Whitepaper

NIS2 – EU Directive on Network and Information Security

A Guide to NIS2 Compliance and Enhanced Cyber Resilience

Table of **contents**

Executive Summary

A Guide to NIS2 Compliance and Enhanced Cyber Resilience

The NIS2 Directive raises the bar for cybersecurity across the EU, extending statutory obligations to a wider range of organizations than its predecessor. Essential and important entities now need to meet clear risk-management requirements, defined incident-reporting timelines, and closer involvement from management in overseeing cybersecurity.

For most organizations, the best approach to meet these requirements is an ongoing process rather than a single project, touching governance, supply chain contracts, technical controls, and staff training alike. Organizations that use this as an opportunity to mature their overall security posture are well placed to turn a regulatory requirement into lasting resilience, and a genuine competitive advantage.

This whitepaper outlines who falls under NIS2, what the Directive requires, and DEKRA's perspective on how organizations can approach these requirements with confidence.

Introduction:
A New Era of Cybersecurity Obligations

The revised EU Directive on Network and Information Security (NIS2) represents a significant advancement in the European Union's cybersecurity strategy. The directive aims to strengthen the cyber resilience of critical sectors across the EU in response to the growing frequency and sophistication of cyber threats.

NIS2 focuses on essential and important sectors that underpin society, the economy, and public services. Many of these sectors operate critical infrastructure, making it essential for organizations to adopt a strong cybersecurity mindset and foster a culture of cyber hygiene. To achieve this, organizations covered by the directive are required to implement robust incident reporting procedures, strengthen risk management practices, and ensure the security of their supply chains. This includes taking responsibility for preventing insecure products and services from introducing vulnerabilities that could be exploited to compromise critical systems.

The directive also establishes a comprehensive enforcement framework, including substantial penalties for non-compliance, emphasizing the importance of proactive cybersecurity governance. This white paper provides an overview of the key principles and requirements of the NIS2 Directive and outlines a strategic approach to achieving, maintaining, and demonstrating compliance.

Expanded Scope:
Who Falls Under NIS2?

A central objective of the NIS2 Directive is the expansion of its scope of application. The previous distinction between operators of essential services and digital service providers is eliminated. The Directive categorizes affected entities into two main types:

- **Essential entities:**
  Sectors that are critical to society and the economy, e.g. energy, transport, banking,financial market infrastructures, healthcare, drinking water, wastewater, digital infrastructure, and space.

- **Important entities:**
  Further key areas such as postal and courier services, waste management, manufacturing/production of goods, chemical industry, food production and distribution, as well as certain research and digital sectors.

Classification is determined by sector and company size, as well as by legally defined exceptions. In many cases, medium-sized and large companies are primarily covered (typically from 50 employees or €10 million in annual turnover or balance sheet total). Depending on the type of entity, however, applicability may also extend beyond classic threshold values.

Decisive are the specific definitions and classifications in each member state's transposition laws, as well as the associated obligations (e.g. registration and reporting to competent national authorities).

The Core of Compliance:
Key Management Measures

The NIS2 Directive concretizes cybersecurity risk management requirements at their core. Affected entities must implement technical and organizational measures that are appropriate and proportionate to the risk. These measures reflect the minimum cybersecurity risk management requirements set out in Article 21 of the NIS2 Directive. They include in particular:

1 **Policies for risk analysis and information systems security:**
Implementation of formal processes for identifying, assessing and mitigating risks.

2 **Incident handling:**
Establishment of robust procedures for the detection, response to, and recovery from security incidents.

3 **Business continuity and crisis management:**
Ensuring operational capability through effective backup strategies, disaster recovery plans, and crisis management protocols.

4 **Supply chain security:**
Management of cybersecurity risks within the supply chain and in relationships with service providers.

5 **Vulnerability management:**
Implementation of processes for handling and disclosing vulnerabilities in systems.

6 **Effectiveness assessment:**
Regular testing and assessment of the effectiveness of cybersecurity measures.

7 **Cyber hygiene and training:**
Promotion of basic security practices and regular employee training.

8 **Cryptography:**
Use of encryption and cryptographic controls where necessary to protect data.

9 **Personnel security:**
Application of policies for access control and secure asset management.

10 **Multi-factor authentication (MFA) and secure communications:**
Use of MFA and protection of internal communications.

Reporting Obligations and Management Responsibility

The NIS2 Directive provides strict and timely reporting obligations. Essential and important entities must report significant security incidents to the competent national authorities designated by each member state. Reporting is generally carried out in stages: an early warning within 24 hours of becoming aware of the incident, followed by a notification within 72 hours including an initial assessment (including severity and impact). Interim reports may be required where applicable. A final report must generally be submitted within one month*.

The requirements establish clear accountability for management. Top management (C-level executives) must not only approve cybersecurity risk management measures but also actively oversee and ensure their effective implementation across the organization. Under the NIS2 Directive, senior management may be held personally accountable if they fail to provide the necessary leadership, governance, and strategic direction to ensure compliance with its requirements. Management is also responsible for fostering a strong cybersecurity culture by ensuring that personnel receive appropriate cybersecurity awareness and training. Furthermore, members of top management are required to participate regularly in cybersecurity training themselves to maintain an up-to-date understanding of cybersecurity risks and to effectively fulfill their governance and risk management responsibilities.

Failure to comply with these obligations may result in significant enforcement measures, including administrative sanctions and substantial financial penalties, as provided for under the national laws implementing the NIS2 Directive in each EU Member State.

* Note: exact timelines may vary by member state.

Substantial Penalties for Non-Compliance

The financial consequences of failing to comply with the requirements of the NIS2 Directive are considerable. The Directive mandates that member states provide fines, depending on whether the entity is classified as essential or important and on the specific violation, of up to €10 million or 2% of total global annual turnover for essential entities, and up to €7 million or 1.4% of turnover for important entities, whichever is higher. In addition to fines, supervisory authorities may impose corrective measures such as binding instructions, security audits, or compliance orders*.

* Note: exact fine amounts and enforcement mechanisms are defined by each member state's national transposition law.

Information Technology vs Operational Technology

Information Technology (IT) primarily focuses on protecting information systems used within office and enterprise environments. The objective is to ensure the confidentiality, integrity, and availability of information. ISO 27001 supports this through organizational policies, risk management, and information security controls.

Operational Technology (OT), on the other hand, consists of the hardware and software that monitor and control physical processes. OT is responsible for operating equipment and infrastructure that directly affects the physical world. Examples range from smart building systems and connected lighting, such as Philips Hue, to electricity grids, water treatment plants, transportation networks, and industrial manufacturing facilities.

Unlike IT systems, OT environments frequently operate remotely and often without direct human intervention. A cyberattack against an IT system may disrupt business operations; however, a successful attack against an OT system can interrupt essential services, damage equipment, create environmental hazards, or endanger human safety. For example, shutting down a corporate email server is inconvenient, but shutting down part of a national power grid could have widespread societal consequences. Consequently, OT cybersecurity places greater emphasis on safety, resilience, continuous availability, and secure operational processes. Standards like IEC 62443 supports to make sure the OT environments are operated and designed safe.

DEKRA's Perspective:
From Compliance to Competitive Advantage

Many organizations approach NIS2 as a standalone regulatory compliance exercise, separate from their existing information security or industrial cybersecurity management practices. In our experience, integrating these frameworks delivers significantly greater value. NIS2, ISO/IEC 27001, and IEC 62443-2-1 address the same underlying objective the systematic management of cybersecurity risk, but from complementary perspectives.

NIS2 establishes mandatory cybersecurity, governance, and incident reporting obligations for essential and important entities. ISO/IEC 27001 provides a management system framework for protecting information assets across enterprise IT environments, while IEC 62443-2-1 defines the requirements for establishing, implementing, maintaining, and continually improving an cybersecurity management system for asset owners/operators. Together, these frameworks provide a comprehensive approach to securing both Information Technology (IT) and Operational Technology (OT) environments.

These are the areas where organizations most often find room to strengthen their approach:

- **Involving management more directly:** Oversight of cybersecurity risk is active and demonstrable, not just approved on paper.
- **Extending visibility into the supply chain:** Most organizations map their own controls well, but have less visibility into their suppliers', even though supply chain security is an explicit NIS2 requirement.
- **Testing incident response plans regularly:** The 24-hour early-warning obligation can be met in practice, not just on paper.

DEKRA's Approach:

Organizations with an established ISO/IEC 27001-certified Information Security Management System (ISMS) and, where applicable, an IEC 62443-2-1-compliant IACS Security Management System (CSMS) are generally well positioned to meet many of the governance, risk management, and security requirements introduced by NIS2 for both the IT and OT counterparts.

Strategic Recommendations for Implementation

Achieving NIS2 compliance requires a strategic, company-wide effort. The key steps include:

- **Conduct a gap IT/OT analysis:** Conduct a thorough assessment of your current security posture against the requirements of the NIS2 Directive.
- **Strengthen your foundation:** Focus on measures that create a stable basis for the resilience of your organization. This enables you to effectively protect your company against unauthorized access and potential attacks.
- **Review your supply chain contracts:** Ensure that contracts with suppliers explicitly address cybersecurity responsibilities and incident reporting certification for IEC 62443-2-1/IEC 62443-2-4 can support in this.
- **Train and empower senior management:** Raise awareness among upper management of their legal responsibilities under NIS2.
- **Test your plans:** Regularly test incident response and business continuity plans through simulations.

How DEKRA Can Support You

DEKRA offers expertise and solutions to support organizations navigate the requirements of the NIS2 Directive. Our services are designed to build resilience from the ground up.

Our services:

- Gap analyses and risk assessments.
- Assistance in developing robust incident response and business continuity plans to ensure the rapid recovery of critical business processes in an emergency.
- Targeted training for technical staff and senior management.
- Training based on OT standards.
- Evaluation and certification for OT IEC 62443 standards (IEC 62443-2-1, IEC 62443-2-4 & IEC 62443-3-3).

Conclusion:
From Compliance to Resilience

The NIS2 Directive is more than a regulatory hurdle; it is a blueprint for building a more secure and resilient organization. By viewing these requirements as an opportunity to strengthen your cybersecurity foundation, you not only reduce the risk of financial penalties, but also significantly improve your ability to repel cyberattacks and recover from them. In doing so, you protect your operations, your reputation, and your customers.

Would you like more information?

Contact Us!

Disclaimer: This document explains the requirements of the EU NIS2 Directive (Directive (EU) 2022/2555). NIS2 is an EU Directive that each member state transposes into its own national law. Implementation details, including competent authorities, reporting timelines, fines, and specific obligations, may vary by member state. Organizations operating in multiple EU countries should consult the transposition laws of each relevant jurisdiction.

July 2026

DEKRA

dekra.com

DEKRA SE