CYBERSECURITY FOR BUILDING CONTROLS

NIS2 Overview

Contents

1. Purpose of the Document

This document summarizes the **Network and Information Security Directive** EU 2022/2555, (NIS2) effective 18 October 2024. The regulation sets new cybersecurity requirements to help essential sectors and industries in the EU maintain business continuity.

1.1. National Cybersecurity Frameworks

The NIS2 Directive mandates that EU member states establish cybersecurity risk management requirements at the national level for critical sectors, including digital infrastructure, energy, transport, and healthcare. Due to their cross-border significance, several subsectors within digital infrastructure and ICT service management are subject to requirements established at the European Union level. To address this, the European Commission issued Implementing Regulation (EU) 2024/2690 on 17 October 2024, detailing the technical and methodological standards for measures outlined in Article 21(2) of Directive (EU) 2022/2555.

EU Member States must adopt a national cybersecurity strategy with clear objectives, governance structures, and risk assessments.

Designation of competent authorities, single points of contact, and CSIRTs (Computer Security Incident Response Teams) is mandatory.

2. What are the Objectives of NIS2

NIS2 policy aims to increase the cyber resilience of critical infrastructures and key companies across the EU. It requires certain companies and organizations to take comprehensive measures to protect their networks and IT systems.

3. Affected Sectors and Industries

The NIS2 Directive is relevant to companies in the EU that provide essential or important services and meet certain size criteria. It's designed to enhance cybersecurity across various sectors and increase resilience to cyberattacks.

3.1. Sectors and Industries:

In addition to the sectors already covered by NIS 1 - energy, transport, healthcare, finance, water management, and digital infrastructure - the new rules also apply to providers of public electronic communications, more digital services (such as social platforms), waste and wastewater management, critical product.

Critical Infrastructure Operators (KRITIS): These are companies in sectors like energy, transport, healthcare, digital infrastructure, and finance.

Essential Entities: These are organization and companies that provide services critical to society and the economy, even if not strictly part of critical infrastructure. These include:

- Energy
- Transport
- Health
- Water supply

- Digital infrastructure (e.g. cloud providers, DNS services)
- Public administration

Important Entities: These entities provide services that are important but not considered critical. These include:

- Postal services
- Waste management
- Chemicals
- Food production
- Manufacturing of medical devices
- Digital providers (e.g. social networks, search engines)

3.2. Size Criteria:

Mid-size and large companies from the following sectors must comply with NIS2: energy; transport; banking; financial market infrastructures; health; drinking water; wastewater; digital infrastructure; ICT service management (business-to-business); public administration; space; postal and courier services; waste.

- **Medium-sized companies:** Generally, companies with 50 or more employees and an annual turnover or balance sheet total exceeding 10 million euros are affected.
- **Large companies:** These are companies with 250 or more employees or with a turnover and balance sheet that exceeds specified thresholds (e.g., 50 million euros in turnover or 43 million euros in assets).
- **Special Cases:** Some companies, regardless of size, may be considered essential due to the nature of their services or activities.

4. What does NIS2 Compliance Require?

4.1. Defined a Network and Information System Security Policy

NIS 2 establishes clear accountability for cybersecurity compliance and reporting at the senior management level. The Act mandates robust governance, transparency, and comprehensive documentation to demonstrate ongoing adherence.

Organizations must adopt an all-hazards approach to safeguard networks, information systems, and their physical environments from potential incidents. A comprehensive network and information systems security policy should be implemented, encompassing all relevant systems, assets, and procedures. At a minimum, the policy should address:

- Risk analysis and information security policies;
- Incident response protocols;
- Business continuity planning, including backup and disaster recovery as well as crisis management;
- Supply chain security measures, covering the security aspects of relationships with direct suppliers and service providers;

- Security in the acquisition, development, and maintenance of network and information systems, including vulnerability management and disclosure processes;
- Procedures for evaluating the effectiveness of cybersecurity risk management strategies;
- Fundamental cyber hygiene practices and structured cybersecurity training programs;
- Policies governing the use of cryptography and, where appropriate, encryption technologies;
- Human resources security measures, access control frameworks, and asset management protocols;
- Where applicable, deployment of multi-factor or continuous authentication, secure communication channels (voice, video, and text), and protected emergency communications within the organization.

Comprehensive IT documentation should be established or updated, providing a clear overview of IT infrastructure, including network topologies, servers, client devices, applications, and user permissions.

It is essential that all relevant staff members and external parties (such as suppliers and service providers) formally acknowledge this policy, typically through signed or digital confirmation, which can be integrated into existing contractual agreements. The policy should be communicated in a clear and accessible format tailored to its audience, and only the relevant sections should be shared to prevent the unintended disclosure of confidential information.

4.2. Rick Management Framework

Relevant entities must establish and maintain a comprehensive risk management framework to systematically identify and address threats to the security of their network and information systems. These entities are required to conduct thorough risk assessments, document outcomes, and based on these findings, develop, implement, and monitor a robust risk treatment plan. Assessment results and any residual risks should be reviewed and formally accepted by governing bodies or individuals delegated with appropriate responsibilities and authority, ensuring that proper reporting to management occurs as necessary.

Entities may leverage an existing risk management framework or adopt a new one. A risk management framework offers a structured methodology for identifying, assessing, managing, and mitigating cybersecurity risks.

A risk treatment plan should be formulated to link identified risks to corresponding assets and specify the measures implemented to address those risks. At minimum, the plan must include:

- A description of each identified risk and its potential impact on security objectives;
- The selected risk treatment option (e.g., avoidance, mitigation, transfer, sharing, or acceptance);
- The relevant assets associated with each risk;
- Measures intended to mitigate each risk;
- Procedures for evaluating the effectiveness of these measures;
- Implementation timelines; and
- Assignment of responsible roles.

It is also essential to consider residual risks originating from third parties, such as data breaches, unresolved vulnerabilities, regulatory non-compliance, or excessive dependence on individual vendors.

Residual risks should be accepted by management bodies, or where applicable, by accountable individuals authorized to manage such risks in line with the entity's defined levels of acceptable residual risk. Additionally, approval for risk assessment results and the risk treatment plan must be obtained from the designated management bodies or accountable persons.

4.3. Reporting Obligation

Essential entities must promptly notify affected service recipients of significant cyber threats and any actions they can take in response. Where suitable, they should also disclose details of the threat. An incident is considered significant if it causes, or could cause, major disruption or financial loss to the entity, or considerable harm—material or non-material—to others.

Essential entities must notify the relevant authority of significant incidents as follows:

a) Provide an early warning within 24 hours of discovery, specifying if the incident may be unlawful, malicious, or have cross-border effects.

b) Submit a full incident notification within 72 hours, updating earlier information and including an initial assessment of severity, impact, and any known indicators of compromise.

5. Key Takeaways:

The NIS2 Directive (Directive (EU) 2022/2555) is the European Union's updated framework for cybersecurity, replacing the original NIS Directive. It aims to strengthen the overall level of cybersecurity across the EU by expanding the scope of regulated sectors, increasing accountability, and enforcing stricter risk management and reporting obligations.

5.1. Expanded Scope of Application

NIS2 applies to a broader range of sectors than its predecessor, including:

- Energy, transport, banking, health, and digital infrastructure.
- ICT product manufacturers
- Organizations are classified as "essential" or "important" based on size and sector, with thresholds defined by employee count and turnover

5.2. Mandatory Cybersecurity Risk Management

Organizations must implement:

- Technical and organizational measures to manage cybersecurity risks.
- Policies for incident handling, business continuity, and supply chain security.
- Alignment with standards like ISO/IEC 27001 is encouraged, though not mandatory

5.3. Stricter Reporting Obligations

- Incidents must be reported within 24 hours of becoming aware.
- Reports must include impact assessments and mitigation steps
- National CSIRTs (Computer Security Incident Response Teams) and competent authorities must be notified

5.4. Governance and Accountability

- Senior management is directly accountable for compliance.
- Non-compliance can lead to fines up to €10 million or 2% of global turnover for essential entities
- CEOs and legal representatives may face temporary bans from managerial roles in severe cases

5.5. Supply Chain and Third-Party Risk

- Organizations must assess and manage cybersecurity risks in their supply chains.
- This includes ensuring that third-party vendors and service providers meet NIS2 standards

6. Timeline

- Member States must transpose the directive by **17 October 2024**.
- Measures apply from **18 October 2024**.
- ENISA and the Commission will review implementation every **36 months** (Article 40).