

T Business

NIS2: Heralding a new era of cyber resilience

Are you ready to embrace the change?



Connecting
your world.



NIS2

what, why, and when

NIS2, the revolutionary update to Europe's cybersecurity law, is on the horizon. Are you prepared to meet the new standards? Whether you're already progressing toward compliance or just beginning to explore NIS2, our quick guide clarifies the key elements of this pioneering legislation and shows how we can support you throughout the process. Understand the profound changes ahead and learn how to adapt effectively.

The objectives of NIS2

Harmonizing rules across the EU

Establishing a unified framework to standardize cybersecurity practices across member states.

Enhancing cooperation between countries

Fostering cross-border collaboration to improve response and resilience to cybersecurity threats.

Strengthening understanding of emerging threats

Improving the collective ability to identify and address new and evolving cybersecurity risks.

Tailoring security and reporting obligations

Adapting requirements based on the significance of each entity to ensure proportionate measures and effective compliance.

NIS2 – the Network and Information Security Directive 2 – represents one of the most significant regulatory changes since GDPR. It is poised **to impact an estimated 160,000** organizations across the EU, a substantial increase from the approximately 30,000 entities affected by the original NIS Directive in 2016.

The directive aims to **bolster the resilience** of the European Union's critical infrastructure and essential services against cybercrime. By introducing stricter security requirements, enhancing incident response, and facilitating intelligence sharing and coordination across member states, it will establish a **unified and higher standard for Europe's digital security**.

Member states have until **October 18, 2024**, to create and publicize their plans to comply with NIS2. The timeline for companies to comply with the new regulations will be determined by the national laws of each member state.

NIS2

who it affects

Check if NIS2
applies to you –
complete our
self-assessment.



The directive takes a tailored approach to different sectors by classifying organizations into two main categories:



- **Essential entities (Annex I):** Organizations **crucial** for maintaining critical infrastructure and services. Their disruption could have **severe consequences** for society and the economy. The sectors covered are energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, ICT service management (business-to-business), public administration, and space.
- **Important entities (Annex II):** Organizations that provide significant services but are less critical than essential entities. Their disruption can have a **considerable impact** but not to the extent of those in Annex I. The sectors covered are postal and courier services, waste management, chemicals (manufacture, production, and distribution), food (production, processing, and distribution), manufacturing, digital providers, and research.

The focus on **supply chain security** is crucial under NIS2, especially as supply chains become increasingly important in cybersecurity frameworks. Both essential and important entities must ensure that their suppliers and service providers have adequate cybersecurity measures to protect the integrity of critical services. This includes undertaking audits and risk assessments to manage supply chain risks effectively.

Importantly, suppliers and service providers within these supply chains are also subject to NIS2 obligations, requiring them to implement and maintain robust cybersecurity measures to safeguard their contributions to critical services. Thus, all parties within the supply chain must collaborate to enhance security and compliance under the directive.

Moreover, the directive could extend to **non-EU entities** that provide services or products to customers in the EU, particularly if those entities have a significant presence or impact within EU territory.



Understanding NIS2's impact on larger organizations and some SMEs

Essentially, NIS2 applies both sector and size criteria to enhance cybersecurity resilience across the EU. This dual approach broadens inclusion and ensures that more significant, potentially impactful entities comply with cybersecurity requirements due to their larger size.

Larger organizations may have to comply with more stringent requirements than smaller organizations, depending on the measures used to address the risks assessed and local legislation.



Large organizations: Typically refers to companies with **over 250 employees** and an **annual turnover exceeding € 50 million**, or a **balance sheet total over € 43 million**.



Medium-sized organizations: Usually companies with **fewer than 250 and more than 50 employees** and an **annual turnover from € 10 million to € 50 million** or a **balance sheet total not exceeding € 43 million**.



Small and micro-sized enterprises: Generally exempt from obligations, **small enterprises have fewer than 50 employees** and an **annual turnover under € 10 million**. **Micro-sized enterprises have fewer than 10 employees** and an **annual turnover under € 2 million**. However, exceptions apply if they are part of **critical infrastructure** or provide essential services, requiring them to comply with NIS2 due to their importance in cybersecurity.

Country-by-country differences

While NIS2 sets a baseline for cybersecurity requirements, it's important to note that local legislators in each EU member state have the authority to strengthen the directive or expand its scope. For instance, they can impose additional responsibilities or add specific sectors to Annex I or Annex II.

As previously mentioned, how supply chains are classified under NIS2 depends on the industry or sector they support. Entities not explicitly covered by the directive may also fall under local regulations.

We recommend staying updated on your country's NIS2 requirements by regularly checking government websites. **Our local experts can help you navigate country-specific rules and meet any additional obligations.**

Local transposition and classification of entities

The implementation of the NIS2 Directive is subject to national transposition laws, which means that each EU member state has the discretion to adapt the directive to fit its national context. This can lead to variations in how entities are classified and the sanctions imposed for non-compliance.

For instance, in Poland, some organizations classified as 'important' may be reclassified as 'essential' based on national considerations. Similarly, the specific sanctions and enforcement measures can differ across member states, reflecting their unique legal and regulatory environments.

It is crucial to monitor the national transposition laws in each member state to understand the specific requirements and potential implications for your organization.

This will help ensure compliance with both the overarching NIS2 framework and the local regulations.

The organizational penalties



As we've shown, NIS2 is a two-tier system. The financial penalties per incident for non-compliance differ depending on an organization's category:

- **Essential entities**
€10 million or 2% of total annual turnover
- **Important entities**
€7 million or 1.4% of total annual turnover

In all cases, the higher amount applies.



The individual penalties

A shift in accountability

NIS2 redefines accountability for cybersecurity within organizations, elevating it from an IT responsibility to placing it firmly on the leadership team's agenda. This shift emphasizes senior executives' duty to ensure robust risk management and cybersecurity oversight.

In addition to the organizational penalties imposed under the directive, **senior executives** can be held **personally liable** for non-compliance, particularly in cases of gross negligence or insufficient governance related to cybersecurity incidents. NIS2 establishes that senior executives **may be held directly accountable** and could face public disclosures or bans on future management roles. Depending on the legal frameworks of individual EU member states, additional penalties, such as criminal sanctions or fines, may also apply.

Senior leadership team responsibilities under NIS2

Responsible role or business function *	Actions required for implementing NIS2
CEO	Implementation oversight and ownership
CSO, Legal	Risk analysis and the company's Information Systems Security Policy (ISSP)
CSO, CIO/CTO	Incident handling
CIO/CTO, CSO	Business continuity, such as backup, disaster recovery, and crisis management
CSO, Procurement, Legal	Supply chain security, including the security aspects of relationships with suppliers or service providers
CSO, CIO/CTO, Procurement, Legal	Security across the acquisition, development, and maintenance of networks and information systems, including vulnerability management
CSO	Evaluating the effectiveness of cybersecurity risk management procedures and policies
CSO, HR	Basic cyber hygiene practices and cybersecurity training
CSO, CIO/CTO	Policies and procedures on cryptography and, where appropriate, encryption
CSO, CIO/CTO, HR	Personnel security, identity management and access control, and asset management policies
CSO, CIO/CTO	Use of multi-factor or continuous authentication, secure communications (voice, text, video), and emergency protocols


The **responsibility for these tasks may vary** depending on the size and structure of the organization. In smaller companies, for example, the business owner might handle multiple roles.

Our NIS2 experts can guide you on how best to organize your team to meet compliance requirements and fill in any existing gaps.

* Chief Executive Officer (CEO), Chief Security Officer (CSO), Chief Information Officer (CIO), Chief Technology Officer (CTO)

Supervision under NIS2

Proactive and reactive approaches

To check your current levels of compliance, book a cybersecurity assessment. 

NIS2 establishes a comprehensive supervision system to ensure that organizations meet cybersecurity requirements, with different approaches based on their significance.

- **Essential entities:** These critical organizations are subject to both **proactive and reactive supervision**. National authorities will regularly assess and monitor their compliance and respond to incidents as they arise.
- **Important entities:** These organizations are **primarily overseen through a reactive approach**. National authorities will investigate incidents as they occur, using a simplified process compared to essential entities.
- **Large organizations outside these categories:** These organizations are **generally subject to reactive supervision**, similar to important entities.

Each EU member state is responsible for designating or establishing appropriate national authorities to carry out this supervision.



The NIS2 reporting system

Three stages

Explore our incident management services. 

NIS2 introduces a **structured reporting system** for managing significant cybersecurity incidents – those that **substantially impact** an organization's operations, critical infrastructure, or essential services. The process involves three stages:

1

Early warning: Organizations must report significant incidents to their relevant Computer Security Incident Response Team (CSIRT) **within 24 hours of detection** to help contain and mitigate the impact.

2

Incident notification: Within 72 hours of detecting the incident, organizations must submit a preliminary report to the CSIRT, including an initial assessment of its impact and potential consequences. While the 72-hour incident notification window is mandated, **local lawmakers** may introduce further requirements or details via national laws.

3

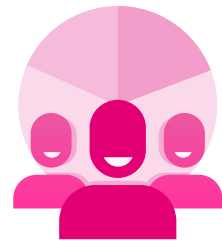
Final report: A detailed **final report** outlining the incident, lessons learned, and mitigation steps must be submitted no later than one month after the initial assessment.

Local legislators are responsible for clarifying and implementing the general rules around incident reporting. To this end, **each EU member state** is responsible for designating or establishing a CSIRT to oversee incident reporting and response within its jurisdiction. Again, the local legislators **may decide to expand** the NIS2 obligations. For example, while the directive focuses on significant incidents, national regulations may also require reporting for non-significant incidents.

How to prepare for NIS2 implementation

Focus on three core areas – technical, legal & procedural, and operational – while incorporating a prevent, detect, respond, and mitigate approach to effectively manage cybersecurity risks.

Use our gap analysis tool



Technical

- **Develop** robust and secure systems that are resilient against cyber threats.
- Establish **early warning systems** and incident response mechanisms to ensure swift reaction/recovery in the face of potential disruptions.
- Implement comprehensive **disaster recovery** plans to minimize downtime in case of incidents.
- Adopt effective **access controls** and authentication measures to protect digital assets, ensuring only authorized personnel can access sensitive information.
- Leverage technologies such as **multi-factor authentication** (MFA) and encryption to enhance security protocols.

Legal & procedural

- Create a comprehensive **library of policies** and procedures as required by the directive, ensuring alignment with NIS2.
- Regularly **review, audit, and update policies** and procedures to reflect changes within the organization or among its suppliers and service providers.
- Promptly **report cybersecurity** incidents to the appropriate national authority, adhering to the timelines and requirements established by NIS2 and the local regulator.
- Implement a **risk management** process that includes third-party assessments to ensure supply chain integrity.
- Ensure **senior management** understands their cybersecurity responsibilities under NIS2, has access to the necessary expertise, and actively oversees the organization's cybersecurity strategy.

Operational

- Conduct regular infrastructure security **assessments and continuous monitoring** to identify vulnerabilities.
- **Monitor and measure** the effectiveness of cybersecurity controls regularly, ensuring ongoing compliance with NIS2 requirements and facilitating continuous improvement.
- Promote **cybersecurity awareness** through regular training programs and strong cyber hygiene practices across all levels of the organization.
- Enhance **HR security protocols** to mitigate internal risks and promote a culture of security awareness.
- Engage all levels of employees in the **security culture**, fostering a sense of shared responsibility for protecting organizational assets.

How we can help

Explore our managed and self-services below, or contact us to arrange a consultation.

Everything in one place

- NIS2 self-assessment
- Off-the-shelf services
- NIS2 gap analysis
- Managed services
- NIS2 consultancy
- Customized services

Why Deutsche Telekom?

As a telecom provider, we operate under the strictest regulations and fully comply with both the original NIS Directive and NIS2. We understand your challenges and can help alleviate your regulatory burden, ensuring you are prepared to meet NIS2 requirements and protect your organization from cyber threats. In addition to our broad portfolio of security services to cover your NIS2 regulation needs, we offer compliance packages specifically tailored to address the updated directive. **Contact us.**

Publisher

Deutsche Telekom AG
Friedrich Ebert Allee 140
53113 Bonn, Germany



Connecting
your world.

