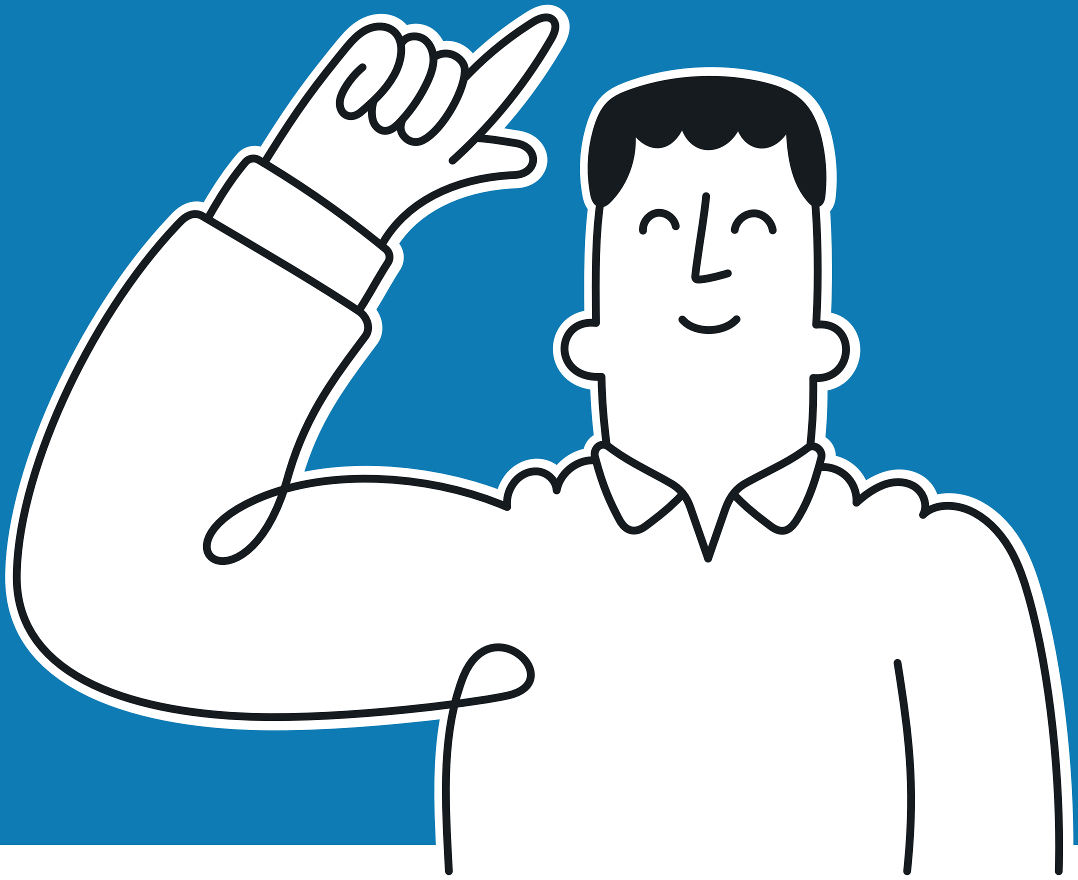
Navigating NIS2

Essential Insights for EU Organisations



MetaCompliance®
Make it personal.

NIS2 in a Nutshell

The NIS2 Directive, also known as the Network and Information Security Directive, is a significant piece of legislation aimed at improving cyber security and protecting critical infrastructure across the European Union (EU). It builds upon the previous NIS Directive, addressing its shortcomings and expanding its scope to enhance security requirements, reporting obligations, and crisis management capabilities. Compliance with the NIS2 Directive is crucial for businesses operating in the EU to safeguard their systems, mitigate cyber threats, and ensure resilience.

Background of the NIS2 Directive

The NIS2 Directive originated as a response to the increasing frequency and sophistication of cyber threats faced by critical infrastructure and essential service providers in Europe. Its development took into account the lessons learned from the implementation of the previous NIS Directive and the need to strengthen cyber security capabilities across member states. The NIS2 Directive aims to create a comprehensive cyber security standard that promotes collaboration, risk management, and preparedness for cyber crises.

Objectives of the NIS2 Directive

The primary objectives of the NIS2 Directive are:

- Enhancing the cyber security and resilience of critical infrastructure and essential service providers.
- Establishing a unified framework for reporting incidents and managing cyber crises.
- Fostering collaboration, knowledge sharing, and peer reviews among EU member states.
- Expanding the scope to cover a wider range of sectors and entities to ensure comprehensive
- protection.
- Strengthening supply chain security and addressing emerging areas of cyber risk.

Who is Affected by the NIS2 Directive?

Entities that fall under the NIS2 framework are divided into two categories: **‘essential’** and **‘important’**.

⚠ Essential Sectors

Threshold

> 250 employees

> 50m € turnover

> 43m € balance

Energy: Power generation companies, electricity transmission operators, and gas suppliers.

Transport: Airports, airlines, railway operators, and maritime ports.

Banking: Banks, credit institutions, and payment service providers.

Financial Markets: Stock exchanges, clearing-houses, and securities trading platforms.

Health: Hospitals, healthcare providers, and medical research institutions.

Drinking Water: Water supply companies and water treatment facilities.

Wastewater: Wastewater treatment plants and sewage management services.

Digital Infrastructure: Internet service providers (ISPs), data centres, and cloud service providers.

ICT Service Management: IT service providers and managed service providers (MSPs).

Public Administration: Government agencies and entities providing essential public services.

Space: Satellite operators and space research organisations.

⚠ Important Sectors

Threshold

50-250 employees

10-50m € turnover

< 43m € balance

Postal and Courier Services: Postal service providers and courier companies.

Waste Management: Waste collection services and waste treatment facilities.

Chemicals: Chemical manufacturing companies and distributors.

Food: Food production and processing companies.

Manufacturing: Industrial manufacturing companies.

Digital Providers: Online platforms, e-commerce websites, and social media networks.

Research Organisations: Scientific research institutions and laboratories.

It's important for organisations falling under these categories to understand their obligations and take appropriate measures to comply with the NIS2 Directive.

It's also worth noting that even if a company does not meet these criteria, it may still choose to comply with the NIS2 Directive to improve its cyber security measures and protect its systems from cyber attacks.

From NIS to NIS2 Directive

Key Changes and Enhancements

The NIS2 Directive builds upon the foundation of the previous NIS Directive and introduces several key changes and enhancements. These include an expanded scope, stricter reporting obligations, a focus on supply chain security, vulnerability management, cyber hygiene, and the introduction of peer reviews for improved collaboration among member states.

Understanding these changes is crucial for organisations to adapt their cyber security practices and comply with the updated requirements.

Key Pillars of the NIS2 Directive

Cyber Crisis Management Structure (CyCLONe)

Cyber Crisis Management Structure (CyCLONe)

The NIS2 Directive builds upon the foundation of the previous NIS Directive and introduces several key changes and enhancements. These include an expanded scope, stricter reporting obligations, a focus on supply chain security, vulnerability management, cyber hygiene, and the introduction of peer reviews for improved collaboration among member states.

Understanding these changes is crucial for organisations to adapt their cyber security practices and comply with the updated requirements.

Stricter Reporting Obligations and Security Framework

The NIS2 Directive introduces stricter reporting obligations for entities, requiring them to promptly report significant cyber incidents to relevant authorities. It also emphasises the implementation of robust security frameworks, risk management practices, incident response procedures, and business continuity planning to enhance cyber resilience.

Supply Chain Security

The directive highlights the importance of assessing and ensuring the security of supply chains. Entities are required to evaluate the security practices of their suppliers and third-party contractors, establish contractual obligations, and implement measures to mitigate risks originating from the supply chain. This focus on supply chain security aims to prevent cyber threats that could potentially infiltrate an organisation through its interconnected network of partners.

Vulnerability Management

The NIS2 Directive emphasises the need for entities to actively manage vulnerabilities in their networks and information systems. This involves conducting regular vulnerability assessments, identifying and addressing vulnerabilities promptly, and implementing effective patch management processes. By proactively managing vulnerabilities, organisations can reduce the risk of exploitation by cybercriminals and enhance the overall security of their systems.

Cyber Hygiene

Ensuring good cyber hygiene practices is a fundamental aspect of the NIS2 Directive. Organisations are encouraged to implement measures such as strong password policies, regular software updates, secure configurations, and employee awareness training. By promoting good cyber hygiene practices, the directive aims to strengthen the overall security posture of organisations and reduce the likelihood of successful cyber attacks.

Core Internet Infrastructure

The NIS2 Directive acknowledges the criticality of core internet infrastructure in maintaining the stability and security of digital services. By focusing on the security of core internet infrastructure, the directive aims to safeguard the integrity and availability of online services.

Peer Reviews for Collaboration and Knowledge Sharing

The NIS2 Directive promotes collaboration and knowledge sharing among member states through the introduction of peer reviews. These reviews facilitate the assessment of cyber security strategies, practices, and capabilities of different countries, enabling the exchange of best practices and the identification of areas for improvement.

Inclusion of More Sectors and Industries

One of the significant changes in the NIS2 Directive is the expansion of its scope to include more sectors and industries. This ensures that a broader range of critical infrastructure and essential services are protected. The directive covers sectors such as energy, transportation, banking, financial markets, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration, space, and more.

Objectives of the NIS2 Directive

The NIS2 Directive sets out several requirements that entities must fulfil to ensure compliance. These requirements include:

- Developing and implementing cyber security policies and risk management practices.
- Establishing incident management procedures, including reporting obligations and response plans.
- Conducting business continuity planning to ensure the continuity of critical services in the event of a cyber incident.
- Implementing supply chain security measures to assess and ensure the security of third-party suppliers.
- Providing training and awareness programs to employees to promote cyber security best practices.
- Implementing asset management practices to identify and protect critical information systems and assets.
- Fulfilling reporting obligations to relevant authorities and maintaining incident response capabilities.

Benefits of Implementing the NIS2 Directive

Risk Management and Mitigation

Implementing the NIS2 Directive's requirements enables organisations to proactively identify, assess, and manage cyber risks. By implementing robust risk management practices, entities can minimise the likelihood of cyber attacks, protect their systems and data, and safeguard their operations and reputation.

Improved Incident Response and Recovery

The NIS2 Directive emphasises the establishment of incident management procedures. By developing effective incident response plans and reporting obligations, entities can respond swiftly and effectively to cyber incidents. This minimises the impact, reduces downtime, and enables faster recovery.

Enhanced Business Continuity

The NIS2 Directive's focus on continuity planning ensures that entities are well-prepared to handle cyber incidents and maintain the continuity of critical services. By implementing robust backup and recovery procedures, redundant systems, and contingency measures, organisations can mitigate the impact of incidents and minimise disruptions to their operations.

Enhanced Business Continuity

The NIS2 Directive's focus on continuity planning ensures that entities are well-prepared to handle cyber incidents and maintain the continuity of critical services. By implementing robust backup and recovery procedures, redundant systems, and contingency measures, organisations can mitigate the impact of incidents and minimise disruptions to their operations.

Strengthened Supply Chain Security

By adhering to the supply chain security measures outlined in the NIS2 Directive, entities can ensure the security of their supply chains. This includes assessing the security practices of third-party suppliers, establishing contractual obligations, and monitoring the security posture of partners. Strengthening supply chain security reduces the risk of cyber attacks originating from the supply chain.

Efficiency and Productivity Gains

Implementing the NIS2 Directive's cyber security measures can lead to improved efficiency and productivity. By streamlining cyber security processes, implementing appropriate controls, and fostering a culture of security, organisations can reduce the administrative burden associated with managing their information systems. This results in cost savings and allows businesses to focus on their core activities.

Understanding the Consequences of Non-Compliance

Non-compliance with the NIS2 Directive can result in significant fines and penalties. Entities that fail to fulfil their obligations may face financial sanctions imposed by the competent national authorities.

The fines for non-compliance can be substantial, with the possibility of reaching up to €10 million or 2% of the entity's global turnover, whichever is higher, for essential entities.

For important entities, the fines can go up to €7 million or 1.4% of the global turnover, whichever is higher. It is crucial for organisations to take compliance seriously to avoid these penalties and protect their reputation.

In addition to financial penalties, national authorities have the power to impose other measures and sanctions for non-compliance with the NIS2 Directive. These measures can include orders to suspend or restrict an entity's activities to protect the security of networks and information systems. It is important for organisations to be aware of the potential consequences of non-compliance and take the necessary steps to meet the requirements of the directive.

Six Steps to Ensure NIS2 Compliance by 2024

Compliance with the NIS2 Directive not only helps organisations meet regulatory obligations but also provides tangible benefits in terms of cyber security readiness, incident response capabilities, and overall resilience. To become NIS2 compliant by the deadline of October 17, 2024, organisations can follow these steps:

1. Assess how the NIS2 Directive impacts their operations and determine if they fall under the scope of the directive.

2. Identify compliance partners or cyber security experts who can provide guidance and support throughout the implementation process.

3. Conduct a thorough gap analysis to identify areas where the organisation's current cyber security practices fall short of the NIS2 requirements.

4. Create awareness among the board and relevant stakeholders about the NIS2 Directive and develop a comprehensive plan for implementing the missing requirements.

5. Allocate appropriate budgets and resources to support the implementation project.

6. Implement the necessary measures, strategies, and routines to ensure compliance with the NIS2 Directive. This may include revising policies, improving incident response capabilities, enhancing supply chain security, and providing training to employees.

Take a Proactive Step Towards a More Secure and Resilient Future

The NIS2 Directive plays a crucial role in enhancing cyber security and resilience across the EU. By understanding the requirements and taking proactive steps to comply with the directive, organisations can protect their systems, mitigate cyber risks, and ensure the continuity of critical services.

We understand the challenges that businesses will face in complying with NIS2. We take a proactive approach to cyber security and support organisations to meet their compliance requirements with cyber security awareness initiatives.

To learn how MetaCompliance can help to implement a best practice Security Awareness Training program and improve cyber security behaviours in your organisation, schedule a complimentary consultation with our cyber security specialists at **https://www.metacompliance.com/nis2-directive**.