bsi.

What is the NIS2 Directive?

To respond to the growing threats posed by digitalization and the surge in cyber-attacks, the European Commission has submitted a proposal to replace the NIS Directive with NIS2. This will strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonized sanctions across the EU.

The NIS2 Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union by placing obligations on:

- Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs)
- Entities referred to as essential for cybersecurity risk management
- Cybersecurity information sharing

NIS vs NIS2 - what’s changed?

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

- The new proposal eliminates the distinction between Operators of Essential Services (OES) and Digital Service Providers (DSP), instead classifying entities as either essential or important
- The coverage of the Directive is expanded to cover new sectors based on their criticality for the economy and society, including all medium and large companies of 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
- Greater coordination is established in the disclosure of new vulnerabilities discovered throughout 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” concerning implementation and supervision of their organization's compliance with the legislation – leading potentially to fines and temporary ban from discharging managerial functions, including at the senior management 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.

bsi.

What is the NIS2 Directive?

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.

The number of sectors covered by the NIS2 Directive increase from 19 to 35. The usual sectors are covered (energy infrastructure, airports, railways, healthcare, water, banks) but also now includes:

- cloud providers
- data centres
- public electronic communications networks
- managed service providers
- postal services, food production
- waste water
- waste management
- chemical manufacturing
- the space sector, and more

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 these new obligations in their national laws before September 2024. Following final approval, in scope entities will have a 21-month compliance window once the directive enters into force. The following list shows the NIS development timeline:

- 6 July 2016: NIS 1 adopted
- 9 May 2018: Deadline for Member States to transpose NIS 1 into national law
- 7 July 2020: European Commission launches consultation on NIS reform
- 16 December 20201: European Commission publishes proposal for NIS 2
- 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 NIS 2
- 28 November 2022: NIS 2 approved by the Council of the EU
- Expected in late 2022: NIS 2 published in the Official Journal
- Autumn 2024: Deadline for Member States to transpose NIS 2 into national law

What is the NIS2 Directive?

How can BSI Consulting help?

At BSI, we have a large team of highly experienced, industry leading consultants that will help ensure that you and your business have all the security requirements you need to get ahead of the NIS2 Directive, which will help organizations to avoid potential financial penalties and instill further confidence in your customers. From initial OES identification to self-assessment, risk assessment and risk treatment, our experience of working with organizations across the sectors can help you on the pathway to NIS Directive 2 compliance.

BSI currently offer the following services in relation to the NIS2 requirements:

Cyber strategy/governance

- Cybersecurity posture/maturity assessments against industry standard frameworks
- Information security/cyber strategy development/board presentations
- Gap analysis and implementation support (ISO 27001, SOC 2, NIST CSF/800-53)
- Information security awareness and training

Crisis Management and Incident Response

- Business Continuity (ISO 22301)
    - Business Impact Analysis (BIA)/Policy Development/Business Continuity Planning
- Disaster Recovery Support, Implementation, and periodic testing
- Threat Led Penetration Testing (TLPT)
- Open-Source Intelligence (OSINT)
- Physical Security Assessments
- Attack simulation (Red/Blue/Purple team)
- Incident Response planning and implementation (ISO27035)
- Threat Modelling/Threat assessments
- Assessment of current incident response planning and reporting capability
- Incident response testing/staff training

Risk Management and Reporting

- IT Risk Management Framework development and implementation (ISO 27005)
- Third Party Risk management (ISO 27036-2)
    - Current state assessment of third-party lifecycle management
    - Develop end to end supplier management framework
    - Implementation of third-party risk management framework alongside ongoing risk management support
- BSI work with technology partners who have tooling to facilitate the entire supplier lifecycle management
    - Threat Intelligence/Computer Emergency Response Team (CERT) Certification
    - Assess current position and determine future state
    - Build a reporting framework

What is the NIS2 Directive?

Why BSI?

At BSI, we have world class capabilities specifically designed to provide confidence to clients in all areas of cybersecurity and cybersecurity hygiene. including:

- Deep domain experience in the field of cyber security, risk management and information resilience.
- Global cross sector experience with a core understanding of the issues impacting the public sector and emerging threats, along with pragmatic industry experience in the area of 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

Contact us:

IE/International Call: +353 1 210 1711
Email: digitaltrust.consulting.ie@bsigroup.com
Visit: bsigroup.com/digital-trust-ie

UK Call: +44 345 222 1711
Email: digitaltrust.consulting@bsigroup.com
Visit: bsigroup.com/digital-trust-uk

US Call: +1 800 862 4977
Email: digitaltrust.consulting.us@bsigroup.com
Visit: bsigroup.com/digital-trust-us