Beyond ISO/IEC 27001: Enhancing Cyber Resilience with CyFun® 2025 in the NIS2 Era

Dirk De Paepe
Senior Certification Expert
Cybersecurity Certification Authority Belgium (NCCA)

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

CENTRE FOR CYBERSECURITY BELGIUM

Strategic Context and the Need for Change

Why This Matters in 2026:
The Shift From Compliance to Resilience

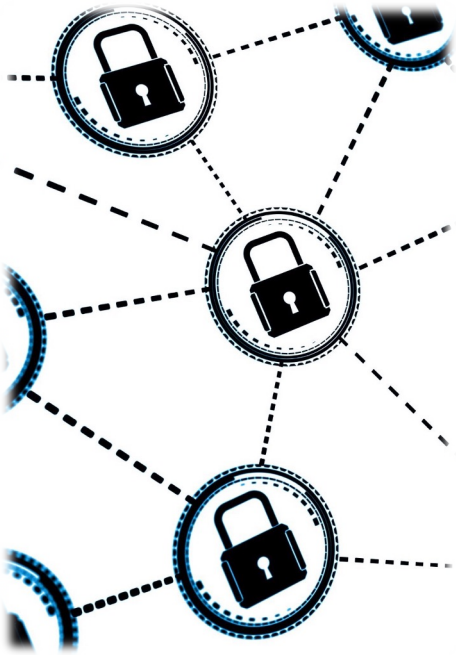
CENTRE FOR CYBERSECURITY BELGIUM

Limitations of Traditional Compliance

Compliance shows documented processes but fails to ensure effectiveness against modern cyber threats.

Shift to Operational Resilience

Resilience focuses on maintaining essential services and operational continuity under cyberattacks and disruptions.

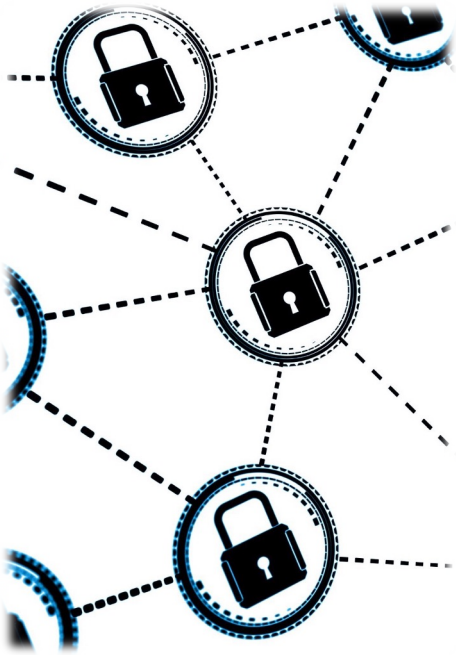


Why This Matters in 2026:
The Shift From Compliance to Resilience

CENTRE FOR CYBERSECURITY BELGIUM

Leadership Accountability in NIS2 Era

NIS2 now holds leadership personally accountable for keeping essential services running, and that responsibility cannot be fulfilled by compliance alone. It requires operational resilience.



CyFun® 2025:
The Framework That Moves Us Beyond ISO 27001

From certification to operational cyber resilience in the NIS2 era.

CENTRE FOR CYBERSECURITY BELGIUM

Why Compliance Falls Short

The Illusion of Safety:
ISO/IEC 27001 ≠ Operational Resilience

CENTRE FOR CYBERSECURITY BELGIUM

ISO/IEC 27001 Certification Limits

Certification proves the ISMS exists – not that operational safeguards work in real attacks.

The Compliance – Resilience Gap

Policies and audits ≠ incident readiness, service continuity, or recovery capability.

The Illusion of Safety:
ISO/IEC 27001 ≠ Operational Resilience

CENTRE FOR CYBERSECURITY BELGIUM

Operational Reality

Real resilience is measured by detection speed, containment ability, and time to recover – not by documentation.

Evolving Threat Landscape

Attackers automate lateral movement and exploit supply chains, areas often untested in traditional compliance programs.

CENTRE FOR CYBERSECURITY BELGIUM

The Regulatory Shift With NIS2

Understanding NIS2: From Documentation to Operational Continuity

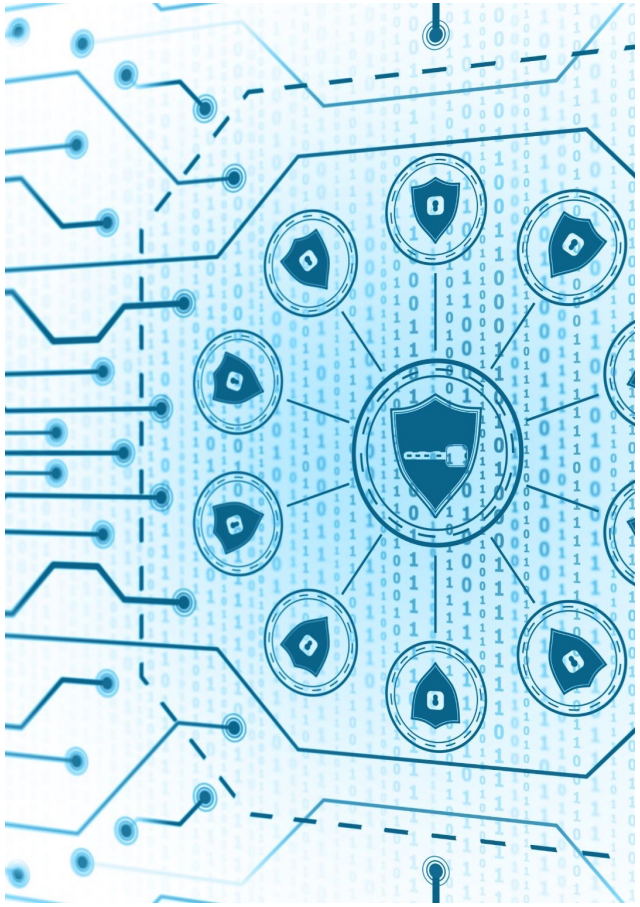
CENTRE FOR CYBERSECURITY BELGIUM

Operational Resilience Priority

NIS2 shifts focus from information security to continuity of essential and important services.

Leadership Accountability

CEO and board members are personally responsible for approving, overseeing, and governing cyber resilience.



Understanding NIS2: From Documentation to Operational Continuity

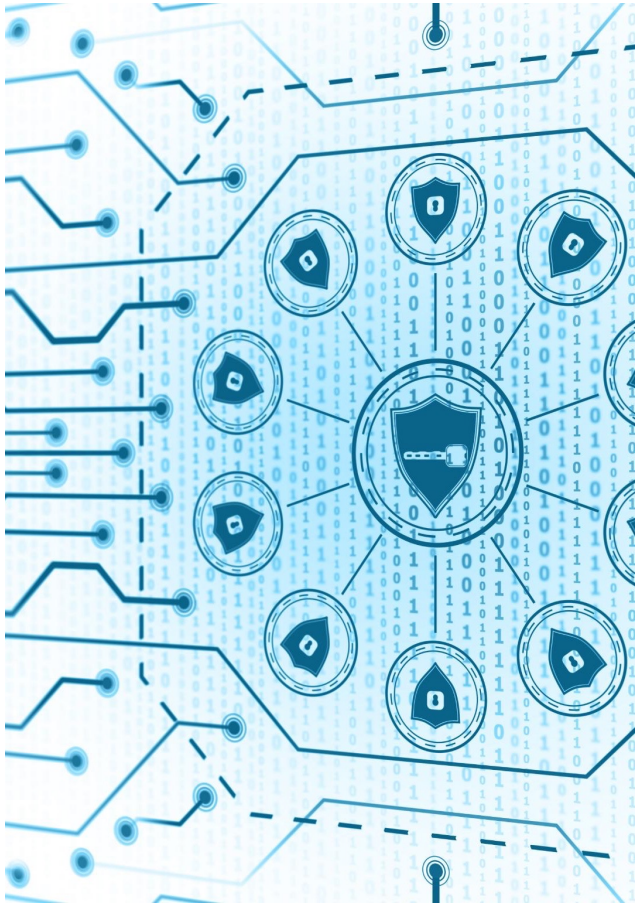
CENTRE FOR CYBERSECURITY BELGIUM

Outcome-Based Security Measures

NIS2 mandatory measures require real capabilities: risk management, incident handling, continuity, supply-chain security, vulnerability handling, and more.

Need for Maturity-Driven Frameworks

CyFun® 2025 provides the structured, measurable approach needed to interpret and implement NIS2's non-prescriptive, outcome-based obligations.



CENTRE FOR CYBERSECURITY BELGIUM

CyFun® 2025 as the Operational Bridge

Core Principles of CyFun® 2025: Execution, Maturity, and Resilience

CENTRE FOR CYBERSECURITY BELGIUM

CyFun®

The Operational Layer Missing in ISO & NIS2

Operational Readiness and Enforcement

Focuses on execution and effectiveness of safeguards through measurable, auditable controls.

Maturity Levels for Proportionate Security

Basic → Important → High (Essential) maturity levels aligned with sector risk and organizational complexity.

Resilience through Real-World Testing

Ensures controls work under attack conditions, with outcomes proven in practice.

Interoperable With Existing Standards & Frameworks

Integrates seamlessly with ISO/IEC 27001, NIST CSF, CIS Controls, and IEC 62443.

CENTRE FOR CYBERSECURITY BELGIUM

Path Forward: Integrating ISO, NIS2, and CyFun®

A Practical Model for Resilience in 2026 and Beyond

CENTRE FOR CYBERSECURITY BELGIUM

ISO/IEC 27001 – A Governance-Focused Option

Provides structured management processes and risk governance for organisations that prefer a traditional ISMS approach.

CyFun® 2025 – A Modern Alternative to Traditional ISMS Certification

Delivers governance and operational resilience in one certification scheme.

A Practical Model for Resilience in 2026 and Beyond

CENTRE FOR CYBERSECURITY BELGIUM

NIS2 – Mandatory Outcomes for Essential & Important Entities

Defines continuity, proportionate security, and leadership accountability – regardless of the chosen framework.

CyFun®

A Single, Coherent Path – Not Dual Certification

Organisations choose the model that fits best: ISO/IEC 27001 or CyFun® 2025.

CyFun® provides the most complete and NIS2-aligned route to demonstrable operational resilience.

CENTRE FOR CYBERSECURITY BELGIUM

Conclusion: The Era Of Resilience

Resilience as the New Competitive Advantage

CENTRE FOR CYBERSECURITY BELGIUM

Shift in Cybersecurity Narrative

"*It's not if you will be breached, but when.*" shifts to "*It's not when you are attacked, but how fast and how well you recover.*"

Resilience as Differentiator

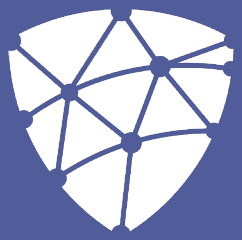
ISO/IEC 27001 will give you structure.

NIS2 will give you obligations.

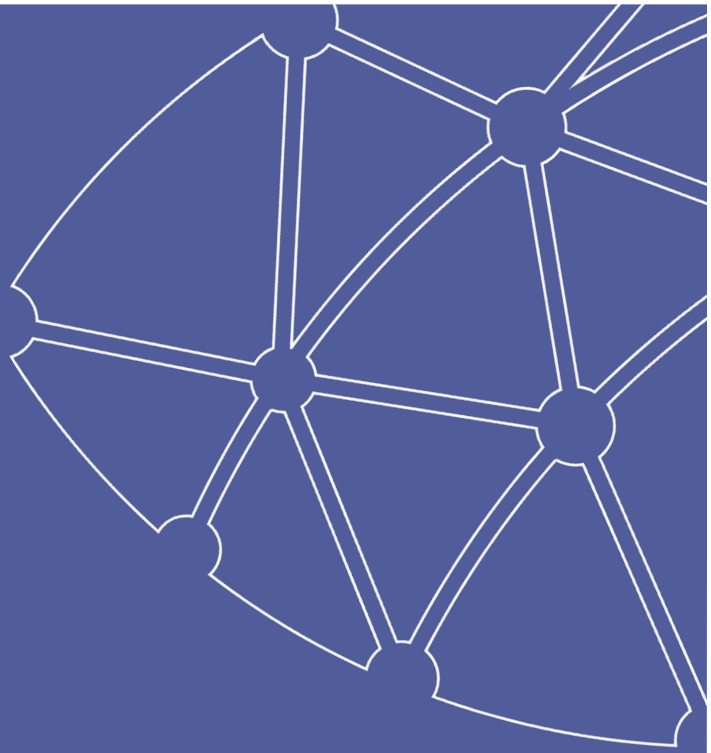
But CyFun® gives you resilience.

Resilience as Strategic Asset

Resilience is a leadership responsibility and competitive advantage in a volatile, AI-driven digital ecosystem.



CENTRE FOR
CYBERSECURITY
BELGIUM



CCB Certification Authority (NCCA)
certification@ccb.belgium.be

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
Rue de la Loi / Wetstraat 18 - 1000 Brussels
www.ccb.belgium.be

.be

What does TLP Green mean?

CENTRE FOR CYBERSECURITY BELGIUM

TRAFFIC LIGHT PROTOCOL (TLP)

Green (TLP GREEN)

Limited disclosure, recipients can spread this within their community.

Sources may use **TLP:GREEN** when information is useful to increase awareness within their wider community.

Recipients may share **TLP:GREEN** information with peers and partner organizations within their community, but not via publicly accessible channels (e.g. websites, LinkedIn…). **TLP:GREEN** information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.