NIS2

Keep your business running, even under cyber pressure

NIS2 is now enforced across Europe, and fully transposed in Belgium organisations, the question is no longer whether you are in scope – it is whether you can withstand disruption and prove it.

Key numbers

160k **Organisations in scope across the EU**

4000+ **Belgian entities registered with the CCB**
1500 essential I 2500 important

+57% **Increase in reported cyber incidents in Belgium**
Q4 2024 vs Q4 2023 (CCB)

What does NIS2 means concretely?

NIS2 requires continuous cybersecurity focus and risk-based approach across your organisation, with board-level accountability.

6 Key requirements

- 24h incident reporting
- Supply-chain audits
- Board certification
- CyFun ISO 27001
- Continuous monitoring
- Awareness training

Where organisations struggle most?



Vulnerability & patch management*



Business continuity & Disaster recovery



Supply-chain risk management

Most organisations understand the regulation. The real gap is operational capacity to execute it – many mid-sized entities lack a functioning security team to ensure NIS2 implementation and sustain compliance.

Financial exposure

Essential entities	€10M or 2% global turnover **personal executive liability**
Important entities	€7M or 1.4% global turnover **management ban risk**

NIS2 accountability goes to the Executive table.
Art. 20 NIS2 foresees personal liability of Board members Leaders can be held personally accountable if their company fails to put basic cyber safety measures in place.

The cost of non-compliance is not only the penalty – it is business disruption, operational paralysis, and leadership accountability when resilience fails.

Belgian timeline for Essential Entities using CyFun

Oct 2024	Mar 2025	Apr 2026	Apr 2027	Apr 2028
Law enforcement	Registration	Demonstrate progress: Basic/Important certification	Essential certification, if unable: remediation plan	Essential certification, in case of a remediation plan submitted

Sectors in scope

Energy I Transport I Banking I Financial market infrastructure I Health I Drinking water I Wastewater I Digital infrastructure I ICT service management I Public administration I Space

Postal services I Waste management I Chemicals I Food I Manufacturing I Digital providers I Research

The world is how we shape it

sopra steria

NIS2: Ask yourself

- Can we continue operating during a cyberattack?
- Can we recover without major financial impact?
- Can we protect customers and reputation?

Our approach to shaping your NIS cyber readiness

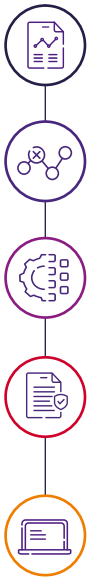
From assessment to implementation to continuous control – aligned with CyFun and EU requirements

Why Sopra Steria

1. Integrated Belgian and European cybersecurity practice – coordinated delivery across Local and EU landscape with a unified methodology.
2. Trusted Cybersecurity partner on Belgian market with proven Cyber experience
3. Local Belgian delivery aligned with CCB CyFun framework and coordinated with any other security and regulatory needs.
4. End-to-End Pragmatic and risk-based Cybersecurity approach tailored to your organisation management-ready reporting at every stage.

> *"Every organisation has its unique story. We understand yours - and we know how to make NIS2 happen. End to end"*
>
> **Sopra Steria • Cybersecurity Business Line BeLux**

Our 5-step methodology



Assess posture
Current-state review against CyFun & ISO27001 and NIS2 relevant articles

Identify gaps
Prioritised and pragmatic action plan by risk and regulatory urgency

Implement
Organisational & technical measures, governance, supply chain

Validate
Intermediate control testing and/or pre-assessment based on KPIs and audit-ready evidence

Monitor
Continuous control improvement & regulatory reporting

Start with a focused NIS2 Readiness Scan

A short, targeted engagement that gives your leadership team a clear and honest view of where you stand – and what must be addressed first to reduce regulatory and operational risk.

Sources : www.aegister.com
www.enisa.europa.eu
*CCB (Centre for Cybersecurity Belgium)

Success story

CyFun-driven NIS2 compliance for a Belgian public institution

With NIS2 bringing Belgian public institutions into the Essential Entity scope, the client needed a practical way to operationalise new obligations quickly. Sopra Steria structured NIS2 governance, aligned operational processes and established sustainable compliance mechanisms across all required domains.

Result

The Client obtained clear NIS2 security posture view, established operational security processes and ensure existed of the necessary documentary evidence supporting CCB oversight. The project outcomes and concrete implementation were delivered ahead of audit deadlines.

Outcomes of Your Readiness Scan

- Current NIS2 posture
- Gap assessment & Prioritised roadmap
- Management-ready report

Reduce uncertainty before it becomes risk

Contact us & Strengthen your NIS2 Position →

ivana.butorac@soprasteria.com | tom.degol@soprasteria.com