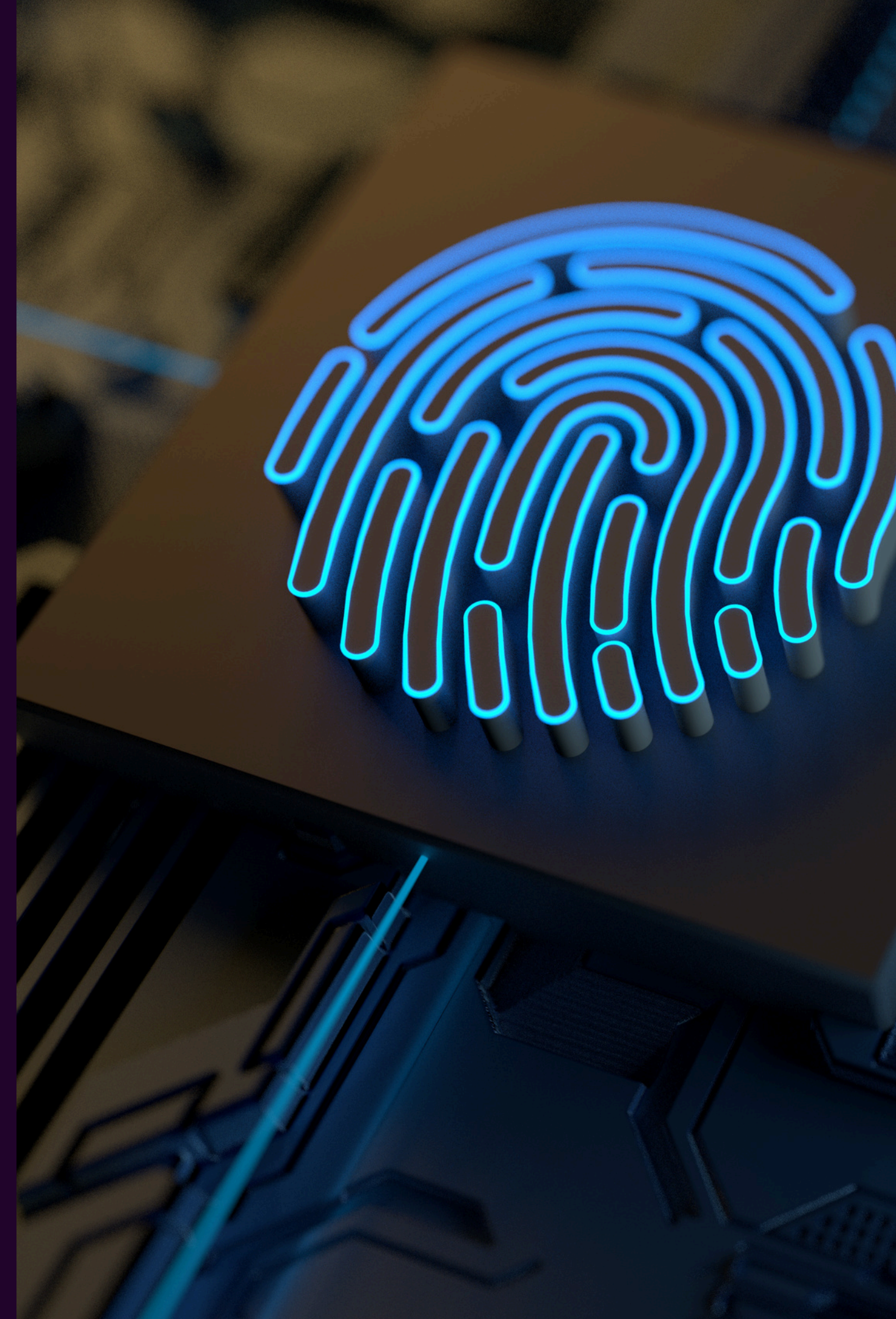




Navigating NIS and NIS2 Regulations:

What Businesses Need to Know



Contents

01

Introduction

02

The Evolution of NIS

03

Expanding the Scope of NIS

04

Does this Apply to my Organisation?

05

Getting it Wrong - Sanctions

06

Summary of Key Points

07

Considerations

08

Getting Help



1 – Introduction to the NIS Directives

About NIS and NIS 2

In the rapidly evolving world of cybersecurity, the NIS (Network and Information Systems) Directive and its successor, NIS2, have become vital components in safeguarding digital infrastructures. Originally established in 2016, the NIS Directive set foundational standards across the EU to enhance resilience against cyber threats. However, with technological advancements and the increasing severity of cyberattacks, NIS2 was introduced in 2023 to bring a more stringent framework, especially for critical and essential sectors.

Whilst NIS 2 is primarily an EU directive currently, The UK Government are likely to adopt to core principles of this and enshrine in UK Law.

Here's a closer look at what these regulations mean for businesses today and how they should prepare.

Drivers – The Changing Cyber Threat Landscape

Over recent years, the attack surface has expanded significantly, driven by increased cloud adoption, remote working, and the proliferation of IoT devices. The average time to detect a cyberattack has reduced dramatically, now often occurring within minutes. Attackers leverage AI, collaborate in groups, and exploit legacy systems, leading to faster and more targeted threats.

Given this complex landscape and the blurring of the perimeter, businesses must ensure that every layer of their security, from firewalls to endpoints are up to date.

Security assessments are now also essential for identifying weaknesses and ensuring robust defences. This evolving landscape has driven the need for a more focused and controlled way of ensuring security and compliance around data at both a personal and national level.



2 - The Evolution of NIS



The shift from NIS to NIS2 reflects a growing need for a unified, robust cybersecurity approach across EU member states. Unlike the original NIS, which allowed individual countries to tailor certain aspects, NIS2 establishes stricter and more harmonised requirements. This change addresses previous fragmentation, enabling a consistent level of security across sectors. Notably, the directive now holds boards more accountable, ensuring that cybersecurity is prioritised at the highest organisational level.

Board Accountability

NIS2 introduces direct accountability for company boards, mandating that cybersecurity be considered a business-critical issue. Boards must understand the organisation's cyber risk landscape and ensure appropriate measures are in place. With organisations now split between new tiers of priority, it's important to understand the requirements unique to your organisation and team.

The NIS2 regulations are to be implemented by each member state, which may result in differing penalties for each state, but these will include potential Jail time or being struck off as a director.

Expanded Scope

The scope of NIS2 is broader, covering a wider range of sectors and organisations. Entities providing digital services, managed service providers, and critical infrastructure operators are now subject to the regulations. This shift means that even organisations indirectly involved in essential sectors must adhere to NIS2's guidelines, extending protection across the supply chain.

Focus on Resilience and Incident Response

NIS2 mandates organisations to develop and regularly test their incident response and business continuity plans. Cyber resilience is a key focus, encouraging organisations to prepare for the entire lifecycle of a cyber incident—detection, response, recovery, and communication.

Reporting Obligations

Breach notification requirements are more stringent. Under NIS2, organisations must report any cybersecurity incident that could impact service continuity to national authorities within a specific timeframe. This early warning system aims to minimise damage and enable quicker, coordinated responses to emerging threats.

Tightened Cybersecurity Requirements

With threats evolving and attack vectors multiplying, organisations are now expected to implement proportional and comprehensive cybersecurity measures. NIS2 emphasises not just the establishment of security policies but also their consistent application. This includes everything from perimeter defences, endpoint protection, to email security.



3 – Expanding the Scope of NIS

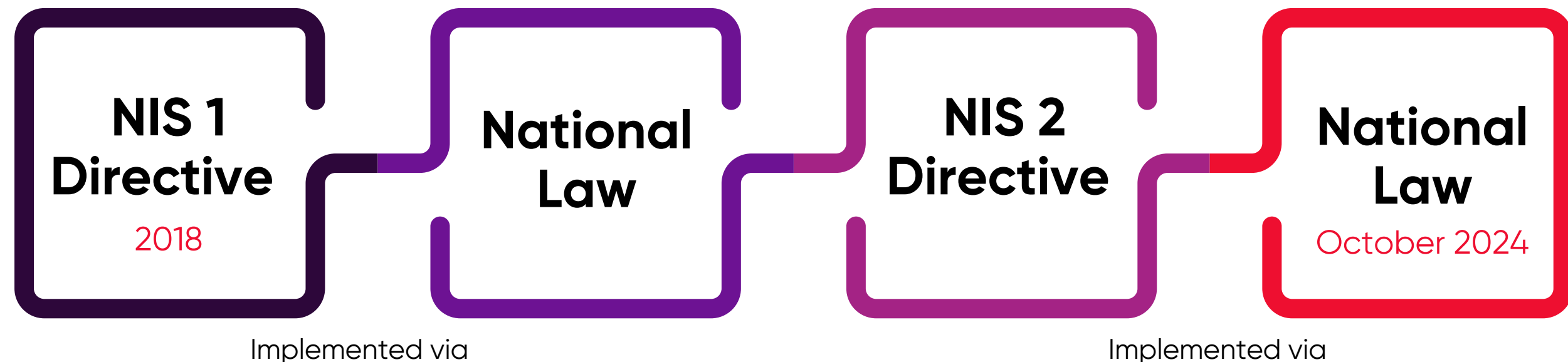
Expansion of the Rules of Scope

Under the original NIS directive, member states held responsibility for identifying which organisations met the criteria to qualify as operators of essential services. The new NIS2 directive, however, introduces a size-cap rule, meaning that all medium-sized and large organisations operating in relevant sectors or providing covered services will now fall within its scope.

While the agreement between the European Parliament and the Council preserves this general rule, the provisionally agreed text includes additional measures to ensure proportionality, strengthen risk management, and define criticality criteria more clearly for determining which entities are covered.

The directive specifies that it will not apply to entities engaged in areas such as defence, national security, public security, law enforcement, or the judiciary. Parliaments and central banks are also excluded from the scope.

Since public administrations are frequently targeted by cyberattacks, NIS2 will apply to central and regional public administration entities. Additionally, member states may choose to extend this application to local-level entities as well.





Expanding the Scope of NIS

NIS2 now applies to a much wider range of industries, covering 18 critical sectors. While the original NIS directive left member states to decide which entities fell within its purview, NIS2 standardises this by automatically including all medium and large businesses within these sectors. Industries such as public administration, waste management, aerospace, and manufacturing are now explicitly covered.

The NIS2 Directive applies broadly to entities within the sectors outlined in Annexes I and II, specifically targeting organisations that meet the European legal definition of a medium-sized enterprise. Typically, this includes entities with a minimum of 50 employees or those with an annual turnover or balance sheet exceeding EUR 10 million. However, Article 2(2)–(5) of the NIS2 Directive expands this scope to include certain organisations irrespective of their size.

This exemption applies to providers of public electronic communication networks or services that are publicly accessible, as well as specific public administration bodies. For these entities, employee numbers, turnover, and balance sheet totals are not determining factors.

NIS 1 Directive	NIS 2 Directive
Energy	Energy
Drinking water supply and distribution	Drinking water, Wastewater
Digital infrastructure	Digital infrastructure
Health sector	Health
Banking, Financial market infrastructures	Banking, Financial market infrastructures
Transport	Transport, Space (partial), Postal and courier services
	Production, processing and distribution of food
	Waste management
	ICT service management (B2B)
	Public administration
	Manufacture, production and distribution of chemicals
	Manufacturing
	Digital providers
	Research

4 – Does NIS 2 Apply to my Organisation?



Essential and Important Entities Under NIS 2

Generally, the NIS2 Directive applies to companies with a workforce of at least 50 employees or those with an annual turnover or balance sheet exceeding EUR 10 million. However, in specific instances—such as for providers of publicly accessible electronic communication services, the directive applies regardless of the entity's size.

The directive's requirements are largely based on whether an organisation is classified as an “essential” or “important” entity.

Essential Entities

- Entities in the sectors listed in Annex I that exceed the thresholds of at least 250 employees or an annual turnover of over EUR 50 million and an annual balance sheet total of over EUR 43 million;
- Qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
- Providers of public electronic communication networks or publicly available electronic communications services that exceed the thresholds of at least 50 employees or an annual turnover or an annual balance sheet total of over EUR 10 million;
- Public administration entities of the central government of a member state (as defined by that member state);¹ Entities explicitly classified by a member state as “essential entities”;
- Entities identified as critical entities under the CER Directive (EU) 2022/2557;
- If the member state so provides, entities which that member state identified as operators of essential services under the NIS 1 Directive or national law
- Providers of public electronic communication networks or publicly available electronic communications services that exceed the thresholds of at least 50 employees or an annual turnover or an annual balance sheet total of over EUR 10 million;

Important Entities

- Entities in the sectors listed in Annex I or II that do not qualify as essential entities;
- Entities explicitly identified by member states as “important entities”.



5 - Getting it Wrong - Sanctions

Sanctions for Violations of NIS 2

The NIS2 Directive requires EU member states to establish provisions for imposing fines on entities that breach Article 21 (concerning risk management measures) and Article 23 (relating to reporting obligations for major security incidents). Additionally, the directive outlines minimum thresholds for the maximum range of these fines.

Essential Entities

Administrative fines of up to
10 million EUR
or
2% of the total worldwide annual turnover in
the preceding financial year of the
undertaking to which the essential entity
belongs, whichever is higher

Important Entities

Administrative fines of up to
7 million EUR
or
1.4% of the total worldwide annual turnover
in the preceding financial year of the
undertaking to which the essential entity
belongs, whichever is higher



The NIS 2 Directive requires essential and important entities to take appropriate and proportionate technical, operational and organisational action to manage the risks posed to the security of the network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on the recipients of their services and on other services

(Article 21(1) NIS 2 Directive)



6 – Summary of Key Points

The NIS2 Directive represents an evolution in cybersecurity legislation, aiming to fortify digital security across the EU and impacting a wider range of sectors than its predecessor. Here are some crucial points from the directive, adapted to provide clarity and actionable insights for organisations.

Broadened Scope and Sectoral Inclusion

NIS2 now applies to a much wider range of industries, covering 18 critical sectors. While the original NIS directive left member states to decide which entities fell within its scope, NIS2 standardises this by automatically including all medium and large businesses within these sectors. Industries such as public administration, waste management, aerospace, and manufacturing are now explicitly covered. For organisations within these sectors, this broadened scope mandates a proactive approach to cybersecurity.

Management Accountability

The directive underscores the importance of cybersecurity as a core management responsibility. Top executives are expected not only to ensure compliance with cybersecurity requirements but also to monitor these measures directly. This responsibility is enforceable, meaning management can be held personally accountable if the organisation fails to meet the NIS2 standards. Executives should prioritise cybersecurity as part of strategic decision-making to avoid legal and financial repercussions.

Mandatory Risk Management Measures

NIS2 introduces a requirement for both “essential” and “important” entities to establish rigorous risk management frameworks. This includes implementing technical and operational safeguards tailored to their organisation’s specific risk profile. The directive suggests a comprehensive approach, considering both digital and physical risks—such as phishing, data theft, and even physical security vulnerabilities. By addressing these areas, organisations can enhance their overall cybersecurity posture.

Incident Reporting Obligations

Timely incident reporting is a significant aspect of NIS2. Organisations must report any serious cybersecurity incidents to the appropriate national authorities within a designated timeframe. This approach is intended to foster rapid, coordinated responses across sectors, minimising disruption and potential harm. Organisations should establish and routinely test their incident response plans to ensure compliance with these reporting requirements.

Supply Chain Security

A notable addition in NIS2 is the emphasis on securing the supply chain. Organisations are responsible for evaluating and managing the cybersecurity practices of their suppliers and partners, particularly those involved in delivering essential services. This requirement extends even to organisations outside the EU if they supply services to EU-based entities. To comply, organisations should integrate security assessments into their supplier selection and management processes, ensuring their broader ecosystem aligns with NIS2 standards.



NIS Practical Steps for Compliance



7 - Practical Steps for Compliance



Now we have provided an overview of the requirements of NIS, what can your organisation do to ensure they are compliant with the directive. Below are the major action areas that will help you be more secure and prepared to meet the demands.

1

Understand and Map Cyber Risks

Organisations must take stock of their unique cyber risk profile, evaluating all potential entry points. This process includes examining both direct and indirect risks, such as those within their supply chains, and ensuring that they understand the data protection responsibilities involved.

2

Invest in Proportional Controls

The concept of proportionality is crucial in NIS2. Businesses should implement controls that match the level of risk they face, balancing cost and complexity.

These risks will be unique to each organisation and you will need to understand the challenges and risks you face and the impact of these to identify areas where controls need to be implemented. This could mean anything from firewalls and endpoint security to sophisticated AI-driven threat detection systems.

Practical Steps for Compliance



3

Educate the Board and Staff

Ensuring a common language of risk within the organisation is essential. Training board members and non-technical staff to understand cyber risks and their impacts will help align the organisation's objectives with its cybersecurity posture.

This may require a multi-faceted approach including in-person mentoring through to organisation-wide cyber awareness training to educate on risks, change behaviours and create a culture of security.

4

Engage in Continuous Improvement

Cybersecurity is not a one-off project but an ongoing process. Regular updates, vulnerability assessments, and strategic improvements are crucial for staying ahead of attackers. Organisations should avoid the trap of outdated defences, instead opting for a dynamic approach that adapts to emerging threats.

Mindset of visibility and dynamically updating controls – this is not a project but a continuous process



Practical Steps for Compliance



5

Prepare Incident Response Plans

Having a well-documented and tested incident response plan is key. Organisations should know how to communicate with stakeholders, manage public relations, and ensure business continuity if a cyber incident occurs.

Organisations must carry out ongoing testing and revisions of these plans and lessons learned are implemented.

6

Consider Managed Cybersecurity Services

Given the technical expertise required and the complexity of compliance, many organisations may benefit from outsourcing aspects of their cybersecurity to managed service providers.

These providers can offer 24/7 monitoring, threat detection, and rapid response, ensuring a high level of security without the overhead of in-house management. Utilising outsourced security expertise can help organisations augment risk.





Looking Ahead

The implementation of NIS2 is just one step in an evolving regulatory landscape. With cyber threats only expected to increase, regulatory bodies are likely to continue tightening requirements, particularly for critical sectors. For UK organisations, there are already indications that stricter regulations, similar to NIS2, may be on the horizon.

For businesses, aligning with NIS2 is about more than avoiding penalties; it's an opportunity to strengthen organisational resilience, protect stakeholders, and enhance trust. As the cybersecurity landscape continues to evolve, proactive compliance with NIS2 and future regulations will be a crucial differentiator in today's digital economy.

Delivering the right security posture isn't a tick-box exercise and there are still many organisations that just give lip service to the importance of cyber security. With greater importance than ever in adopting a culture of security, especially within the public sector, who will be critical in taking steps to drive up standards. More legislation and mandates will follow so , don't wait till you are attacked until you start to take action.



Cybersecurity is a journey, not a destination – you need to continually work at it



NIS Getting Help

About **FourNet**

FourNet works with some of the most secure, critical and commercially driven organisations in the UK.

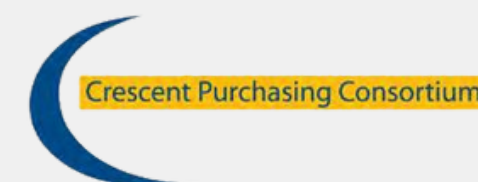
Our expertise is in transitioning and integrating complex, legacy systems to deliver the latest communication, collaboration, and contact centre capabilities.

We provide the knowledge and technical expertise to help our customers achieve their digital transformation and customer experience goals. FourNet's Intelligent Managed Service frees up time for our customers to focus on running their business, without having to worry about their communications infrastructure.

Our Infrastructure Partners



Easy To Procure



How we can Help



FourNet Assess

Organisations need to understand cyber risks and their ability to handle and manage a cyber attack. Our consultative approach creates a benchmark of your current security strengths and weaknesses. This allows us to prioritise areas for attention in line with organisational goals and priorities overlayed with risk analysis. Approaching cybersecurity not just as technical issue, our methodology revolves around three key elements, people, process and technology.

FourNet Protect

FourNet Protect provides next generation security services including mail protection, advanced Endpoint Detection and Response (EDR) and Security Access Service Edge (SASE) to protect applications and services. Wherever the network is accessed, and however the perimeter moves, FourNet Protect ensures users are safe and secure.

FourNet Defend

No matter what technology solutions are in place an attacker only needs to be successful once to compromise the network and organisation. With FourNet Defend our team of experienced cybersecurity professionals work in unison with internal teams, utilising advanced tools and methodologies to swiftly detect, analyse, and mitigate threats.

Defence in Depth

Defence in depth is essential in cybersecurity as it provides multiple layers of protection, reducing the risk of breaches if one layer is compromised. In the UK, where cyber threats are constantly evolving, this layered approach helps organisations detect and respond to attacks more effectively, minimising the impact on business continuity and national security. By combining controls like firewalls, encryption, and access management, defence in depth strengthens overall resilience, fostering greater trust in systems and services.

Delivering a Zero Trust Strategy

In today's threat landscape, traditional perimeter-based security is no longer sufficient. Zero Trust is a security model that assumes no trust and requires continuous verification of all entities. This approach significantly reduces the risk of breaches, ensuring robust protection for your sensitive data and systems.

Discover more about ZTNA in our quick guide to Zero Trust

[Download Here >>](#)



Thank you

Discover how we can help you achieve secure outcome and Compliance

Get in touch

0845 055 6366

hello@fournet.co.uk f