What is the NIS2 Directive?

In today's digital age, cybersecurity is a major concern for individuals and organizations due to the increasing frequency of cyber-attacks. Recognizing this, the European Commission introduced the EU Network and Information Security (NIS) directive in 2016 to enhance cybersecurity across the European Union. However, the directive lacked accountability, prompting the Commission to plan its replacement with the more robust NIS2 directive.

NIS2 mandates companies to implement key cybersecurity measures, including supply chain security, cryptography, and encryption (Article 18). Article 89 emphasizes the adoption of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, and identity and access management for essential and important entities.

NIS vs NIS2 - what's changed?

There are some important differences between the old and the new Directive:

- The new proposal removes the distinction between Operators of Essential Services (OES) and Digital Service Providers (DSP), instead classifying entities as either essential or important.
- The scope of the Directive is expanded to cover new sectors based on their criticality for the economy and society, including all medium and large companies in these sectors. Member States can also identify smaller entities with a high-risk profile.
- The establishment of a European Cyber Crisis Liaison Organization Network (EU-CyCLONe) is proposed to work collectively in preparing and implementing rapid emergency response plans, for example in case of a large-scale cyber incident or crisis.
- Increased coordination in the disclosure of new vulnerabilities discovered across the Union. A list of administrative sanctions (similar to those of the GDPR) is established, including fines for violating cybersecurity risk reporting and management obligations.
- NIS2 imposes direct obligations on management bodies to implement and oversee their organization's compliance with the legislation – potentially resulting in fines and temporary ban from exercising management functions, including at the C-suite level.

In addition, it introduces more precise provisions on the process of reporting incidents, **the content of the reports and the timing** (within 24 hours of the discovery of the incident). At European level, the proposal strengthens cybersecurity for key information and communication technologies. Member States, in cooperation with the Commission and ENISA European Union Agency for Cybersecurity, will have to carry out coordinated risk assessments of critical supply chains.

Who does it apply to?

While under the old NIS directive member states were responsible for determining which entities would meet the criteria to qualify as operators of essential services, the new NIS2 directive introduces a size-cap rule. This means that **all medium-sized and large entities operating within the sectors or providing services covered by the directive will fall within its scope**.

Below you can find a classification by size-cap rule:

Essential Entities (EE) Size threshold: varies by sector, but generally 250 employees, annual turnover of €50 million or balance sheet of €43 million	**Important Entities (IE)** Size threshold: varies by sector, but generally 50 employees, annual turnover of €10 million or balance sheet of €10 million
Energy	Postal Services
Transport	Waste Management
Finance	Chemicals
Public Administration	Research
Health	Foods
Space	Manufacturing
Water supply (drinking & wastewater)	Digital Providers (e.g. social networks, search engines, online marketplaces)
Digital Infrastructure (e.g. cloud computing service providers and ICT management)	

NIS2 also covers public administration bodies at central and regional level but excludes parliaments and central banks.

When will it be enforced?

All EU Member States must incorporate the new obligations into their national laws before 17 October 2024. Following final approval on 16 January 2023, covered entities have been given a 21-month compliance window once the directive enters into force. The following list shows the NIS development timeline:

- **6 July 2016:** NIS adopted
- **9 May 2018:** Deadline for Member States to transpose NIS into national law
- **7 July 2020:** European Commission launches consultation on NIS reform
- **16 December 2020:** European Commission publishes proposal for NIS2
- **22 November 2021:** European Parliament adopts its negotiating position
- **3 December 2021:** European Council adopts its negotiating position
- **13 January 2022:** First round of trilogue negotiations
- **16 February 2022:** Second round of trilogue negotiations
- **13 May 2022:** Political agreement reached
- **10 November 2022:** European Parliament votes to adopt NIS2
- **28 November 2022:** NIS2 approved by the Council of the EU
- **27 December 2022:** NIS2 published in the Official Journal and comes into force 20 days later, on 16 January 2023
- **17 October 2024:** Deadline for Member States to transpose NIS2 into national law

How can we help your business stay NIS2 compliant?

At BSI, we have a large team of highly experienced, industry leading experts that will help ensure that you and your business have all the security requirements you need to get ahead of the NIS2 Directive. Through a pragmatic, risk-based approach to cybersecurity in line with international best practice, as outlined in standards such as ISO 27001 for Information Security and ISO 22301 for Business Continuity, your route to NIS2 compliance with BSI is assured. With our help, organizations can avoid potential financial penalties and inspire further trust among your customers.

Why are ISO 27001 and ISO 22301 key to NIS2 compliance?

The NIS regulations recommend that companies, in their compliance efforts, should prioritize "compliance with international standards". Additionally, the technical guidelines from the European Union Agency for Cybersecurity (ENISA) align each security objective with best practice standards, such as ISO 27001.

Of all the services that BSI can provide to your company in relation to NIS2, two standards seem to be key: ISO 27001 and ISO 22301.

- Implementing an ISO 27001-compliant Information Management System (ISMS) empowers organizations to minimize risks and exposure to security threats. It entails identifying necessary policies, employing suitable technologies, and providing staff training to prevent errors. Mandating annual risk assessments, ISO 27001 enables organizations to proactively address the evolving risk landscape.
- ISO 27001 not only facilitates meeting NIS2 requirements but also enables organizations to attain independently audited certification. This certification serves as tangible evidence for suppliers, stakeholders, and regulators, showcasing the adoption of "appropriate and proportionate" technical and organizational measures and establishing a competitive advantage in the market.
- For organizations seeking an enhanced approach, the addition of ISO 22301 for business continuity management is recommended. ISO 22301 assists in implementing, maintaining, and continuously improving business continuity practices. While ISO 27001 incorporates aspects of business continuity management (BCM), ISO 22301 provides a defined process for BCM implementation. Certification against ISO 22301 further reinforces compliance with NIS2.

The synergy between ISO 27001 and ISO 22301 allows organizations to develop an integrated management system encompassing both an ISMS and a BCMS. This holistic approach not only aids in compliance but also fosters the development of robust cyber resilience.

Why BSI?

At BSI, our world-class capabilities instil confidence in clients across cybersecurity and hygiene. We offer deep expertise in cybersecurity, risk management, and information resilience, with a global cross-sector perspective. Our understanding spans issues affecting the public sector, emerging threats, and practical industry experience in managing cyber risk and resilience.

What should you do next?

- Check if your organization is in scope
- Inform your management/board of the impending regulations
- Contact us to get NIS2 compliance support: sales.nl@bsigroup.com