NIS2 in Belgium: what does it mean for your organisation?

The Belgian NIS2 Act and the CCB's CyberFundamentals framework — in a single overview.

NIS2 is European Directive (EU) 2022/2555 on cybersecurity, transposed into Belgian law by the **Act of 26 April 2024** and in force since **18 October 2024**. The **Centre for Cybersecurity Belgium (CCB)** is the national cybersecurity authority, the national CSIRT and the supervisory body, with its own inspection service. Where NIS1 covered a few hundred organisations, more than 4,000 Belgian entities are now in scope — and through the supply chain, many more companies feel the effects.

1 Are you in scope?

Two criteria apply together: **your sector** (18 sectors, including energy, transport, health, digital infrastructure, ICT service management, food, chemicals, waste, manufacturing and public administration) and **your size** (from 50 employees or €10 m turnover). There is no active designation any more: you assess this yourself.

Category	Supervision
Essential entity large, most critical sectors	Proactive, regular supervision. Mandatory conformity assessment by an external body.
Important entity often mid-sized players	Ex-post supervision. No audit up front, but you must be **demonstrably** compliant when the CCB calls.

Not in scope? Still relevant. NIS2 entities must assess their supply chain and pass those requirements on contractually to suppliers and IT partners. The CCB advises every organisation in the chain to reach **CyFun Basic** as a minimum. The CCB can also designate critical organisations after the fact, regardless of their size.

2 The core obligations

- **Registration** with the CCB through the Safeonweb@work portal.
- **Risk-management measures** (art. 21): risk analysis and security policy, incident handling, backup and continuity, supply-chain security, patch and vulnerability management, cryptography, access and asset management, **MFA**, cyber hygiene and training, plus periodic evaluation of effectiveness.
- **Reporting obligation** for significant incidents: **24 h** early warning → **72 h** incident notification → **1 month** final report. Ransomware triggers additional questions.
- **Management accountability**: the management body approves the measures, oversees implementation and must follow training itself. Personal liability is possible.

3 CyberFundamentals (CyFun®)

CyFun is the CCB's framework, translating the legal text into concrete, verifiable measures based on NIST CSF 2.0, ISO 27001, the CIS Controls and IEC 62443. A CyFun or ISO/IEC 27001 verification gives a **presumption of conformity**. Three in four entities choose CyFun, because it is more accessible for SMEs.

Level	Measures	Coverage*	Intended for
Small	7 (free)	—	micro-organisations, entry level
Basic	34	±82%	SMEs and suppliers in the chain
Important	±132	±94%	important entities
Essential	±217	±100%	essential entities, critical infrastructure

* Coverage of the most common attack techniques as estimated by the CCB. Each level builds on the previous one.

The route: **(1)** risk assessment and choice of level, **(2)** self-assessment with supporting evidence, **(3)** verification or certification by a BELAC-accredited Conformity Assessment Body (CAB). Note: a CyFun label alone is not full NIS2 compliance — the reporting deadlines, among other things, must be set out separately in your procedures.

4 Timeline

18 Oct 2024	Belgian NIS2 Act enters into force.
18 Mar 2025	Deadline for registration with the CCB.
18 Apr 2026	Essential entities submit their first conformity assessment: a CAB verification at Basic or Important level, or their ISO 27001 scope and Statement of Applicability. Those under the inspection route submit a self-assessment.
18 Apr 2027	Target level reached: full Essential or ISO 27001 certification, or a progress report under inspection supervision. Entities designated later get the same deadlines (18 and 30 months) counted from notification.

5. Penalties. For essential entities, administrative fines run up to **€10 m or 2%** of worldwide annual turnover; for important entities up to **€7 m or 1.4%**. Binding instructions, public disclosure of the breach, temporary suspension of the service and personal liability of directors are also possible. The CCB takes a coaching stance, but anyone unable to demonstrate any effort is in a weak position.

How Brick9 supports you

1. Scope & baseline

Establishing whether and how you are in scope, choosing the right CyFun level, and a gap analysis of your environment against that level, with a priority list and budget.

2. Technical remediation

Identity and MFA/conditional access, endpoint protection and 24/7 detection, next-gen firewall and segmentation, backup and recoverability, patch management, logging and monitoring.

3. Evidence & upkeep

Policies and procedures, an incident response plan with the 24/72-hour flow, documented evidence per measure, awareness training and guidance through to CAB verification.

Sources: ccb.belgium.be · atwork.safeonweb.be · the Act of 26 April 2024 (NIS2) and its implementing Royal Decree. | This sheet is informative and general in nature, prepared in July 2026, and does not constitute legal advice; your actual obligations depend on your sector, size and risk assessment. | **Brick9** · brick9.com — questions, or a no-obligation NIS2 scan? Contact your account manager.