EU NIS2 Directive

Network and Information Security Requirements for Critical Infrastructure

OT Security Learning Series

Document 140 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

The NIS2 Directive (Directive (EU) 2022/2555) is the European Union's updated cybersecurity legislation that significantly expands requirements for operators of critical infrastructure, including industrial and OT environments. It replaces the original NIS Directive from 2016 and introduces stricter security obligations, broader scope, and substantial penalties for non-compliance.

The Network and Information Security Directive 2 (NIS2) represents a major evolution in EU cybersecurity regulation. As cyber threats to critical infrastructure have increased in sophistication and frequency, the EU recognized the need to strengthen and harmonize cybersecurity requirements across member states.

For organizations operating OT and industrial control systems, NIS2 introduces specific obligations that directly impact how these environments must be secured, monitored, and reported upon.

2 Evolution from NIS1

The original NIS Directive (2016) was the EU's first comprehensive cybersecurity legislation. However, implementation varied significantly across member states, creating an uneven security landscape.

Aspect	NIS1 (2016)	NIS2 (2022)
Scope	7 sectors	18 sectors
Entity classification	OES and DSP	Essential and Important
Incident reporting	72 hours (varied)	24h early warning, 72h notification
Penalties	Member state discretion	Up to €10M or 2% turnover
Supply chain	Limited coverage	Explicit requirements
Management liability	Not specified	Personal accountability

Table 1: Key differences between NIS1 and NIS2

3 Scope and Covered Sectors

NIS2 significantly expands the sectors and entities covered by cybersecurity requirements. Organizations are classified as either **Essential** or **Important** entities based on their sector and size.

3.1 Essential Entities (Annex I)

These sectors face the strictest requirements and supervision:

- **Energy** – Electricity, oil, gas, hydrogen, district heating

- **Transport** – Air, rail, water, road
- **Banking and Financial Market Infrastructure**
- **Health** – Healthcare providers, laboratories, pharmaceuticals
- **Drinking Water and Wastewater**
- **Digital Infrastructure** – IXPs, DNS, TLD registries, cloud, data centers
- **Public Administration**
- **Space**

3.2 Important Entities (Annex II)

These sectors have slightly reduced oversight but similar security obligations:

- **Postal and Courier Services**
- **Waste Management**
- **Chemical Manufacturing and Distribution**
- **Food Production and Distribution**
- **Manufacturing** – Medical devices, machinery, motor vehicles, electrical equipment
- **Digital Providers** – Online marketplaces, search engines, social networks
- **Research Organizations**

Warning

Size thresholds apply: Generally, medium-sized enterprises (50+ employees or €10M+ turnover) and large enterprises are in scope. However, some entities are covered regardless of size, including critical infrastructure operators and those providing essential services.

4 Key Security Requirements

NIS2 Article 21 mandates specific cybersecurity risk management measures. These requirements apply directly to OT environments.

4.1 Risk Management Measures

Organizations must implement measures that are **appropriate and proportionate** to the risks, considering:

- State of the art technologies
- Relevant standards (ISO 27001, IEC 62443)

- Cost of implementation
- Likelihood and severity of incidents

4.2 Minimum Security Elements

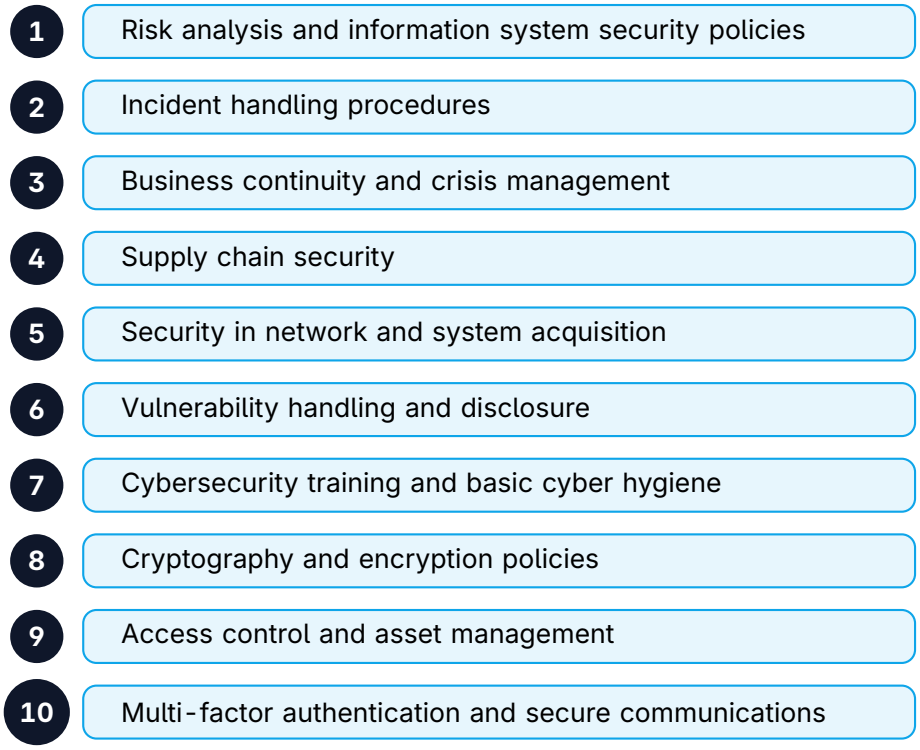

Figure 1: NIS2 Article 21 minimum security measures

5 Incident Reporting Requirements

NIS2 establishes a structured incident reporting framework with strict timelines.

Report Type	Deadline	Content
Early Warning	24 hours	Initial notification of significant incident
Incident Notification	72 hours	Assessment of severity, impact, and indicators of compromise
Intermediate Report	On request	Status update if requested by authority
Final Report	1 month	Root cause, mitigation measures, cross-border impact

Table 2: NIS2 incident reporting timeline

Critical

A **significant incident** is one that has caused or could cause severe operational disruption or financial loss, or has affected or could affect other entities by causing considerable damage. OT incidents affecting safety or physical processes typically meet this threshold.

6 OT and ICS Implications

NIS2 has direct implications for operational technology environments across covered sectors.

6.1 Specific OT Considerations

- **Asset Inventory** – Complete inventory of OT assets is required for risk management
- **Network Segmentation** – Separation between IT and OT networks is implicitly required
- **Access Control** – MFA requirements may need adaptation for OT constraints
- **Patch Management** – Vulnerability handling must account for OT patching challenges
- **Monitoring** – Detection capabilities must extend to OT networks
- **Incident Response** – Plans must cover OT-specific scenarios

6.2 Supply Chain Security

NIS2 explicitly addresses supply chain risks, particularly relevant for OT environments:

- Security requirements for suppliers and service providers
- Assessment of supplier cybersecurity practices
- Contractual security obligations
- Monitoring of third-party access to OT systems

Tip

IEC 62443 alignment is valuable for NIS2 compliance in OT environments. The standard's security levels and zone/conduit model provide a framework that supports NIS2's risk-based approach.

7 Management Accountability

NIS2 introduces personal accountability for management bodies, a significant change from NIS1.

7.1 Management Obligations

- **Approve** cybersecurity risk management measures
- **Oversee** implementation of security measures
- **Undertake** cybersecurity training
- **Be held liable** for infringements

Warning

Member states may hold natural persons (executives, board members) personally liable for failures to comply with NIS2 obligations. This extends accountability beyond the organization to individual decision-makers.

8 Enforcement and Penalties

NIS2 establishes harmonized penalty frameworks across the EU.

Aspect	Essential Entities	Important Entities
Maximum fine	€10M or 2% global turnover	€7M or 1.4% global turnover
Supervision	Proactive (ex-ante)	Reactive (ex-post)
Audits	Regular mandatory audits	Audits after incidents

Table 3: NIS2 penalty framework

Additional enforcement measures include:

- Binding instructions and compliance orders
- Public disclosure of non-compliance
- Temporary suspension of certifications
- Temporary management bans for essential entities

9 Implementation Timeline

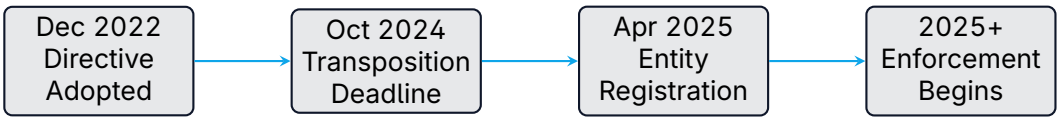

Figure 2: NIS2 implementation timeline

Member states must transpose NIS2 into national law. Organizations should:

1. Determine if they fall within scope
2. Assess current security posture against NIS2 requirements
3. Identify gaps, particularly in OT environments
4. Implement necessary measures before enforcement begins
5. Register with national authorities as required

10 Summary

Key Takeaways

- **Expanded Scope:** NIS2 covers 18 sectors with Essential and Important entity classifications, significantly broadening coverage of industrial operations
- **Stricter Requirements:** Minimum security measures explicitly include risk management, incident handling, supply chain security, and access control
- **Fast Reporting:** 24-hour early warning and 72-hour notification requirements demand prepared incident response capabilities
- **OT Relevance:** Requirements directly impact OT environments including asset management, network security, and vulnerability handling
- **Management Liability:** Personal accountability for executives creates board-level attention to cybersecurity
- **Significant Penalties:** Fines up to €10M or 2% of global turnover, plus potential management bans

11 Further Reading

Official Sources

- **NIS2 Directive Full Text** – Official Journal of the European Union
  https://eur-lex.europa.eu/eli/dir/2022/2555
- **ENISA NIS2 Resources** – European Union Agency for Cybersecurity
  https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Related Standards

- **IEC 62443** – Industrial Automation and Control Systems Security
  https://www.isa.org/standards-and-publications/isa-standards
- **ISO/IEC 27001** – Information Security Management Systems
  https://www.iso.org/standard/27001

Books

- Boehmer – *EU Cybersecurity Regulation and Directive* (Springer)
- Markopoulou et al. – *The New European Cybersecurity Framework* (Kluwer)

Part of the OT Security Learning Series