NETWORK AND INFORMATION SYSTEMS DIRECTIVE – UK NIS & NIS2 (EU)

August 2024

INTRODUCTION

The Network and Information Systems (NIS) Directive (not to be confused with NIST) is a legislative framework introduced by the European Union (EU) back in 2013. The framework provides a comprehensive approach to reducing cyber risk and enhancing the cyber security posture of the UK and EU member states, and their essential services and critical infrastructure.

Around the same time as the NIS Directive was coming into force, the UK were exiting the EU and so introduced the UK NIS Regulations which came into force for the UK in 2018 around the same time as the General Data Protection Regulation (GDPR). The regulations served as the instrument for transposing the NIS Directive into UK law and specified the obligations and requirements for operators of essential services (OES) and digital service providers (DSPs) in the UK. It was the same framework with the same penalties.

Non-compliance may lead to enforcement and/or penalty notices, and an incident could result in multimillion pound fines. Add to that any reputational and additional financial impact and you are facing potentially damaging consequences. NIS and the related Cyber Assessment Framework (CAF) is, simply put, a set of good practice cyber controls which any wise business should be reasonably expected to be implementing anyway.

The regulation covers governance, risk management, asset management, supply chain, identity and access management, data security, secure design, logging & monitoring, resiliency, incident management and training & awareness.

NIS2

With the threat landscape evolving and the increased reliance on tech since the Covid pandemic, in 2023 the European Union (EU) introduced the second iteration of the NIS Directive known as NIS2. NIS2 enhances some of the requirements and introduces new ones but will only apply to those organisations operating within the European Union. If the organisation is head-quartered and solely operates within the UK then the UK NIS regulation applies.

SECTOR APPLICABILITY

The UK NIS regulation applies to Digital Service Providers (DSPs) and any Operator of an Essential Service (OES). An OES is an organisation that provides an essential service to the UK, which is critical to the national infrastructure. Where the service provision depends on network and information systems, and if an incident would have 'significant disruptive effects' on that service, then the NIS regulation applies.

Sectors currently covered in UK NIS are:

- Energy - Electricity, Gas, Oil
- Health
- Transport - Aviation & aerodromes, rail, road, maritime
- Water - supply & distribution of drinking water
- Postal
- Digital Service Providers (DSPs) (Cloud computing services, search engines)

The NIS2 Directive expands the scope to cover more entities and sectors such as manufacturing, telecoms, wastewater, and food. It also eliminates the distinction between operators of essential services and digital service providers. It also introduces a split between essential and important entities, grouping by disruption impact and size of the business. The same security measures apply to both.

WHO ENSURES THAT COMPANIES ARE COMPLYING?

Both the NIS Directive and UK NIS Regulations designate competent authorities to oversee and enforce compliance with the regulations. Competent authorities, such as those in the UK like Ofwat, Ofgem, Civil Aviation Authority etc, play a crucial role in overseeing the implementation of the NIS Directive and monitor compliance. Alongside member states own national cyber organisations (e.g. the UK's NCSC) as the technical authority for cyber, who provide guidance and work collaboratively with OESs to ensure a cohesive and effective cyber security strategy.

WHAT'S A CAF?

The CAF is the "Cyber Assessment Framework" which is used to assess the OES's cyber controls and can also be used to form the corrective action plan to address any gaps identified during the NIS assessment. It's a systematic approach and is intended to be used as a self-assessment tool, although it can also be used by the regulator or independent auditor.

NIS2 DIFFERENCES

- Expanded Scope of Critical Sectors: The directive expands the definition of critical sectors to include emerging areas that have become increasingly vital to the functioning of society and the economy. Sectors such as wastewater, food, manufacturing, and space.
- Important Entities and Essential entities: The expanded sectors will be defined as either essential or important entities based on how critical they are to society and the economy. This replaces the OES and DSP terminology. Essential entities have a serious impact to society and economy. Important entities are other large sized organisations which play an important role in the economy but would not have such a serious impact. There is an April 2025 deadline to establish this list.
- Incident Reporting: Strengthening the reporting requirements the directive provides more precise provisions on the process of incident reporting, the content of reports and timelines.
- International Collaboration: NIS2 emphasises increased international collaboration and information sharing on cyber security matters. This aligns with the global nature of cyber threats and promotes a collective defence against cyber-attacks.
- Stricter Enforcement and Penalties: The updated directive strengthens enforcement mechanisms and penalties for non-compliance. It introduces administrative fines, differentiating the amounts between essential and important entities.
- Integration with Other Regulations: NIS2 is designed to align with and complement other relevant cyber security regulations and standards. Closely linked are both the Critical Entities Resilience (CER) Directive and the Digital Operational Resilience Act for the financial sector (DORA).
- Increased Regulatory Oversight: The new version provides a minimum list of supervisory measures for the competent authorities and includes regular and targeted audits of the organisations' cybersecurity measures.
- Accountability: For the cyber security measures at organisational level, NIS2 introduces provisions on the liability of natural persons holding senior management positions in the entities. Cyber security risk management measures will need to be approved by these individuals and cyber security training undertaken. Failure to adopt the cyber security measures may result in being held personally liable.
- NIS2 includes a list of 10 key elements that all companies have to address or implement as part of the measures they take, including incident handling, supply chain security, vulnerability handling and disclosure, the use of cryptography and where appropriate, encryption.

Member states have until October 2024 to adopt and publish measures to comply.

WHAT DOES NIS2 MEAN FOR THE UK?

At the time of writing there has been no formal decision on NIS2 for the UK, however following a 2022 consultation, the government did announce its intention to update the UK NIS regulations and in July 2024, the King's speech included an announcement of the Cyber Security and Resilience Bill which will see crucial updates to legislation and will align with the EU's NIS2 directive.

The most recent update on the UK government website is that *"these updates to the NIS regulations will be made as soon as parliamentary time allows."*. As developments unfold, staying informed through official government communications and regulatory updates is crucial.

It is even more likely that the UK regulation will be revised to include enhanced incident reporting, a stronger focus on vulnerability management, and greater cooperation and information sharing requirements.

More details are available via the same government site state that the changes will include:

- bringing managed service providers (MSPs) into scope of the regulations to keep digital supply chains secure.
- improving cyber incident reporting to regulators.
- establishing a cost recovery system for enforcing the NIS regulations.
- giving the government the power to amend the NIS regulations in future to ensure they remain effective.
- enabling the Information Commissioner to take a more risk-based approach to regulating digital services.

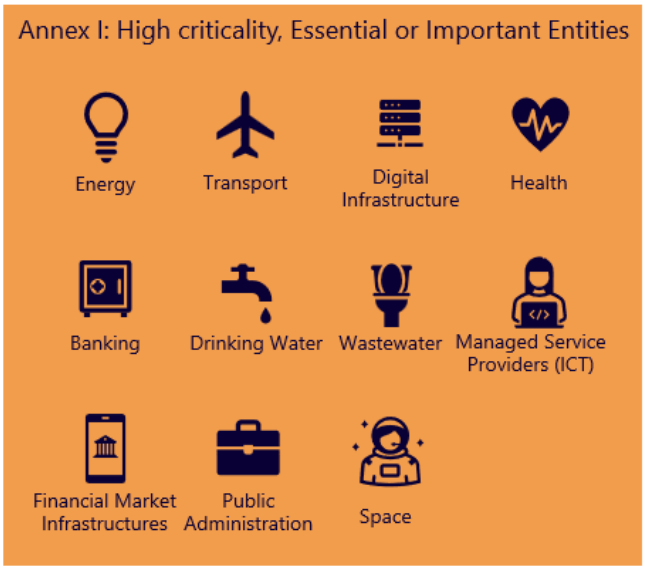
HOW WILL YOUR ORGANISATION BE IMPACTED?

You will need to assess if your company falls under the scope of NIS2:

- Is the company headquarters based in the EU?
- Does your company provide a critical service? See Annex I and Annex II below.
- Is your company based outside of the EU but still operates critical or essential services within the EU?
- Is your company multinational? You will need to assess whether the scope applies to your company in each member state. Also ensure that your organisation is adhering to the different assessment processes which may exist between the member states.

If your company already complies with the UK NIS regulation and does not operate in the EU you do not have to do anything just yet. However, you should prepare now for the impact from the proposed updates.

NIS2 ANNEXES OF SECTORS



Essential
Large enterprises: >€50m annual revenue; 250+ employees
Member State selected: Any size; selected based on risk profile
Important
Large enterprises: >€50m annual revenue; 250+ employees
Medium enterprises: >€10m annual revenue; 50+ employees
Member State selected: Any size; selected based on risk profile

FINANCIAL PENALTIES

Essential Entities	Important Entities
€10m or **2%** of total worldwide annual turnover, depending on which is larger.	**€7m** or **1.4%** of total worldwide annual turnover, depending on which is larger.

FSP.

MANAGING COMPLIANCE TO MULTIPLE DIRECTIVES AND FRAMEWORKS

The regulatory landscape is complex and increasingly we see overlap between the many governance frameworks such as ISO 27001, NIST, IEC 62443 etc. A unified control framework is key to managing and assuring compliance across the different frameworks, resulting in a clear view of mapping to the various regulations. This approach provides the benefit of only testing once to demonstrate compliance with the many requirements. The unified control framework can be expanded to include mappings to policies, standards, procedures, responsible roles, test criteria, and assurance evidence requirements.

Domain	Control Title	Control Description	ISO 27001	NIST CSF 2.0	IEC 62443	NIS2	Documented Evidence	Assurance Activity
Governance	Information Security Roles & responsibilities	• Information security roles and responsibilities are defined, documented, and communicated. • Individuals are aware of their responsibilities and held accountable. • Roles and responsibilities in developing, implementing, and assessing the company's information security strategy are agreed, communicated and understood by the executive management team. • The executive management team set expectations regarding culture and risk management. • Leaders are supporting and enforcing the information security policies & standards. • The Information Security Team is adequality resourced for people and technology.	ISO 27001:2022 Clause 5.3	GV.RR-01/02/03	IEC 62443-2-1 Element 4.3.2.3	NIS 2 Article 7 & 20	• Target Operating Model • Information Security Strategy • Information Security Policy • Job descriptions • Risk Management Strategy • Governance forum terms of reference	• Document review • Interview based • KPIs

LET US SUPPORT YOUR NIS JOURNEY

Choosing FSP for cyber security services, particularly for NIS2, ensures comprehensive protection and compliance with stringent regulations. We leverage deep industry expertise and cutting-edge technology to safeguard critical infrastructure and sensitive data against evolving cyber threats.

By partnering with FSP, customers gain a reliable ally committed to enhancing cyber security resilience and regulatory compliance, ultimately fortifying their business operations in an increasingly digital landscape. We can ensure that your organisation meets all mandatory requirements, avoiding hefty fines and reputational damage.

We take a risk-based approach, firstly conducting an assessment to create a baseline. Gaps will be identified, and quick wins highlighted. An improvement plan will be shaped to address high, medium and low priorities, alongside a longer strategic plan and roadmap. We can recommend target operating models, roles and responsibilities, and support embedding change into your organisation.

Get in touch today!

OUR PEOPLE

Ben Hampshire - Partner
Cyber Security Leadership & Transformation

Derek Taylor - Principal Conslultant
Cyber Security Leadership & Transformation

Louise Pearson - Senior Security Consultant
Cyber Security Leadership & Transformation

+44 (0)118 9357 168 | info@fsp.co | www.fsp.co
Now Building Here & Now, Thames Valley Park, Reading, Berkshire, RG6 1RB | VAT no. 369763244 | Company No. 07717182