NIS2: STAYING COMPLIANT IN 2025

Your comprehensive guide to understanding the core principles and obligations of the new European cybersecurity directive, with practical steps to create an effective action plan and ensure you're fully prepared.

Insight helps you get started...

Insight | Microsoft

NIS2: a brief overview

The European Union (EU) has drawn up the NIS2 legislation to improve cybersecurity and cyber resilience. Member states have until 17 October 2024 to transpose NIS2 measures into national law, which organisations must comply with.

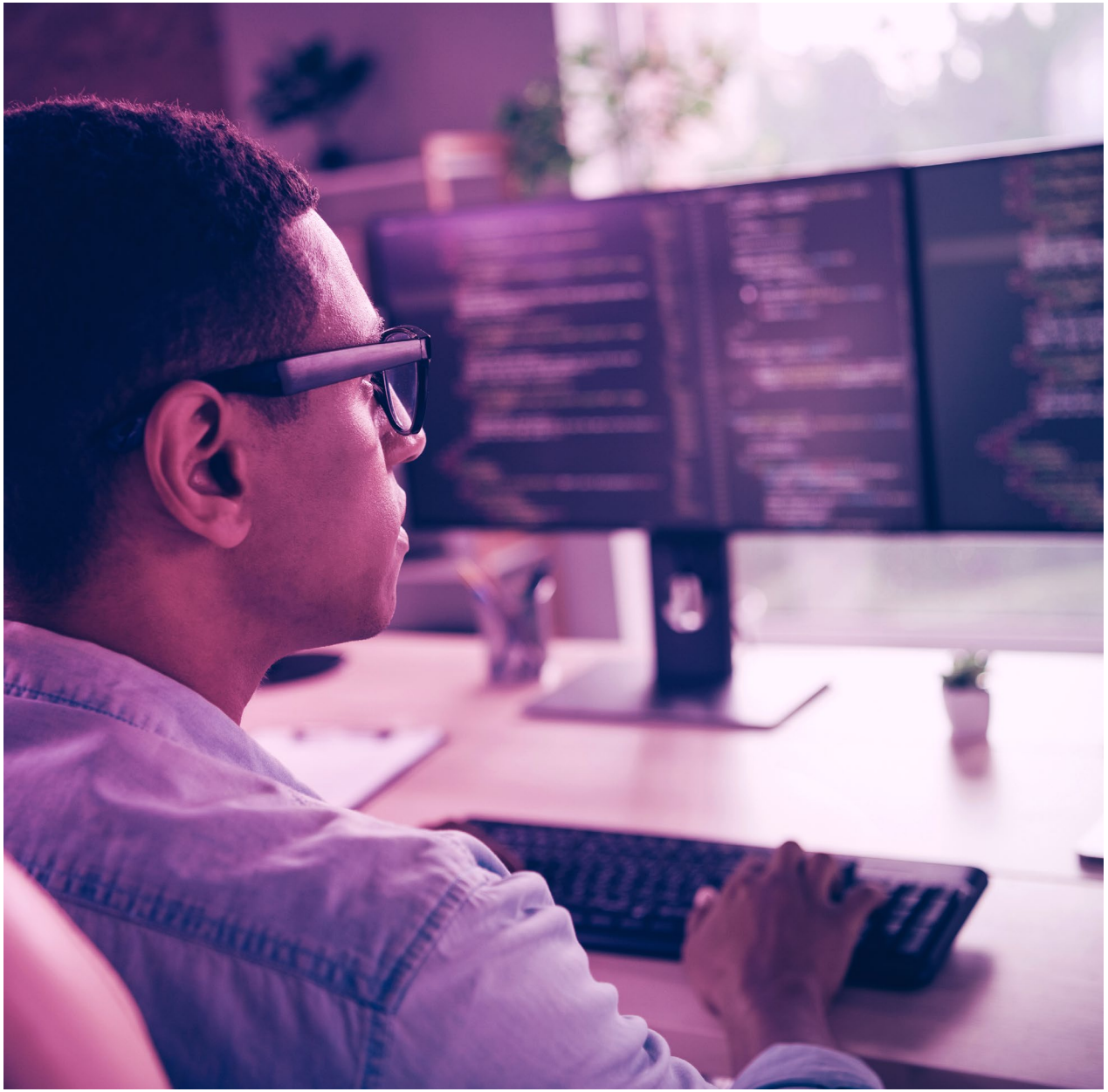
NIS2 applies to 'essential' and 'important' entities in certain sectors of a certain size. Supply chain partners and specific organisations must also comply. The law includes responsibilities such as duty of care, reporting obligations, and supervision. The duty of care requires organisations to conduct their own risk assessments and take measures to ensure digital security and continuity. Under the reporting obligation, incidents must be initially reported within 24 hours if there is a service disruption. Oversight includes proactive and reactive controls for key entities. Fines can be imposed for non-compliance, and directors are personally responsible and jointly liable for following the NIS2 guideline.

It is crucial for all organisations, even those not directly affected by NIS2, to critically assess their resilience against cyber threats. Every organisation faces risks such as reputational damage, data theft, and financial losses. Implementing NIS2 guidelines provides an excellent starting point for enhancing and continually improving cybersecurity measures. As the new NIS2 Directive raises the bar for security and compliance, Insight and Microsoft help organisations align regulatory readiness with broader cloud security transformation, helping organisations build resilience, strengthen security, and simplify compliance.

Understanding NIS2

NIS2 is the new European directive for network and information security, replacing the 2018 NIS directive. It will come into force in October 2024. The purpose of NIS2 is twofold: to harmonise cyber resilience practices across Europe and to enhance cybersecurity for companies and organisations. Unlike the original NIS guidance, which only focused on essential sectors such as water, energy, and telecoms, NIS2 will apply to a wider range of organisations.

> "To comply with the NIS2 guidelines, you need to identify which of your organisation's systems and services are considered critical infrastructure and assess the associated risks. Once you have this information, you can determine the necessary measures to implement and how to integrate them into your organisation."
>
> Dirk de Goede, Security Specialist at Insight



Who does NIS2 apply to?

The NIS2 guideline classifies organisations based on their sector and their significance to society and the economy. It distinguishes between two types of entities: 'essential' and 'important' entities, with additional provisions for special cases, such as supply chain partners.

Essential Entities:	Important Sectors
Energy	Postal and courier services
Infrastructure for the financial market	Foodstuffs
Digital infrastructure	Waste management
Government services	Digital providers
Health	Manufacturing industry
Banking	Chemicals
Transportation	Research
IT services administrators	
Drinking water	
Space travel	
Waste water	

The following criteria is used to decide if NIS2 applies to your organisation:

Essential Entities:

Large organisations with over 250 employees, a turnover above 50 million euros, and a balance sheet total exceeding 43 million euros. These are crucial to the economy and society, and the government actively monitors them.

Important Entities:

Medium-sized organisations from the essential entities group and medium-to-large organisations in other key sectors. These entities have at least 50 employees or an annual turnover and balance sheet total above 10 million euros. They face less stringent oversight but will be audited if there are signs of non-compliance or following an incident.

Additionally, NIS2 will apply to:

- **Certain small organisations**
- **Supply chain partners of essential and important entities**
- **Some other exceptions**

What are the obligations outlined in NIS2?

NIS2 includes three main obligations:

Duty of care

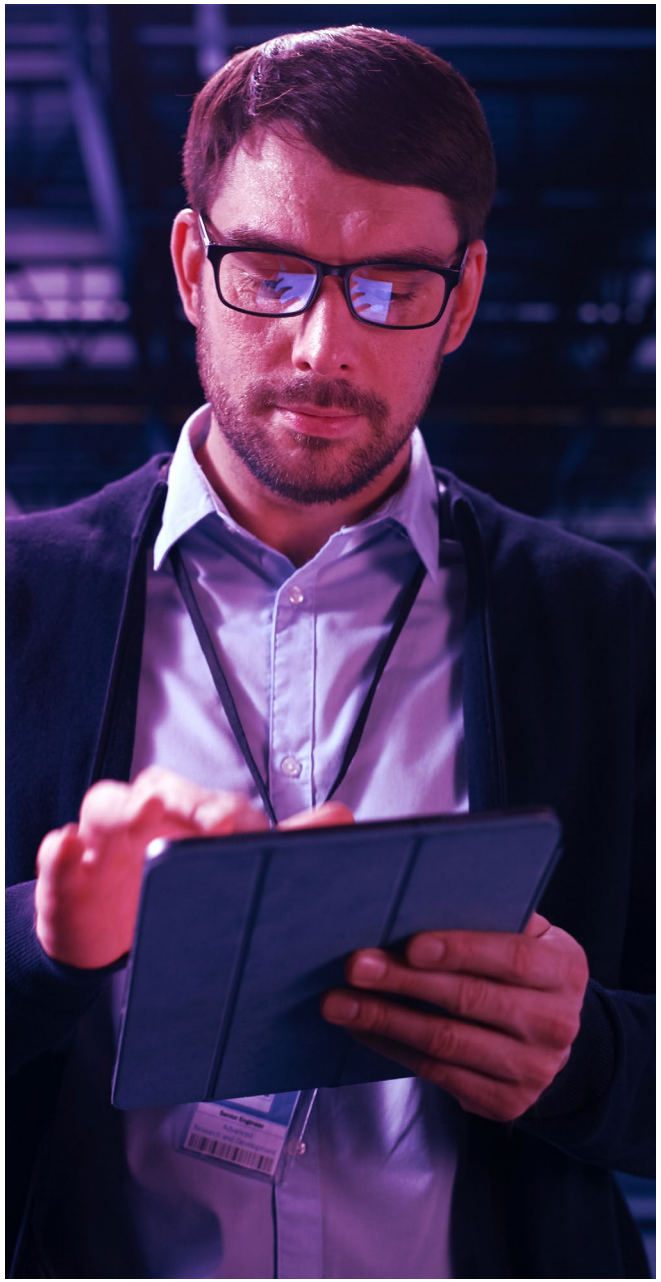
Organisations must conduct their own risk assessments and implement measures to secure their services and protect information.

Reporting incidents

Organisations must report incidents that could significantly disrupt essential services to the supervisory authority within 24 hours. Cyber incidents also need to be reported to the Computer Security Incident Response Team (CSIRT). Factors such as the duration of the disruption, the number of people affected, and potential financial losses determine whether an incident needs to be reported.

Supervision

Organisations must adhere to stringent supervision obligations, including regular assessments of their cybersecurity measures and risk management practices. They are also required to cooperate with relevant authorities and provide timely updates on significant incidents or changes affecting their security.



What if you don't comply?

Once NIS2 is transposed into law in your country, all organisations within the specified categories and special cases must comply. Depending on the organisation's classification, compliance checks may be conducted proactively or reactively.

Fines:

If an organisation fails to comply with NIS2, the supervising authority can impose a fine following an inspection. Each member state sets its own fine amounts, but the maximum fines are:

- **For essential organisations:** Up to 10 million euros or 2% of global annual turnover
- **For important organisations:** Up to 7 million euros or 1.4% of global annual turnover

Joint and Several Liability:

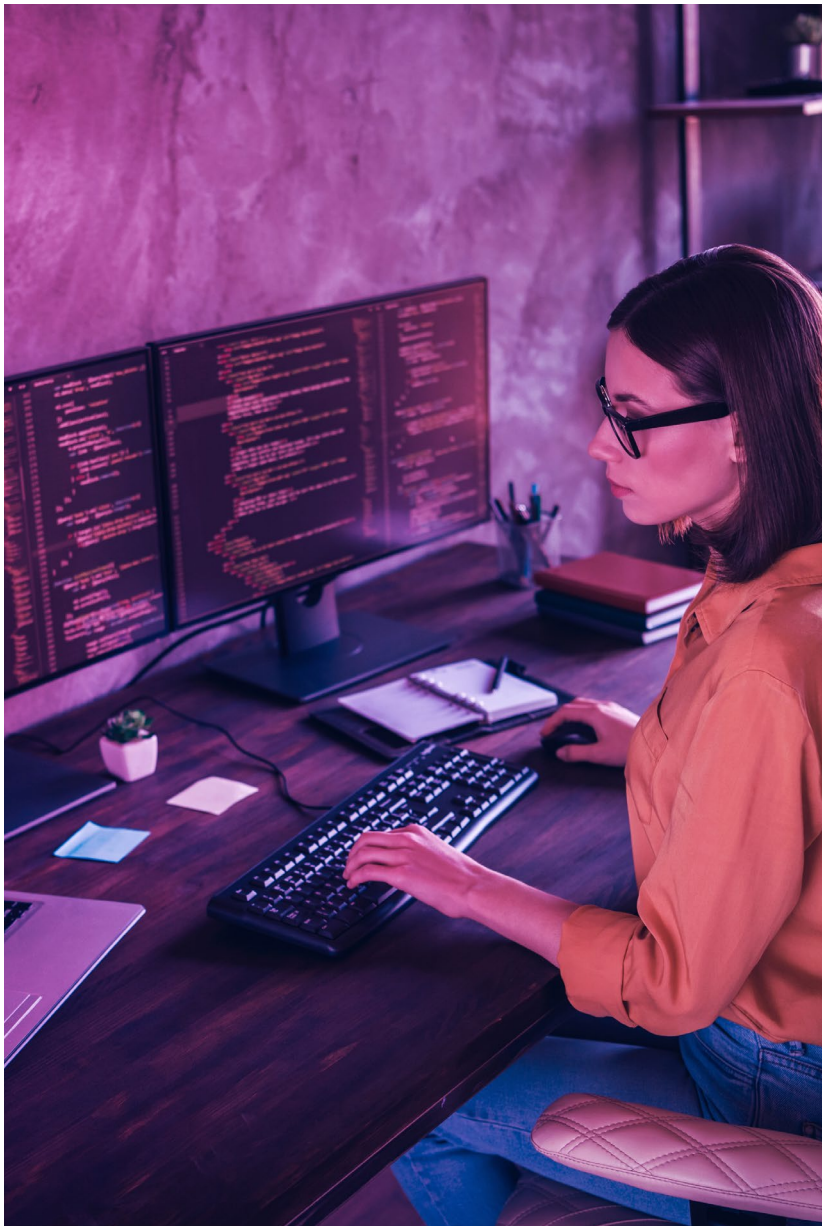
Each director is personally responsible for ensuring their organisation complies with NIS2. They cannot transfer this responsibility or blame others for failures.

Minimum NIS2 requirements for cybersecurity risk management

Article 21 of the NIS2 Directive contains a list of cybersecurity risk management measures that essential and important entities must implement to protect their network and information systems.

Minimum NIS2 requirements:

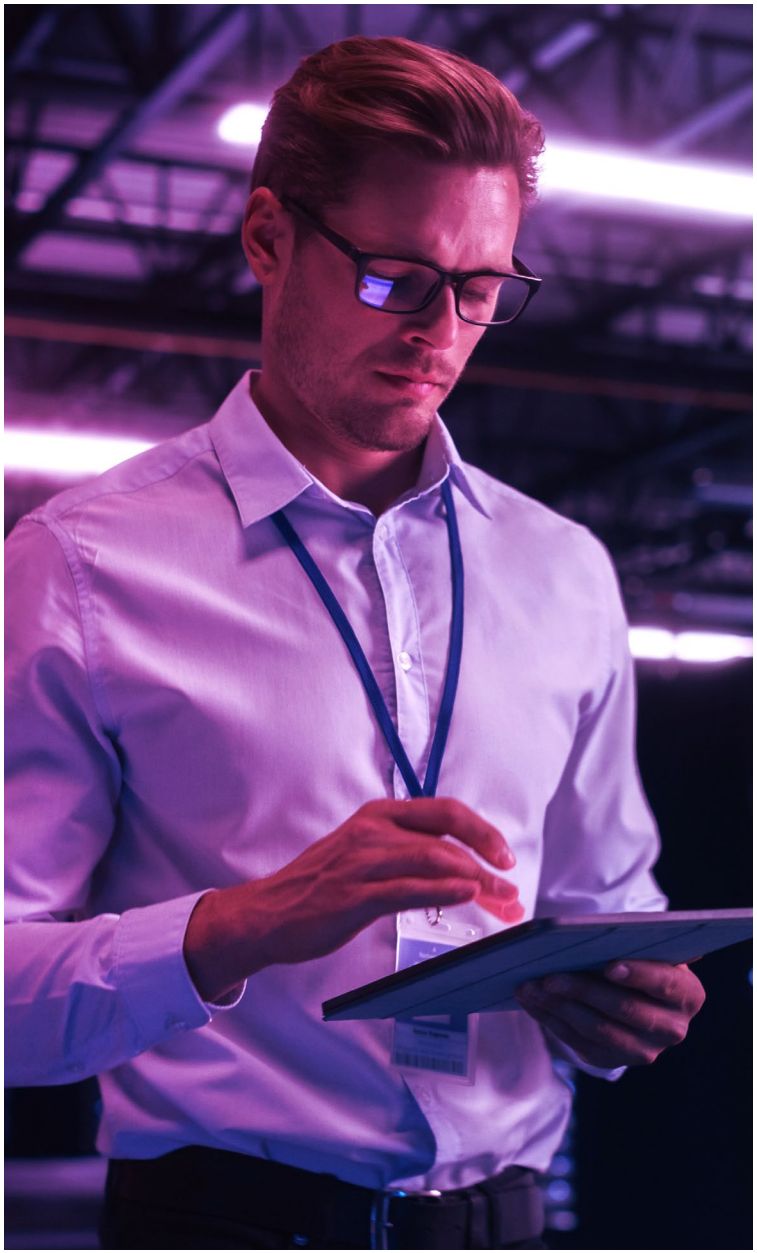
1. **Risk analysis:** Which systems and services are the most vital for your organisation and therefore pose the greatest risk? How is the security of your environment organised?
2. **Business continuity:** What procedures are in place for incident management, including a robust backup system? What crisis management and recovery measures are implemented?
3. **Security of network and information systems:** How are your systems configured, and how are vulnerabilities addressed?
4. **Effectiveness:** How is the effectiveness of your security measures tested? Are there established procedures for this?
5. **Security incident response plan:** How are incidents handled and registered?
6. **Supply chain security:** What potential risks does your organisation face from external suppliers and service providers?
7. **Cybersecurity awareness:** How is your personnel security managed? Is everyone aware of and adhering to the security policy? What staff training is provided?
8. **Cryptography and encryption:** What policies and procedures are in place regarding the use of cryptography and encryption?
9. **Identity and access:** What are the security aspects related to personnel, access policies, and asset management?
10. **Multi-factor authentication:** Is multi-factor authentication implemented for accounts accessible from the internet, those with administrative rights, and essential systems?



Your NIS2 checklist

It's important not to focus solely on the minimum requirements. At Insight, we know that a thorough NIS2 assessment requires more detailed information. The following checklist of 25 items are recommended to ensure full compliance and readiness with NIS2 measures.

No.	Checklist	✓
1.	Access Control	
2.	Situational Awareness	
3.	Configuration Management	
4.	Security Assessment & Internal Audits	
5.	Cryptography	
6.	Personnel Security/Insider Threats	
7.	Identity, Authorisation & Authentication	
8.	Asset Management	
9.	Remote/Offsite Working	
10.	Risk Management	
11.	Information Security Aspects of BCP/BCDR	
12.	Legal & Contractual Requirements	
13.	Compliance & Data Protection	
14.	Incident Management	
15.	Recovery Planning	
16.	Software/ Application Development and Testing	
17.	Physical Security	
18.	Data Classification	
19.	Training & Awareness	
20.	Security Policy, Procedures & Workflows	
21.	Supply Chain Risk Management/ Third-Party Supplier Security	
22.	Vulnerability Management	
23.	Patch Management	
24.	Network & Communications	
25.	Data Leakage Prevention	



How Insight and Microsoft can help you comply with NIS2

At Insight, we understand that preparing for NIS2 is a significant undertaking for many organisations, and we're here to help. If you have any questions about NIS2 or need more information about the measures on our checklist, please don't hesitate to get in touch.

As a Microsoft Solutions Partner across Security, Modern Work, and Azure, Insight brings deep expertise in Microsoft's most advanced tools. We combine this with our proven delivery model - from initial readiness assessments and roadmap planning to deployment, integration, and fully managed security services.

We don't just focus on ticking compliance boxes, we help organisations align NIS2 compliance with broader business goals like improving operational resilience, reducing risk, and optimising costs. Whether you're navigating complex hybrid environments, managing third-party risk, or strengthening incident response capabilities, we ensure your compliance strategy supports long-term agility and growth.

Insight and Microsoft provide an integrated approach to achieving NIS2 compliance. We build on your existing processes and ensure alignment with other EU directives and regulations, making the transition as smooth as possible.

Immediate action

Looking for immediate guidance with your specific situation? Insight offers services such as our NIS2 Awareness Workshop or NIS2 Assessment Service to give you a head start in complying with the upcoming NIS2 regulations. Together, we'll ensure your IT infrastructure is secure and your business data is protected.

Useful links to resources for NIS2:

United Kingdom

(although not directly affected, UK plans to evolve its current NIS regulations)

Government response to the call for views on proposals to improve the UK's cyber resilience - GOV.UK (www. gov.uk)

The Network and Information Systems (NIS) framework aims to enhance the cybersecurity resilience of critical infrastructure | Fieldfisher

Insight

Take the next step

Trust Insight to support you through your journey to meet your NIS2 obligations. We'll provide detailed advice and practical actionable measures your organisation may need to take to prepare your business for NIS2.

Get in touch

Visit our **uk.insight.com** and connect with your Insight account representative to get additional resources and assistance to help you meet your NIS2 obligations.

uk.insight.com

MKT7148