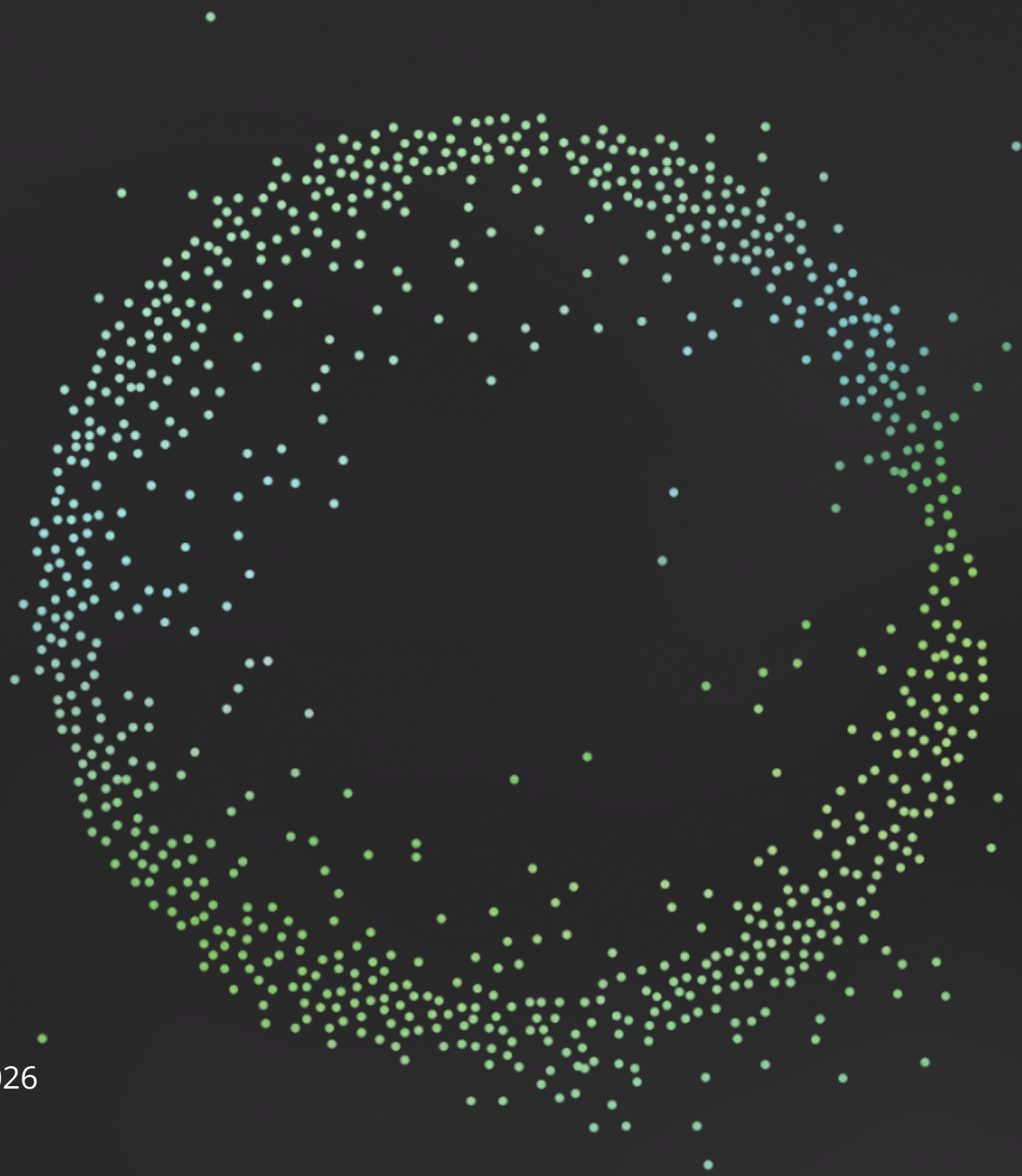
Deloitte.



NIS2 overview:
Implications and next steps

Network and Information Security Directive | 2026

NIS2 Directive – Why is this important?

The NIS2 Directive is designed to raise the EU's baseline for cybersecurity through stricter governance, reporting, and control requirements. While October 2024 was the deadline for EU member states to transpose the Directive into national law, many organizations are still working to understand and meet the resulting national compliance requirements.

- **Affecting medium to large corporations as well as their supply chains and consumers**
- **Similar to General Data Protection Regulation (GDPR), NIS2 has an extraterritorial reach**
- **It mandates compliance for organizations outside the EU that offer services within the EU market**

- Mandatory **cybersecurity risk assessment** for the entire organization
- Measures required to keep your cybersecurity **risks acceptable** for the organization

Security incident reporting

First notification within 24 hours, then within 72 hours; within 1 month, a **final report must be provided**

- **Fines** of up to €10 million or 2% of the organization's annual global turnover
- Management can be **suspended** from their duties

- **Accountability for management and board** on cybersecurity risks
- **Mandatory cyber training** for staff, management, and board

Inspections (regular, ad hoc, thematic, and post-incident)

Key requirements of NIS2

NIS2 sectors in scope

The Directive applies to all large and medium-size enterprises[1] operating in the sectors in scope 2, identified as essential or important entities.

Sectors in scope of the NIS1 directive

- **Operators of essential services**
  - Financial market infrastructures
  - Banking
  - Drinking water supply and distribution
  - Digital infrastructure
  - Energy
  - Transport
  - Health
- **Digital service providers***

NIS 2

New sectors in scope[2]

Annex I

- ICT service management
- Public administration
- Space
- Waste water
- Energy
- Health

Annex II

- Chemicals (manufacture, production, distribution)
- Manufacturing
- Food (production, processing and distribution)
- Postal and courier services
- Waste management
- Research
- Digital service providers**

** Limited scope*

*** Expanded to include more entities, such as managed service providers (MSPs), online marketplaces, and search engines, as well as digital infrastructure providers*

Enterprises[1]		
	Essential entity	Size varies by sector, but generally 250 employees and an annual turnover of €50 million or balance sheet of €43 million
	Important entity	Size varies by sector, but generally 50 or more employees with an annual turnover of €10 million or balance sheet of €10 million

1 - Refer Article 34 of NIS Directive
2. – Refer ANNEX I & ANNEX II of NIS Directive

Focus: Supervisory organization and administrative fines

The NIS2 Directive establishes a differentiation in the supervisory organization and the application of fines between essential and important entities.

Essential entities should be subject to a **fully fledged supervisory** organization (ex ante and ex post), while **important entities** should be subject to a **light supervisory organization**, ex post only

Essential entities

Fully fledged supervisory regime (ex ante and ex post)

1. Onsite inspections and offsite supervision, including random checks
2. Regular audits
3. Targeted security audits
4. Security scans
5. Requests for information necessary to assess the cybersecurity risk-management measures adopted
6. Requests to access relevant data, documents, and information
7. Requests for evidence of implementation of cybersecurity policies

Important entities

Light supervision (ex post)

- When provided with **evidence**, indication or information that an **important entity** allegedly **does not comply** with this Directive, competent authorities shall take action through ex post supervisory measures

1. Onsite inspections and -offsite ex post supervision
2. Targeted security audits
3. Security scans
4. Requests for information necessary to assess ex post the cybersecurity risk-management measures adopted
5. Requests to access relevant data, documents, and information
6. Requests for evidence of implementation of cybersecurity policies

Administrative fines

Competent authorities can impose administrative fines up to €10 million or 2% of the total global annual turnover of the company

Competent authorities can impose administrative fines up to €7 million or of the total global annual turnover of the company

Focus: Risk management measures

The Directive identifies security measures that all essential and important entities will be required to implement to ensure adequate management of cybersecurity risks.

Technical, operational, and organizational measures

- **Policies on risk analysis and information system security**
- **Incident handling**
- **Business continuity and crisis management**
- **Supply chain security**
- **Basic cyber hygiene practices** (e.g., zero trust principles, software updates, device configuration, network segmentation, organize training for staff, raise awareness of cyberthreats, phishing or social engineering techniques)
- **Policies and procedures** to **assess** the effectiveness of cybersecurity **risk-management measures**
- **Security** in **network** and **information systems acquisition, development, and maintenance**, including vulnerability handling and disclosure
- **Policies and procedures** regarding the **use** of **cryptography** and **encryption**
- **Human resources security, access control policies, and asset management**
- **The use of multi-factor authentication** or continuous authentication solutions; secured voice, video, and text communications; and secured emergency communication systems within the entity

Focus: Supply chain security

Entities are required to monitor on the security of their supply chain.

Essential and important entities

- Have at least the measure in place: **supply chain security**
- Assess and take into account the overall **quality of suppliers' development procedures**
- Exercise **increased diligence** in selecting managed security services providers (**MSSPs**)

Business implications

- **Reengineering supplier due diligence process**
- **Assessing secure development process internally and externally**

National and European levels

- Member states shall develop a **policy addressing cybersecurity in the supply chain** for ICT products and services used by essential and important entities
- The Cooperation Group, the European Community (EC), and European Union Agency for Cybersecurity (ENISA) should carry out **coordinated sectoral supply chain risk assessments**

Market impact

- **Identification of previously overlooked risk in certain sectors**
- **Potential for stricter security requirements on IT product level**

Focus: Incident reporting

NIS2 Directive provides for stricter requirements for cyber incident reporting and management.

Member states should ensure that the requirement to submit initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritized

Threshold of reporting obligations (NIS2)

Incident is classified as significant if:

- **Caused** or has **potential** to **cause substantial operational disruption** or **financial losses** to the entity concerned
- **Affects** or has **potential** to **affect** other **natural** or **legal persons** by causing considerable material or non-material losses

Within 24 hours after becoming aware of the incident:

- **Early warning**, which shall **indicate whether** the **significant incident** is **suspected** of being **caused** by **unlawful** or **malicious acts** or could have a cross-border impact
- **Computer Security Incident Response Team (CSIRT)** or the **competent authority** shall provide a **response** including initial **feedback**

Within 72 hours of becoming aware of the incident:

- An **incident notification** shall **update** the **information referred** to in the **early warning** and provide an initial **assessment** of the **incident**

Upon the request of a CSIRT or the competent authority:

- An **intermediate report** on relevant **status updates**

No later than one month after initial notification:

- **Final report** with **analysis** of **the incident, including:**
  - ✓ A detailed description of the incident
  - ✓ Type of threat or root cause
  - ✓ Applied and ongoing mitigation measures
  - ✓ Cross-border impact

Threshold of reporting obligations (GDPR)

Incident is reported:

- In the case of a personal data breach

Without undue delay and no later than 72 hours:

- Incident notification to the National Data Protection Authority and to the data subject if necessary

Information may be provided in phases:

- Where, and in so far as, it is not possible to provide the information at the same time

Readiness assessment approach

To support clients in the compliance process, we have defined a methodological approach that, following a Readiness Assessment phase, involves the identification of interventions to be implemented to enable compliance.

Directive impact analysis

Analysis of the potential **impacts** of the **Directive** on the **company** with regard to different **prescription areas**, taking into consideration the company's operations in different countries

Identification of regulatory obligations

Identification of regulatory obligations and definition of a Framework of Controls by mapping with ISO27001 and the National Framework for Cybersecurity and Data Protection

Domains

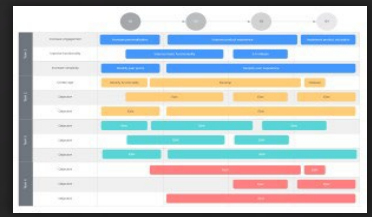
- Policies on risk analysis and security
- Incident management
- Business continuity and crisis management
- Supply chain security
- Training and awareness
- Effectiveness of security measures
- System acquisition, development and maintenance
- Cryptography and encryption
- Human resources security and access control
- Authentication solutions

Readiness assessment

Performing an assessment using the defined Framework of Controls to assess whether the company's cybersecurity management is in line with the security requirements of the Directive

Definition of intervention plan

Definition and sharing of the Intervention Plan including the activities to be carried out, methods, and their timelines, to ensure that the company is prepared for the compliance requirements of the Directive



Services being provided by Deloitte

NIS2 considerations

There are several variables that should be taken into consideration when determining the scope of a NIS2 readiness assessment, including:

Location: *Compliance is specific to each country and their associated framework(s).*

Law: *Has the country transposed the NIS2 Directive into national law at the time of the assessment?*

Entity designation: *Essential or important?*

Scope of assessment: *IT and/or OT? Sample size or complete set of assessments? How many centralized controls? Are any of these controls ISO certified?*

Deadline to be compliant: *The actual deadline for companies to fully implement the required cybersecurity measures will be set by the individual member states' laws. This period can range from 6 to 18 months from the date of registration.*

Let’s Talk

Mehdi Houdaigui

Principle, Cyber Strategy Leader
Deloitte & Touche LLP
mhoudaigui@deloitte.com

Theresa Woolcott

Managing Director, Cyber Strategy
Deloitte & Touche LLP
twoolcott@deloitte.com

Edward Guerrero

Manager, Cyber Strategy
Deloitte & Touche LLP
edwguerrero@deloitte.com

Debolina Sinha

Senior Manager, Cyber Strategy
Deloitte & Touche LLP
debosinha@deloitte.com

Contributors

Angad Deep Singh

Manager, Cyber Strategy
Deloitte & Touche AERS India Private Limited
angaddsingh@deloitte.com

Thank you!