nccgroup

People powered tech-enabled cyber security

A Guide To Preparing For The

Network and Information Security Directive (NIS2)

How to ensure compliance with the EU's new harmonising cyber security directive

Contents

What is NIS2?

NIS2 is a significant piece of Legislation that provides legal measures aimed at increasing the overall level of cyber security across organisations within the European Union (EU).

The NIS2 directive, which succeeds the original NIS directive expands its scope to new sectors and places greater focus on governance and accountability, cybersecurity risk-management, incident reporting and supply chain security.

To achieve compliance, organisations must be able to demonstrate appropriate and proportionate technical, operational and organisational measures are in place to manage risk, as well as processes to meet incident reporting and cyber security governance requirements.

In cases of non-compliance, regulators will have the power to impose steep penalties of up to 10,000,000 EUR or up to 2% of total worldwide

Deadline
17 Oct 2024

EU Member States have until October 17, 2024, to transpose the directive into their national legislation, making this the effective date for NIS2 to come into force across the EU.

However, timelines could potentially vary due to aligning national laws with NIS2 and how the directive will be enforced in each Member State.

Who does NIS2 apply to?

All organisations that offer essential and important services within the EU are impacted by NIS2. This includes organisations based in non-EU countries such as the UK, who have a presence in the EU.

To determine whether your organisation falls within the scope of NIS2 requirements involves numerous factors, many of which are specific to individual states.

Our concise visual guide can help you identify key areas of impact. To better understand your specific needs, consider requesting a NIS2 Readiness Assessment.

Even if you are not currently subject to NIS2, future expansion may bring you into scope, necessitating the demonstration of robust cybersecurity controls to your clients and supply chain.

NIS2 applies to Private and Public entities that provide services or carry out activities in any country in the European Union that meet the threshold of NIS2 as below.

Highly Critical

- Energy
- Public Administration
- Transport
- Health
- Finance
- Space
- Drinking & Waste Water Supply
- Digital Infrastructure
- ICT Services

Other Critical

- Postal services
- Waste Management
- Chemicals
- Research
- Foods
- Digital Providers
- Manufacturing

Essential

Large entities
50m annual revenue
250+ employees

- Qualified Trust Service Providers
- Public Admin
- Operators of Essential Services
- Member State selected: Any size entity; selected based on risk profile

Important

Medium entities
10m annual revenue
50+ employees

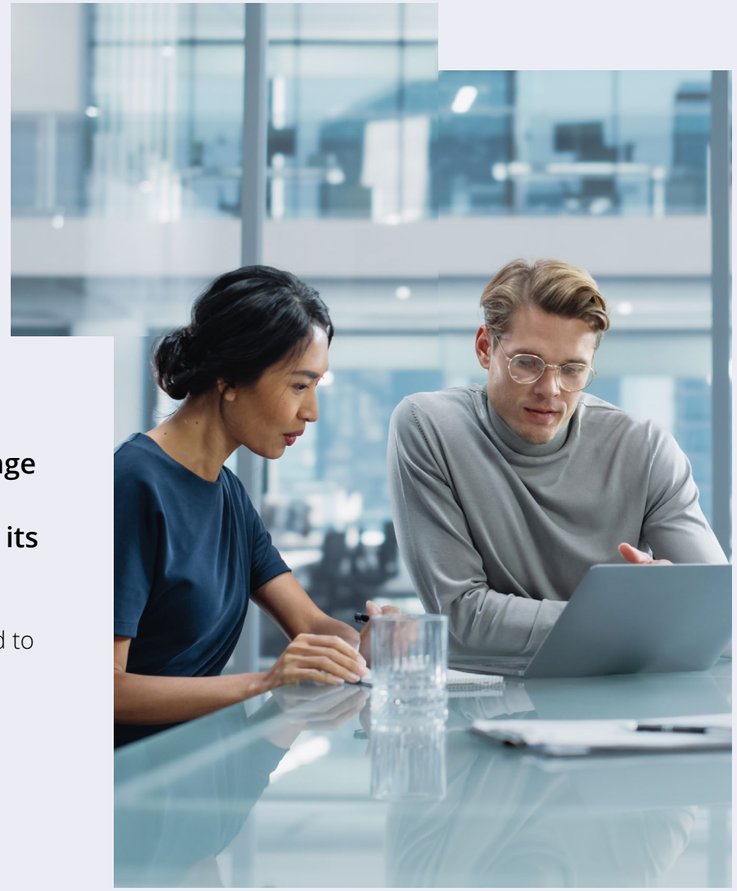
Important

Large entities
50m annual revenue
250+ employees

Medium entities
10m annual revenue
50+ employees

- Member State selected: Any size entity; selected based on risk profile

Key requirements under NIS2



The major challenges of NIS2 compliance Under NIS2, your organisation must comply with a range of cyber security requirements to ensure the security and resilience of its operations.

As you work towards compliance, you will need to address issues including:

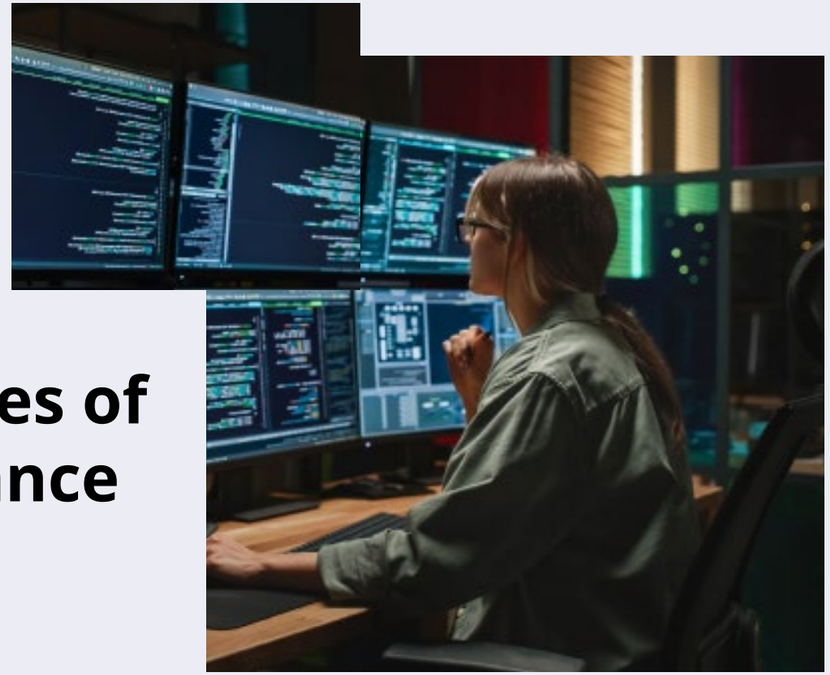
- Top management accountability for non-compliance
- Specific security measures
- Providing notification of incidents within a given timeframe

If your organisation falls within the scope of NIS2, what requirements must it comply with?

1. Policies on risk analysis and information system security
2. Incident handling and notification
3. Business continuity (backup management, contingency provisioning, crisis management)
4. Supply Chain Security
5. Security in the acquisition, development, and maintenance of network (including vulnerability response and disclosure)
6. Measuring the effectiveness of measures (policies and procedures)
7. Cyber hygiene and training
8. Cryptography and Encryption Usage Policies and Procedures
9. Human resources security aspects (rights management)
10. When appropriate, MFA, Continuous Authentication Solutions, Secure Communications, Secure Emergency Communication Systems

Supervision under NIS2 will differ for ‘Essential’ entities vs ‘Important’ entities.

‘Essential’ entities will be subject to proactive (ex ante) supervision under NIS2, whereas ‘Important’ entities will be monitored under reactive (ex post) supervision.



Consequences of non-compliance with NIS2

NIS2 provides national authorities a range of enforcement powers and specifies penalties for non-compliance, including:

Non-monetary remedies

- Warnings: Issue warnings for non-compliance,
- Compliance Orders: Directing organisations to take specific actions to comply with the directive.
- Binding Instructions: Issuing mandatory instructions that organisations must follow.
- Security Audits: Mandating that organisations undergo security audits, implement the provided recommendations, and fulfil reporting obligations within a reasonable deadline to ensure compliance.
- Threat Notifications: Requiring organisations to notify their customers about potential threats

Administrative fines

For ‘essential entities’, fines can reach a maximum of at least 10,000,000 EUR or up to 2% of the total worldwide annual turnover from the preceding financial year.

For ‘important entities’, this is a maximum of 7,000,000 EUR or 1.4% of turnover.

Criminal sanctions

Top management can face criminal sanctions for gross negligence in cyber security incidents. These sanctions include:

- Public Disclosure: Ordering that organisations make compliance violations public.
- Public Statements: Issuing public statements identifying the individuals responsible for the violations.
- Temporary Bans: Temporarily banning individuals from holding management positions in case of repeated violations.

These penalties can be imposed on essential entities and important entities for infraction such as failure to meet security requirements and failure to report incidents.

The exact fines will differ based on the Member State, which will levy financial penalties on organisations that do not comply within the specified timeframe.

Incident handling

NIS2 introduces stringent reporting obligations for significant cyber incidents. Organisations must promptly report incidents that have a substantial impact on the provision of their services to national authorities.

The directive also encourages organisations to analyse incidents thoroughly and implement lessons learned to enhance future security measures.

To be able to meet the reporting objectives, it is crucial to have a structured mechanism in place to detect, analyse, communicate and respond to security incidents.

Leveraging continuous improvement initiatives and scenario testing can improve the overall effectiveness of an incident response capability, while well-defined communication protocols can facilitate the timely and accurate communication with regulatory authorities as required by NIS2.

Assessing cyber risk

Appropriate and proportionate measures to manage risk are essential under NIS2.

Assessments such as (but not limited to) vulnerability scans, threat led penetration testing, red teaming, attack path analysis, and internal audits enable your organisation to identify and address vulnerabilities within the organisation's cyber defences.

By regularly evaluating the effectiveness of risk-management measures, you significantly improve your capabilities in detecting weaknesses before they are exploited by malicious actors.

Effective assessment of response procedures involves rigorous testing and simulation of potential attack scenarios.

This not only prepares the organisation for real-world threats but also educates and trains employees on how to respond effectively during an incident.

Appropriate and proportionate action

Your approach to cyber risk management should be appropriate and proportionate to ensure that resources are efficiently utilised to protect against threats without overburdening operations.

An appropriate approach tailors the security measures to the specific risks faced by the organisation, considering its size, industry, criticality of assets and social and economic impacts.

A proportionate approach balances the cost and complexity of security measures with the level of risk.

Overly stringent measures for low-risk scenarios can waste resources and hinder productivity, while insufficient measures for high-risk areas can leave the organisation vulnerable to significant breaches.

The dangers of delaying compliance

Why act now?

• Getting ready for compliance could cost you considerable time, resource, and budget, depending on the maturity of your current policies and ICT risk management processes. The nation state you operate within could affect how soon you must comply with NIS2.

• Your organisation may be liable for significant penalty payments, depending on your local regulatory body. NIS2 provides national authorities with a minimum list of enforcement powers for non-compliance, reaching up to 10,000,000 EUR or up to 2% of global turnover.

• Management bodies for both essential & important entities can be held personally liable for infringements, to their cyber security risk-management and reporting obligations. Specifically for essential entities, individuals can be prohibited from carrying out managerial or chief executive duties under the directive.

Your Roadmap to NIS2 Compliance

Implementation for NIS2

Services to support with NIS2 compliance

Your compliance journey is easier with NCC Group. We offer unique 360° readiness to help organisations of all sizes and sectors to prepare for regulations like NIS2.

- Managed Extended Detection and Response (MXDR)
- Digital Forensics & Incident Response
- Red/Purple Teaming
- Threat Intelligence
- Business Continuity/ Disaster Recovery Reviews
- Cyber Security Review (CSR)
- Policy Packs
- Third Party Risk Management
- Training and Awareness
- ISO 27001

Get in touch to discuss how you can plan for NIS2 compliance within your organisation.

Call: 0161 209 5111
Email: response@nccgroup.com
nccgroup.com

Hannah McCartney
Cyber Security Consultant
NCC Group
hannah.mccartney@nccgroup.com

Juilian Brown
Managing Consultant,
NCC Group
julian.brown@nccgroup.com