classified as either essential or important entities, and the applicable supervisory regimes will be different as between them.
- Strengthens and streamlines the security and reporting/ notification requirements. NIS2 imposes a risk management approach which lists out minimum security requirements. It also requires organisations to address cyber risk in their supply chains and provide an early warning notification within 24 hours.
- Establishes senior management liability and training obligations as part of its governance provisions.
- Introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims to harmonise sanctions across Member States.
- Introduces changes at European level, including increased information sharing and co-operation between Member State authorities and setting up an EU vulnerability database for publicly known vulnerabilities in ICT products and services.

2. EXPANDED SCOPE: WHO IS IN SCOPE OF NIS2?

One key feature of NIS2 is that it expands the range of organisations and sectors that are now in scope. NIS2 applies to public and private entities which satisfy the following criteria:

1. LISTED IN ANNEX I AND ANNEX II

- » **Annex I** entities in sectors of high criticality like energy undertakings, healthcare providers etc.
- » **Annex II** entities in other critical sectors like cloud service providers, online marketplaces and postal services.
- » **Fig 1** below lists all sectors in Annex I and II.

2. MEDIUM SIZED ENTITY OR LARGER

- » Must employ 50 persons or more, and have an annual turnover of over EUR 10 million.
- » Group figures may be relevant here.
- » **Note:** some entities are in scope regardless of their size - see below.

3. PROVIDES SERVICES OR CARRIES OUT ACTIVITIES IN EU

- » The jurisdictional rules may, however, differ, depending on where the entity is established. See Q5 for more detail.

In addition, NIS2 applies to a list of certain other entities, regardless of their size, including:

- providers of public electronic communication networks ("**PECN**"), publicly available electronic communications services ("**PECS**"), trust services, top level domain name registries or domain name systems services and providers of domain name registration services;
- sole providers of an essential service in a Member State – i.e. a service which is essential for the maintenance of critical societal or economic activities;
- providers of a service, the disruption of which could have a significant impact on public safety, security or health or where disruption could induce a significant systemic risk (in particular for sectors where the disruption could have a cross-border impact);
- entities which are critical because of their specific national or regional importance for a sector or service; and
- certain public administration entities and critical entities under the Directive (EU) 2022/2557 (the "**CER Directive**").

ACTION

Check if you are in scope. If you are part of a larger group, then you may need to assess the group's staffing and turnover numbers to see if the exemption applies.

FIG 1. NIS SECTORS

ORIGINAL NIS DIRECTIVE	NIS2
Operators of essential services	**Sectors of high criticality (Annex I)**
Energy (electricity, oil and gas)	Energy (expanded to include district heating and cooling, and hydrogen)
Transport (air, rail, water, road)	Transport (air, rail, water, road)
Banking	Banking
Financial market infrastructures	Financial market infrastructures
Health (healthcare providers)	Health (expanded to include EU reference laboratories, entities carrying out R&D into medicinal products, manufacturers of basic pharmaceutical products, and entities manufacturing certain critical medical devices)
Drinking water supply and distribution	Drinking water (supply and distribution)
Digital Infrastructure (Internet Exchange Point providers, DNS service providers, top-level domain name registries)	Digital Infrastructure (expanded to include cloud computing service providers, data centre service providers, content delivery network providers, trust service providers, providers of public electronic communications networks and publicly available electronic communications services)
N/A	Waste water
N/A	ICT service management (business-to-business)
N/A	Public administration
N/A	Space
Relevant digital service providers	**Other critical sectors (Annex II)**
Providers of (i) online marketplaces, (ii) online search engines, and (iii) cloud computing services.	Digital providers (providers of (i) online marketplaces, (ii) online search engines, and (iii) cloud computing services)
N/A	Postal and courier services
N/A	Waste management
N/A	Manufacture, production and distribution of chemicals
N/A	Production, processing and distribution of food
N/A	Manufacturing of (i) medical devices, (ii) computer, electronic and optical products, (iii) electrical equipment, (iv) machinery and equipment, (v) motor vehicles, trailers and semi-trailers, and (vi) other transport equipment.
N/A	Research

3. HOW ARE ENTITIES CLASSIFIED? ESSENTIAL v IMPORTANT ENTITIES

NIS2 classifies entities (based on importance) as either **essential** or **important entities**. These replace the previous classifications under the original NIS regime which designated organisations as operators of essential services or relevant digital services providers.

Essential entities are:

- Entities listed in Annex I (*Sectors of high criticality – see above*) which exceed the ceiling for medium-sized enterprises (i.e. they employ 250 persons or more and have an annual turnover exceeding EUR 50 million, or an annual balance sheet exceeding EUR 43 million – which may include partnership and linked enterprises); or
- Entities listed as essential entities in NIS2 (Article 3). This includes a wide range of entities, from qualified trust service providers and top-level domain name registries (regardless of their size) to providers of PECN or PECS which qualify as medium-sized enterprises, certain public administration entities and other entities listed in Annex I or II that Member States identify as essential entities because they meet the national risk assessment criteria (for example, they are the sole provider of an essential service in a Member State).

Important entities are those listed in either Annex I (*Sectors of high criticality*) or Annex II (*Other critical sectors*) which do not qualify as essential entities, or entities identified as important following the national risk assessment criteria.

Member States must establish a list of all essential and important entities as well as entities providing domain name registration services by 17 April 2025.

There are some notable differences in rules depending on whether an organisation is classified as essential or important. Essential entities are subject to a comprehensive ongoing supervisory regime (ex-ante and ex-post), while important entities are subject to a lighter regime which will generally only apply if an incident occurs (ex-post). Fines for essential entities are also higher than those for important entities (see Q5 below).

ACTION

If you are in scope, check if you are an essential or important entity. The way you will be supervised, as well as the fines and some obligations you face, differ depending on which category you fall into.

4. WHAT OBLIGATIONS DO ORGANISATIONS FACE?

NIS2 aims to strengthen and streamline the security and reporting/notification requirements organisations faced under the original NIS regime. It imposes:

A. a risk management approach which lists out minimum security requirements;

B. incident notification obligations; and

C. establishes senior management liability and training obligations as part of its governance provisions.

A. Cybersecurity risk management measures

Essential and important entities must take appropriate and proportionate technical, operational and organisational measures to manage and minimise the risks posed to the security of their networks and systems (i.e. those they use for their operations or for the provision of their services). These measures should take into account the state-of-the-art, relevant standards (European or international) and the cost of implementation as well as factors such as the likelihood of suffering an incident and its potential severity (e.g. its societal and economic impact).

The measures should be based on an "all-hazards approach" that aims to protect both the network and information systems and their physical environment. NIS2 lists ten security measures which should, as a minimum, be included (see Fig 2). Examples include implementing policies on risk analysis and information security, setting up incident handling processes, ensuring business continuity (such as backup management) and using multi-factor authentication where appropriate.

The list also includes managing supply chain security. Entities should take into account the vulnerabilities specific to each direct supplier and service provider as well as the overall quality of the products and cyber security practices of their suppliers and service providers. In addition, the EU may carry out coordinated security risk assessments of critical supply chains, and the results of these assessments should be taken into account.

FIG 2. SECURITY MEASURES

Appropriate and proportionate technical, operational and organisational measures shall include (at least):

I. policies on risk analysis and information system security;

II. incident handling;

III. business continuity, such as backup management and disaster recovery, and crisis management;

IV. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

V. security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

VI. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

VII. basic cyber hygiene practices and cybersecurity training;

VIII. policies and procedures regarding the use of cryptography and, where appropriate, encryption;

IX. human resources security, access control policies and asset management; and

X. 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.

In order to demonstrate compliance, Member States may require that essential and important entities use particular ICT products, services and processes, either developed in-house or procured from third parties, that are certified under European cybersecurity certification schemes.

The Commission is also implementing acts laying down the technical, methodological and sectoral requirements of these measures for some in-scope organisations (namely DNS service providers, TLD name registries, cloud and data centre providers, managed security service providers, online market places, search engines, social network platforms and trust service providers). It may also produce implementing acts for other essential and important entities as well as sectoral requirements.

Note: These provisions do not apply where sector specific rules require essential or important entities to adopt equivalent cyber security risk management measures. An example of such sector specific rules (which was provided by the Commission in a Communication this September) is Regulation (EU) 2022/2554 (Digital Operational Resilience Act) with regard to financial entities.

ACTION

Ensure you have the correct measures in place to manage and minimise your cyber risk.

These are not just technology measures. As a minimum, check you have complied with the ten measures listed in NIS2 and ensure you have incorporated cyber security risk management measures into the contracts with your direct suppliers and service providers. While NIS2 does not contain a list of provisions to include (unlike the GDPR and the financial sector's Digital Operational Resilience Act) you should consider the materiality and nature of the arrangement and ensure measures are proportionate to the risk.

B. Incident notification

In scope entities may need to notify both their regulators and the recipients of their services, depending on the type of incident.

CSIRTs/competent authorities:
Essential and important entities must notify, without undue delay, any incidents that have significant impact on the provision of their services to their relevant Cyber Security Incident Response Team (or "CSIRT"), or, where applicable, their competent authority. NIS2 states that an incident will be significant if it could cause severe operational disruption of the services or financial loss for the entity or could affect others by causing considerable damage.

The entities concerned must submit to the CSIRT (or to the competent authority, if applicable):

- an early warning within 24 hours of becoming aware of the incident: this should indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

- an incident notification within 72 hours of becoming aware of the incident: this should update the information already given and provide an initial assessment of the incident, its severity and impact; and
- a final report not later than one month after the submission of the incident notification: this detailed description of the incident should include information relating to its severity, impact, type or root cause, mitigation measures and (where applicable) cross border impact. Further reports may then be required if the incident is ongoing.

In addition, where the competent authority becomes aware that the incident would also constitute a data breach under the EU GDPR, it will notify the relevant privacy supervisory authority.

Service recipients:
Essential and important entities may also be required to notify the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. This notification should take place without undue delay. They may also need to tell those recipients about any measures or remedies they can take in response to the threat.

These provisions do not apply where sector specific rules require essential or important entities to notify significant incidents (provided the requirements are at least equivalent to those set out in NIS2). Guidance from the Commission confirms that the sectoral rules must be at least equivalent to the NIS2 notification provisions; and that any notifications made under sectoral rules must also be made immediately (and where appropriate, automatically and directly) accessible to the CSIRTs, the competent authorities, or the SPOCs.

ACTION

Update your incident response and notification plans to ensure you:

i. understand who you need to notify and when your notification obligations begin (e.g. when do you become aware); and

ii. are able to comply with your notification requirements, including providing an early 24 hour notification where required. Remember: these notification obligations are on top of any other (e.g. GDPR) notification obligations you may have. Ensure you have good escalation and communication processes and practice all of this as part of your cyber preparedness plans.

C. Governance - role of management bodies

While we have known for some time that cyber is not just an IT issue and requires board and senior management engagement and good governance, NIS2 introduces new obligations on the management bodies of essential and important entities. Management bodies:

- have an obligation to approve the cybersecurity measures taken by their organisations in order to comply with the risk management measures mentioned in Q5 above, and oversee their implementation; and
- can be held responsible for the infringements of their organisations. In relation to essential entities, in certain cases the relevant authorities can request that the CEO or person who acts as the 'legal representative' of the entity is temporarily stopped from exercising managerial functions in that entity. They can also hold that person liable for breach of their duties to ensure compliance with NIS2.

Management bodies are also required to attend training on cybersecurity risks and risk-management practices, and are encouraged to offer similar training to their employees on a regular basis.

ACTION

Identify those responsible within your organisation for ensuring compliance of cyber security risk management measures (individuals and departments). For many organisations this will include stakeholders from across the business. Consider how the board will manage cyber – e.g. will it be delegated to a board committee? How will the full board be kept informed? Are the board (and others) receiving regular training? Do they have sufficient knowledge to ask questions, challenge and (if appropriate) approve the risk management measures? Monitor how Member States are implementing this requirement in local law as it may differ.

5. ENFORCEMENT AND FINES: WHAT HAPPENS IF YOU DO NOT COMPLY?

Competent authorities must effectively supervise and ensure compliance with NIS2 but can prioritise supervisory tasks taking a risk-based approach. Competent authorities will also closely co-operate with the data privacy supervisory authorities when an incident results in a data breach.

A. Fines

NIS2 imposes minimum fines for when essential and important entities breach the risk management (and security) or incident notification obligations. The fines can reach the higher of:

- EUR 10 million or 2% of the total worldwide annual turnover for essential entities; and
- EUR 7 million or 1.4% of the total worldwide annual turnover for important entities.

In both cases, the turnover relates to the preceding financial year of the undertaking to which the essential entity belongs. Member States can also impose periodic penalty payments to compel an entity to stop infringing in accordance with a previous decision of the competent authority.

B. Penalties and powers

In terms of enforcement, Member States will notify the Commission of their rules on penalties under their national implementing laws by 17 January 2025. These rules must be effective, proportionate, and dissuasive.

There will also be a range of additional supervisory and enforcement measures imposed on both essential and important entities, although the rules for essential entities are stricter and ex-ante. For example, competent authorities can subject them to on-site inspections, regular security audits and information/evidence requests as well as providing binding instructions and ordering the entity to stop any infringing conduct.

As mentioned above, there may also be personal implications for the CEO or 'legal representative' of the entity, who may be temporarily suspended/ prevented from exercising their managerial functions and held personally liable for breach of their duties to ensure compliance.

Further, essential and important entities can be ordered by the competent authorities to make public (in a specified manner) aspects of any infringements.

C. Jurisdiction

In scope entities will fall under the jurisdiction of the Member State in which they are established, except in certain specified circumstances. For example:

- Providers of PECN or PECS will fall under the jurisdiction of the Member State in which they provide services.
- Certain IT related or online service providers will fall under the jurisdiction of their main establishment. These include entities such as domain name registries, cloud service providers, managed service providers, data centre providers, social networking platforms, search engines and online market places. NIS2 also states that this list of entities must, if established outside the EU, appoint an EU representative in one of the Member States where its services are offered. This appointment is, however, stated to be *"without prejudice to legal actions which could be initiated against the entity itself"*.

ACTION

It is important to understand which jurisdictions (and therefore which regulators) apply to you, what enforcement regime you face (i.e. are you an essential or important entity) and how personal liability may impact your CEO/legal representative and other senior managers.

COMMENT

If your organisation is already used to complying with an NIS regime, NIS2 is about checking your risk management, security, notification and training processes are still fit for purpose, and adjusting to the new senior management liability provisions. If you are new to the regime, more work will be required to put these processes in place, possibly building on existing sector, or GDPR, processes and procedures.

If your organisation operates across a number of jurisdictions, you will also have to look carefully at the specific local implementing laws in each relevant Member State. While part of the driver for NIS2 was to address issues caused by the significant divergences that existed in the original regime, it is not directly effective and relies on implementation by Member State governments. Divergence is therefore still likely to be an issue.

OUR CYBER PRACTICE

We have advised on some of the highest-profile cyber attacks internationally. We worked alongside a number of our clients including Bupa, Interserve, other listed companies, a series of financial institutions and other clients in regulated industries to advise them on their business-critical response to cyber incidents.

We have a Cyber Hub with experts from our corporate, data privacy, regulatory, technology, investigations and dispute resolution teams which enables us to advise on the full spectrum of cyber issues and, most importantly, equips our clients with a team who know how to tackle cyber issues from every angle.

ROB SUMROY
Partner
+44 (0)20 7090 4032
rob.sumroy@slaughterandmay.com

NATALIE DONOVAN
PSL Counsel
+44 (0)20 7090 4058
natalie.donovan@slaughterandmay.com

This article was written by Rob Sumroy and Natalie Donovan (with thanks to Ralie Belcheva). If you would like to discuss any issues relating to NIS2, the UK's Cyber Security and Resilience Bill (see our blog) or any other cyber matters, please contact Rob, Natalie or your usual Slaughter and May contact.

ACTION

You can find a list of actions to take now to prepare for NIS2 on the next page.

ACTIONS ORGANISATIONS CAN TAKE

SCOPE

- Check if you/your services are in scope. If in scope, check if you are an essential or important entity. We can help with this process.

SECURITY MEASURES

- Check you have the correct measures in place to manage and minimise your cyber risk. These are not just technology measures. As a minimum, check:
  - you have complied with the ten measures listed in NIS2, considering the materiality and nature of the arrangement and ensuring measures are proportionate to the risk; and
  - you have incorporated cyber security risk management measures into the contracts with your direct suppliers and service providers.

NOTIFICATION

- Update your incident response and notification plans to ensure you:
  - understand who you need to notify and when your notification obligations begin (e.g. when do you become aware);
  - are able to comply with your notification requirements, including providing an early 24 hour notification where required;
  - understand how this fits with other notification obligations. Some (e.g. GDPR) will still apply while others (e.g. DORA) may mean you do not need to make separate NIS2 notifications; and
  - have good escalation and communication processes in place and that NIS2 notifications are practised and built into your cyber preparedness plans.Management responsibility

MANAGEMENT RESPONSIBILITY

- Identify those responsible within your organisation for ensuring compliance of cyber security risk management measures (individuals and departments). For many organisations this will include stakeholders from across the business.
- Consider how the board will manage cyber – e.g. will it be delegated to a board committee? How will the full board be kept informed? Are the board (and others) receiving regular training? Do they have sufficient knowledge to ask questions, challenge and (if appropriate) approve the risk management measures?
- Monitor how Member States are implementing this requirement in local law as it may differ. For example, under draft Irish implementing legislation, directors of important entities (and not just essential entities) can also be stopped from exercising managerial functions where those entities have not complied with enforcement measures.

JURISDICTION

- Identify your key European jurisdictions, and check the detail of their relevant national law(s) which may differ slightly from the text of the Directive.
- Check which regulators / Member States will have jurisdiction over you. For some entities this will be where you are established, for others it will be where your main establishment is, or even where services are provided.

MONITORING

- Monitor development at both EU and Member State level. Although NIS2 now applies in Member States, we are still expecting additional information about how it will work in practice (and will be monitoring these for our clients). For example Member States must:
  - notify the Commission of their national rules on penalties by 17 January 2025; and
  - establish a list of all essential and important entities as well as entities providing domain name registration services by 17 April 2025.