Module 1: NIS2 in a nutshell

Six short lessons on what every manager and employee of a NIS2 organisation should know, followed by a 10-question quiz. Score 80% or more to pass.

NIS2 Aware · nis2aware.eu · November 2026

LESSON 1 OF 6

Why NIS2?

Hospitals, ports, energy suppliers, food producers, cloud services: our economy runs on networks and information systems. A single ransomware attack can stop production, block deliveries or put patients at risk, and the damage often spreads to customers and suppliers.

The European Union first tackled this with the **NIS Directive** in 2016. It covered a limited number of operators, and each country applied it differently. Its successor, the **NIS2 Directive** (Directive (EU) 2022/2555), was adopted in December 2022 to raise the level of cybersecurity across the Union.

What NIS2 changes

- **Broader scope:** many more sectors and, as a rule, all medium-sized and large organisations in those sectors.
- **Stricter obligations:** a common set of risk-management measures and harmonised incident reporting deadlines.
- **Management accountability:** the board must approve and oversee cybersecurity and must be trained.
- **Real enforcement:** supervision by national authorities and significant fines.

The directive itself does not apply directly to companies: each Member State had to transpose it into national law by 17 October 2024. In Belgium, that is the NIS2 law.

KEY POINTS

- NIS2 is Directive (EU) 2022/2555, the successor of the 2016 NIS Directive.
- It covers more sectors and more organisations, with stricter rules.
- It applies to companies through national law.

LESSON 2 OF 6

The Belgian NIS2 law

Belgium transposed NIS2 through the **law of 26 April 2024** establishing a framework for the cybersecurity of network and information systems of general interest for public security, supplemented by a **Royal Decree of 9 June 2024**. The law entered into force on **18 October 2024**.

The key players

Who	Role
CCB, Centre for Cybersecurity Belgium	National cybersecurity authority: supervision, inspections, sanctions and guidance. Its CERT.be team is the national CSIRT that handles incident notifications.
Sectoral authorities	Work alongside the CCB in certain sectors (for example finance, telecoms, energy, transport, health).
Safeonweb@Work (atwork.safeonweb.be)	The CCB portal where entities register and find guidance and tools.

CyberFundamentals: the Belgian toolbox

The CCB developed the **CyberFundamentals (CyFun®)** framework: a set of concrete security measures with assurance levels (Basic, Important and Essential). An updated version, CyFun 2025, was published in October 2025. Organisations can use CyFun, or the international standard **ISO/IEC 27001**, to structure their measures and demonstrate compliance.

> **Good to know:** NIS2 Aware is an independent training provider. For official information, always refer to the CCB.

KEY POINTS

- Belgian NIS2 law: 26 April 2024, in force since 18 October 2024.
- The CCB is the national authority; registration happens on Safeonweb@Work.
- CyberFundamentals (CyFun) or ISO/IEC 27001 help structure and prove your measures.

LESSON 3 OF 6

Who is concerned?

The law applies to organisations established in Belgium that pass two tests: they are active in a **sector** listed by NIS2, and they are at least **medium-sized**.

Test 1: the sector

Sectors of high criticality (Annex I)	Other critical sectors (Annex II)
Energy · Transport · Banking · Financial market infrastructures · Health · Drinking water · Waste water · Digital infrastructure (cloud, data centres, DNS, telecom…) · ICT service management, B2B (managed IT and security service providers) · Public administration · Space	Postal and courier services · Waste management · Chemicals · Food production, processing and distribution · Manufacturing (medical devices, computers and electronics, electrical equipment, machinery, motor vehicles, other transport equipment) · Digital providers (online marketplaces, search engines, social networks) · Research

Test 2: the size

- **Medium-sized:** from 50 employees, or an annual turnover and balance sheet total above €10 million.
- **Large:** from 250 employees, or a turnover above €50 million and a balance sheet total above €43 million.

Partner and linked enterprises (for example in a group) can count towards these figures.

Exceptions

Some organisations are covered **whatever their size**, for example DNS service providers, top-level domain registries, qualified trust service providers and some providers of public electronic communications. The CCB can also designate specific entities.

> **Your responsibility:** nobody will send you a letter. Each organisation must assess for itself whether it falls within scope.

Not in scope? You can still be affected: NIS2 entities must manage the security of their suppliers, so they will pass requirements on to you.

KEY POINTS

- Two tests: a NIS2 sector and at least medium size (50+ employees or more than €10M turnover and balance sheet).
- Some digital providers are covered regardless of size.
- Every organisation must check its own status; suppliers are affected indirectly.

LESSON 4 OF 6

Essential or important entity?

Organisations in scope fall into one of two categories. The core obligations are the **same**; what differs is the intensity of supervision and the level of fines.

	Essential entity	Important entity
Typical profile	Large organisations in high-criticality sectors (Annex I), plus some specific cases	Medium-sized organisations in Annex I, and medium or large ones in Annex II
Supervision	Proactive (*ex ante*): the CCB can inspect at any time	Reactive (*ex post*): mainly after an incident or indications of non-compliance
Conformity assessment	Mandatory and periodic (CyberFundamentals or ISO/IEC 27001)	Voluntary, but it gives a presumption of conformity
Maximum fine	€10 million or 2% of worldwide annual turnover	€7 million or 1.4% of worldwide annual turnover

Beyond fines, the authorities can issue binding instructions and, for essential entities that keep failing to comply, temporarily prohibit a person from exercising management functions.

> **In practice:** for essential entities, the CCB is rolling out the conformity assessment in phases. A first checkpoint fell on 18 April 2026, and further milestones follow. Check the CCB for the dates that apply to you.

KEY POINTS

- Same obligations; different supervision and fines.
- Essential: proactive supervision and mandatory conformity assessment; fines up to €10M or 2%.
- Important: reactive supervision; fines up to €7M or 1.4%.

LESSON 5 OF 6

The four core obligations

1. Register

Entities register with the CCB on **Safeonweb@Work**. The deadlines were 18 December 2024 for certain digital providers and 18 March 2025 for all others. An organisation that comes into scope later must register without delay.

2. Take risk-management measures

Measures must be appropriate and proportionate to the risks, following an "all hazards" approach. The law lists at least these areas:

- risk analysis and information system security policies
- incident handling
- business continuity: backups, disaster recovery, crisis management
- supply chain security
- security in the acquisition, development and maintenance of systems, including vulnerability handling
- assessing the effectiveness of the measures
- basic cyber hygiene and cybersecurity training
- cryptography and encryption
- human resources security, access control and asset management
- multi-factor authentication and secured communications

3. Report significant incidents

Deadline	What
24 hours	Early warning to the CCB after becoming aware of a significant incident
72 hours	Incident notification with a first assessment
1 month	Final report

Where appropriate, the recipients of your services must also be informed.

4. Involve and train the management

The management body must **approve** the measures, **oversee** their implementation and can be held **liable**. Its members must **follow training**; regular training for staff is encouraged as well.

KEY POINTS

- Register on Safeonweb@Work.
- Implement measures in at least ten areas, from risk analysis to MFA.
- Report significant incidents: 24 hours, 72 hours, one month.
- The board approves, oversees, is liable and must be trained.

LESSON 6 OF 6

Key dates and next steps

December 2022
NIS2 Directive adopted at EU level

26 April 2024
Belgian NIS2 law adopted

18 October 2024
Entry into force in Belgium

18 December 2024
Registration deadline for certain digital providers

18 March 2025
Registration deadline for all other entities

October 2025
Publication of CyberFundamentals 2025

18 April 2026
First conformity checkpoint for essential entities

2027 and beyond
Further conformity assessment milestones for essential entities (check the CCB)

Five steps to take now

1. **Check your scope** and your category (essential or important).
2. **Register** on Safeonweb@Work if you have not already done so.
3. **Assess your gaps** against CyberFundamentals or ISO/IEC 27001 and plan the improvements.
4. **Set up incident reporting**: who decides, who notifies, within 24 hours.
5. **Train your board and staff**, and keep evidence of it.

> You have completed the lessons of Module 1. Take the quiz to test your knowledge.

KEY POINTS

- In force since 18 October 2024; registration deadlines have passed.
- Essential entities are in the conformity assessment phase.
- Next steps: scope, registration, gap analysis, incident procedure, training.

This module gives general information on the Belgian NIS2 framework as of November 2026. It is not legal advice. Always check the latest guidance from the CCB (ccb.belgium.be and atwork.safeonweb.be).