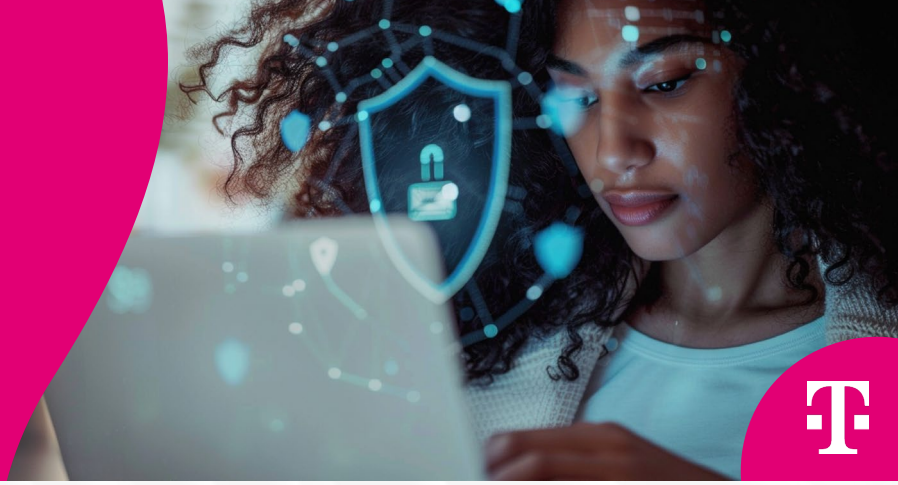
T Security

NIS2 Directive

NIS2 readiness starts with visibility, control, and structured security actions.



What is NIS2 and what is its purpose?

The NIS2 Directive is the European Union's updated cybersecurity framework designed to strengthen resilience across critical industries and digital services. It expands the scope of the original NIS Directive and introduces stricter requirements for risk management, incident reporting, governance, and supply chain security.

For organizations operating in modern, hybrid and cloud-native environments, NIS2 is a clear signal that cybersecurity must now be treated as a business priority, with accountability at both operational and leadership levels.

Who is affected by the NIS2 Directive?

Whether and how companies are affected by the NIS2 Directive depends on their **company size** and their **area of activity.**

Company Size

- Medium organizations with 50+ employees and €10M+ turnover
- Large organizations with 250+ employees and €50M+ turnover

Area of Activity

Sectors of high criticality include areas of activity where disruptions would have a major societal or economic impact:

energy, transportation | banking | financial market infrastructure | health |drinking water | wastewater | digital infrastructure | management of ICT services | public administration | space

Other critical sectors that support broader infrastructure and operations:

Digital Service Providers | Production, processing and distribution of food | Production, processing and distribution of chemicals | Manufacturing / Production of goods | Waste management | Postal and Courier Service | Research Organizations

Organizations that are not directly classified may still be affected through supply chain obligations, as regulated entities increasingly require partners to meet NIS2 aligned security standards.

Why this matters today

NIS2 reflects a shift from basic compliance to business-critical risk management. Organizations are expected to secure complex hybrid environments, manage third-party risks, and respond to incidents within strict timelines. Failure to adapt impacts not only compliance, but also operations, partnership, and market trust.

How compliance is enforced

NIS2 introduces stricter supervision and enforcement across EU member states. Regulators can conduct audits, request risks- and security documentation, and assess how effectively organizations detect and respond to incidents. Authorities may also enforce corrective actions within defined timelines. The supervision process varies by entity type.

Essential entities: Large organizations which operate in a sector with high criticality

Important entities: Large and medium organizations which operate in other critical sectors

Essential entities are subject to proactive oversight, while important entities are typically reviewed after incidents or identified risks.

Penalties and business impact

- Essential entities may face fines **> €10M or 2% of global turnover**
- Important entities may face fines **> €7M or 1.4% of global turnover**

Beyond penalties, organizations risks service disruptions, contract loss and reputational damage.

A practical approach to NIS2 readiness

Achieving NIS2 compliance requires a structured and phased approach aligned with the current environment.

Organizations should start by assessing their current posture, identify gaps, and prioritize high-risk areas such as identity, access, and incident response. This is followed by strengthening controls across systems and users, enabling continuous monitoring, and establishing clear governance and accountability.

Benefits to industries

Risk Management
Definition of security policies and risk assessments across systems and operations

Incident Reporting
Direct report of incidents within strict timelines

Business Continuity
Ensured back-up recovery, and crisis management readiness

Supply Chain Security
Risk management across vendors, partners, and third-party services

Identity and Access Control
Enforcement of strong authentication and user access policies

Vulnerability Management
Continuous identification, patching, and management of system weaknesses

Where organizations struggle

Many organizations face similar challenges when aligning with NIS2:

- Limited visibility across hybrid environments
- Unclear or delayed incident response processes
- Weak identity and access control frameworks
- Limited control over third-party and supply chain risks

These gaps increase both compliance risks and exposure to operational disruptions.

How T Security supports your NIS2 readiness

NIS2 Readiness Assessment
Identify gaps, risks, and compliance priorities across your environment

Secure Infrastructure and Cloud
Build and operate secure, compliant environments aligned with European regulations

Identity and Access Management
Strengthen access controls using zero trust principle

Threat Detection and Response
Enable continuous monitoring, detection and incident response

Compliance and Audit Support
Simplify reporting, governance and audit readiness

Resilience Planning
Establish clear workflows, reporting process, and recovery strategies aligned with NIS2 timelines.

Get in touch with our experts
cyber.security@t-systems.com

Published by
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn, Germany
security.telekom.de
t-systems.com