



WHITE PAPER

Understanding & implementing the NIS2 specifications

NIS2 Directive: Cybersecurity in the EU

Contents

1 What is NIS2?	03
2 What's New With NIS2?	04
2.1 NIS2 affects more industry sectors and organizations	04
2.2 Non-compliance is expensive	04
2.3 Additional measures in NIS2	04
2.4 Management liability for violations	05
Protection against cyber threats – NIS2 requirements at a glance	05
3 Who is Affected by NIS2?	06
4 Mandatory Measures	08
4.1 Strict registration obligation	08
4.2 Obligation to report security incidents	08
5 The Focus of NIS2: Risk Management	09
Which risk management measures are regulated by the NIS2 Directive?	10
6 Using baramundi Solutions for NIS2 Compliance	11
7 Seven Steps to NIS2 Compliance	13



1 What is NIS2?

The number and severity of cybersecurity threats continue to rise globally, including in the EU. Critical infrastructure is a primary target: a single cyberattack on the power grid could simultaneously shut down hospitals, communication systems, and water treatment plants.

From NIS to NIS2

Although the classification of critical infrastructure varies across EU countries, Member States have been working to strengthen cybersecurity in key sectors by defining uniform standards, including the first Network and Information Security (NIS) Directive in 2016. NIS required critical infrastructure organizations -- including those labelled KRITIS in Germany -- to comply with a set of standards for network and system security. The NIS Directive defined common principles and minimum requirements but left implementation to each member state.

Those requirements were expanded under the NIS2 Directive, which took effect on January 16, 2023. EU Member States began enacting corresponding national laws in October 2024, and NIS2 enforcement began in January 2026. Although specific enforcement mechanisms, competent authorities, and reporting procedures vary by country, the core security requirements and risk management obligations are consistent across the EU.¹

Higher Requirements for Companies

From tools and practices that improve the transparency and security of IT infrastructure to specific measures for cyber risk management, most affected companies need to commit additional resources to achieve and maintain NIS2 compliance.

Cybersecurity as a Management Responsibility

In addition, one of the most important aspects of NIS2 is that the regulations affect more people in each organization than just IT specialists. Various senior managers, executives such as the Chief Information Security Officer (CISO), and departments, including operations and finance, share responsibility for ensuring reliable cybersecurity. This effectively makes network and information security an increasingly strategic and corporate cultural issue. Unified Endpoint Management (UEM) solutions directly support NIS2 compliance by automating routine security tasks -- a meaningful advantage for organizations managing complex IT environments with lean teams.

¹ The entire directive can be found at: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555>.

2 What's New With NIS2?

NIS2 significantly strengthens and expands the regulations of the 2016 NIS Directive, particularly in the following core areas:

- 1 Includes more industry sectors and defines „Essential entities“ and „Important entities“
- 2 Increased fines for non-compliance and greater oversight
- 3 Directly involves and holds senior management accountable for compliance
- 4 Increases reporting obligations
- 5 Defines mandatory security measures that companies must implement and document regularly, with an increased focus on risk management

2.1 NIS2 affects more industry sectors and organizations

A significantly larger number of industries must implement mandatory cybersecurity measures. In total, the new directive affects organizations in 11 “Essential” and seven “Important” sectors. A company's classification as Essential or Important depends on its sector and its size (see Chapter 4).

2.2 Non-compliance is expensive

Penalties for non-compliance are substantial. Fines may reach up to 2% of annual global revenue for Essential entities and up to 1.4% for Important entities. While penalties vary by national regulations and the severity, duration, and recurrence of violations, the Directive emphasizes consistent and proportionate enforcement across the EU.

2.3 Additional measures in NIS2

Companies affected by NIS2 must implement broader, more stringent IT security measures, with an emphasis on risk management and supply chain security. Other requirements include regular penetration tests, systems for reporting security incidents, and active measures to secure networks and systems. Organizations are required to report incidents either within their home countries or EU-wide depending on the severity of the incident.

2.4 Management liability for violations



Extremely important:
NIS2 holds management particularly accountable when security standards are violated.

Among the more significant elements of NIS2 are measures that hold senior managers and executives personally liable for security incidents resulting from gross non-compliance or negligence. Managers must monitor the implementation of cybersecurity measures. Managing directors and other executives must undergo regular training in cybersecurity risk management and develop the knowledge and skills needed to ensure their organizations remain compliant and cyber-resilient.

Protection against cyber threats – NIS2 requirements at a glance

- ➔ Guidelines („policies“) for risk management and information security
- ➔ Incident management to prevent, detect and respond to security incidents
- ➔ Business continuity based on backup, disaster recovery, and crisis management
- ➔ Supply chain security and measures for secure procurement of IT and network systems
- ➔ Specifications for assessing and managing cyber risks
- ➔ Specifications for encryption („cryptography“)
- ➔ Access control using multi-factor authentication and single sign-on
- ➔ Measures to secure voice, video and text communication

3 Who is Affected by NIS2?

NIS2 significantly expands the number of industry sectors and organizations subject to its requirements in two primary categories. “Essential entities” are organizations deemed crucial to the functioning of the economy and society. “Important entities” are organizations that operate in high-risk sectors but may have less critical infrastructure than Essential entities.

Include organizations in the energy, transportation, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, information and communication service management, public administration and aerospace industries. They include organizations engaged in postal and courier services, waste management, manufacturing of critical products such as pharmaceuticals, medical devices and industrial goods, chemicals production and distribution, food production, processing, and distribution, digital services, and research and education.

Company size also determines whether an organization is “Essential” or “Important”. NIS2 applies to organizations that are not classified as micro, small, or medium-sized enterprises (SMEs) – typically those with 50 or more employees and annual revenue or assets exceeding €10 million. Smaller companies can also be subject to NIS2 if they are critical to national or EU-level security or operate within key supply chains. Regardless of sector or size, some companies are subject to the regulations if they have NIS2-affected companies as customers or are part of those companies’ supply chains. Affected organizations must conduct regular self-assessments and document compliance. Authorities in each member state may also request documentation during audits or incident reviews.



It’s estimated that more than 100,000 additional companies in Europe are subject to NIS2. The NACE code can be used to determine whether an organization is affected² and which obligations apply. Each organization must maintain an ongoing impact analysis (self-assessment) and regularly update documentation to demonstrate compliance. Authorities may audit documentation at any time, after incidents, or during scheduled reviews.

² More information on NACE codes can be found at: https://ec.europa.eu/competition/mergers/cases/index/nace_all.html

Company-size criteria:

A company can be classified in one of three SME categories based on the number of full-time employees (FTE) and thresholds for annual turnover or assets. Regardless of size, companies can still fall under NIS2 if they are deemed critical to national security or key supply chains.

Company Category	FTE (Annual Work Units)	Annual Turnover	Annual Balance Sheet
Medium-sized	≤ 250	≤ 50 Mil EUR	≤ 43 Mil EUR
Small	≤ 50	≤ 10 Mil EUR	≤ 10 Mil EUR
Micro	≤ 10	≤ 2 Mil EUR	≤ 2 Mil EUR



Example:

An independent company with 49 FTE, annual revenue of €11 million and assets of €9 million may be classified as a small company based on its balance sheet. However, if its total assets reached or exceeded €10 million, it would be considered a medium-sized company and subject to NIS2.

4 Mandatory Measures

NIS2 imposes two core formal obligations on covered organizations: registration with the competent authority and reporting of significant security incidents. Member States specify the precise registration process and deadlines, typically within three months of classification as an Essential or Important entity.

4.1 Strict registration obligation

Affected entities must submit the following information to the competent authority in each country no later than three months after their initial or renewed NIS2 classification: company name, legal form, commercial register number, address, contact details (including email, telephone, and IP address ranges), relevant sector or sub-sector, and a list of EU Member States in which the company operates. Affected entities must register with their designated national authority within three months of being identified as subject to NIS2. Registration includes company details, sector classification, and contact information. Member States maintain their own registration platforms or contact points, and updates to registered data must be reported promptly. Failure to register or late updates are considered administrative offenses under national law.³

4.2 Obligation to report security incidents

Companies affected by NIS2 must promptly notify the appropriate authority of a „significant security incident“ that has caused or could cause serious operational disruptions or financial losses for the affected organization. Reporting is also required if the incident has caused or could cause significant material or other damage to other persons.

Because reporting requirements vary by country, each must be considered independently. NIS2 requires entities to promptly report significant incidents that cause or could cause substantial operational disruption or financial loss, or that could negatively affect other entities. The Directive defines clear stages for incident notifications: an early warning without undue delay and within 24 hours of detection; a detailed incident notification within 72 hours; and a final report no later than one month after the initial alert. Member States provide specific national procedures for each stage. Each Member State specifies the exact timing and procedures in its national implementation law.

³ Each Member State operates its own national cybersecurity incident portal. Contact points are listed on the ENISA website: <https://www.enisa.europa.eu/topics/nis-directive/>. US organizations subject to NIS2 should use the ENISA website as a primary reference.

5 The Focus of NIS2: Risk Management



Risk Management as a Core Requirement

Comprehensive risk management is at the heart of the new NIS2 directive. In general, NIS2 requirements stipulate that risk management measures align with the latest applicable standards, the extent of risk exposure, the size of the organization, and the probability and severity of security incidents. They must also consider potential social and economic impacts. Organizations that fail to implement risk management measures, implement them incorrectly, or do not do so in a timely manner are in breach of NIS2 regulations.



Putting NIS2 Requirements into Practice

At many companies, NIS2 implementation initially requires a range of technical and organizational measures. NIS2 also emphasizes cyber hygiene and incident prevention practices. While no single tool fully addresses all NIS2 requirements, most companies already use a range of IT security solutions to achieve compliance. These include solutions for network access control and monitoring, and UEM.



Creating Transparency Through Asset Management

Automated tools in a UEM system can help companies efficiently comply with a wide range of NIS2 requirements, beginning with a comprehensive inventory of hardware and software. It is important to account for all device types, including servers, network devices, desktop and laptop computers, and mobile devices. Hardware and Software Asset Management forms the basis for meeting NIS2 requirements such as transparency, risk analysis and general information security.



Strengthening Cyber Hygiene with UEM

UEM capabilities also include valuable tools for automated and reliable endpoint maintenance and protection including vulnerability and update management, disk encryption, allow or block listing of software, and a ticketing system for rapid problem resolution.

Which risk management measures are regulated by the NIS2 Directive?

- | | | | |
|----------|--|-----------|--|
| 1 | Policies:
Introduction of guidelines for risk management and implementation of information security measures | 8 | Personnel:
Protection of human resources data |
| 2 | Incident management:
Detection and management of security incidents | 9 | Asset management:
Information security management system (ISMS) rules, procedures, methods, and tools aligned with ISO 27001 |
| 3 | Business continuity:
Backup management, disaster recovery and crisis management | 10 | Access control:
Monitoring and logging of network access activity |
| 4 | Supply chain:
Measures to secure procurement, maintenance and operation of IT and network systems | 11 | Authentication:
Use of multi-factor authentication (MFA) and single sign-on (SSO) |
| 5 | Effectiveness:
Specifications for assessing cyber risks and implementing appropriate measures | 12 | Communication:
Encryption for voice, video and text communication |
| 6 | Training courses:
Regular cybersecurity training for executives and employees | 13 | Emergency response:
Use of secure emergency communication systems |
| 7 | Data security:
Specifications for encryption in all key areas | | |

6 Using baramundi Solutions for NIS2 Compliance

The baramundi Management Suite provides comprehensive UEM capabilities that IT teams can use to address the following areas of the NIS2 directive:



Article 21 Risk management measures in the area of cybersecurity

Member States shall ensure that [...] entities take appropriate [...] measures to manage the risks to the security of network and information systems [...] and to minimize the impact of security incidents [...].

a)

Concepts related to risk analysis and security for information systems.

- **Vulnerability Scanner:** Automatically detect known vulnerabilities across your whole network
- **Inventory & Network Devices:** Detect and inventory existing IT-devices within your network
- **Update Management & Managed Software:** Deploy updates and patches as tested, ready-to-deploy packages

c)

Business continuity, such as backup management and disaster recovery, and crisis management.

- **OS-Deployment & Configuration:** Wipe and re-install systems and configurations automatically across your network





f)

Concepts and procedures for assessing the effectiveness of risk management measures in the area of cybersecurity.

- **Vulnerability Scanner:** Automatically identify the latest CVE
- **Update Management & Managed Software:** Automatically install security patches and updates from trusted sources

h)

Concepts and procedures for the use of cryptography and, where appropriate, encryption.

- **Endpoint Security:** Centrally configure and manage encryption based on MS BitLocker technology, including PIN and Recovery Key management
- **Device Control (powered by Drivelock):** Reliably restrict and control access to data and information on your network.

i)

Personnel security, access control concepts, and asset management.

- **Endpoint Security:** Securely manage local admin passwords and ensure immediate password changes after use
- **Inventory & Network devices:** Discover and document all IT-assets in your network



Compliance with NIS2 is not just a legal obligation; it's an essential way to improve your company's cybersecurity posture and resilience. UEM solutions like the baramundi Management Suite not only lower IT workloads for establishing, maintaining, and reporting NIS2 compliance, but also reduce the costs and duration of downtime caused by cybersecurity incidents, and the risk of NIS2 enforcement actions and penalties.

7 Seven Steps to NIS2 Compliance

Time is of the essence for IT teams affected by NIS2. Thorough planning, timely implementation, and continuous review of compliant cybersecurity measures are necessary as EU nations enact or update requirements. We recommend the following steps:

- 1 Start with an impact analysis:**
Conduct and maintain an ongoing impact analysis (self-assessment) to determine the NACE classification and requirements under EU or country-specific laws. Focus on sustained, demonstrable compliance by continuously reviewing, documenting, and upgrading cybersecurity measures, rather than treating NIS2 implementation as a one-time project.
- 2 Actively involve management in NIS2 processes:**
Explain the potential impact of non- or late compliance as well as the benefits of proactive implementation. Describe how NIS2 can strengthen your company's cyber-resilience and business reputation over the long term.
- 3 Plan risk management measures:**
Conduct a comprehensive gap analysis to identify where action is needed and to determine targeted steps to improve cybersecurity. Use proven IT automation and vulnerability management solutions to free up valuable resources for both implementing needed measures and for ongoing IT tasks.
- 4 Plan and budget for NIS2 compliance:**
Use dedicated, step-by-step procedures to ensure compliance, and include them in budget and staffing plans.
- 5 Complete registration and prepare reporting processes:**
Complete registration as required, prepare, test, and practice reporting procedures for a security incident so you can act quickly and efficiently.
- 6 Set up regulatory monitoring:**
Establish a system to stay informed about current, proposed, or new regulations at an early stage. Analyze them thoroughly to assess their impact on your company.
- 7 Prioritize training:**
Millions of business managers and employees need to be trained for NIS2 each year. Each country defines and updates its applicable training requirements.

UEM: A Key to NIS2 Compliance

NIS2 demands a systematic approach to cybersecurity — one that extends well beyond IT. The consequences of non-compliance include administrative, financial, and criminal sanctions, but the stronger case for action is organizational: NIS2 compliance strengthens cyber resilience, demonstrates a security commitment to customers and partners, and reduces the risk of a successful attack. An effective UEM solution provides IT teams with a practical path to achieving and sustaining compliance while reducing IT costs, improving workforce productivity, and enhancing user satisfaction.

About baramundi software GmbH

baramundi software's Unified Endpoint Management (baramundi Management Suite) and Proactive Endpoint Operations (baramundi Proactive Hub) solutions enable organizations to manage IT environments and digital workplaces efficiently, securely, and across platforms — on-premises and in the cloud. baramundi software GmbH is headquartered in Augsburg, Germany. Founded in 2000, the company develops its products and services in the EU and supports them through offices in the U.S., Italy, and Poland. baramundi also collaborates with sales, consulting, and customer support partners worldwide.

More information about baramundi: www.baramundi.com



Register for our live webinar to learn more about the baramundi Management Suite!

Discover how the baramundi Management Suite automatically manages and secures your endpoints, servers, and mobile devices, then try it free for 30 days in your own network.

<https://www.baramundi.com/en-us/events-trainings/webinars/>

Get in Touch.

We are looking forward to meeting you!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+49 821 56708-390
request@baramundi.com



Making IT Admins Smile