CyFun® 2025 as an Objective and Maturity based Evaluation Framework for NIS2 Compliance Assessments

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

NIS2's Implicit Question

NIS2 does not ask:

Do you have controls?

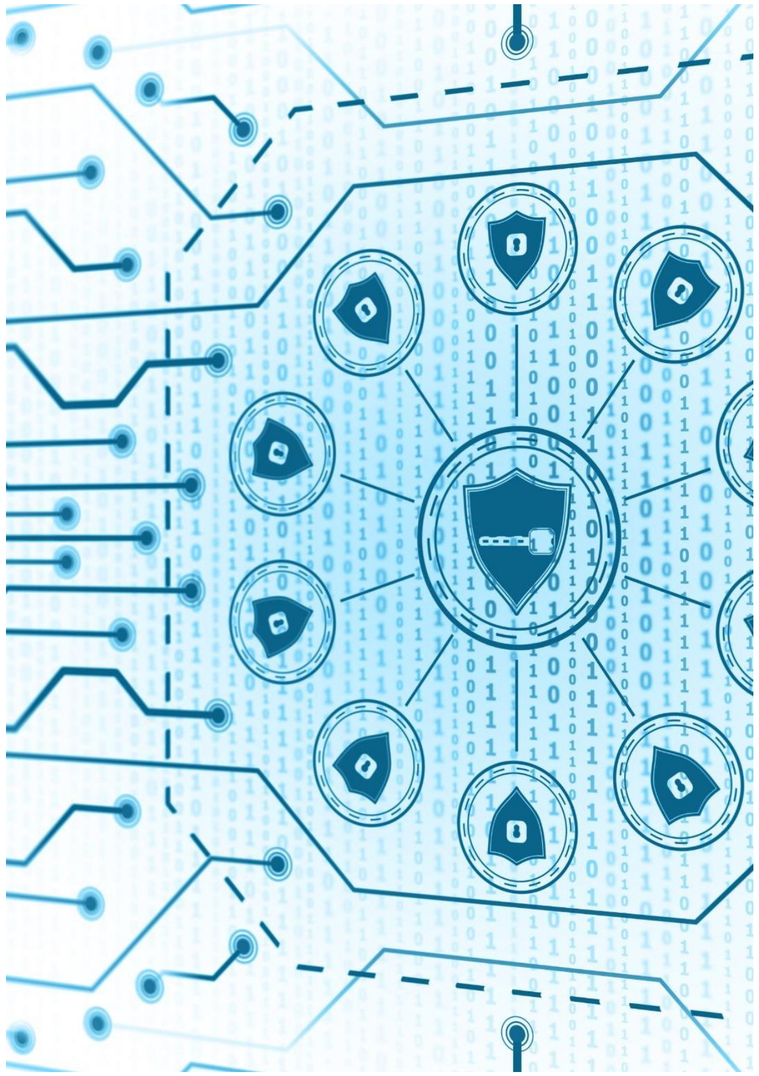
NIS2 asks:

Can you manage cyber risk, sustainabl
and under governance?

This is a **capability** question,

not a **checklist** question.

Why Controls Are Not Enough



Controls tell us:

That something exists

They do not tell us:

- If it works
- If it is governed
- If it will still work tomorrow
- If management is accountable

Controls alone ≠ cyber resilience (NIS2 intent)

Introducing “Capability”

In CyFun®, a capability is:

The demonstrable ability of an organization to manage a specific cyber risk in a sustainable, governed, and repeatable way.

Key aspects:

- Organisational
- Lifecycle-based
- Outcome-driven

What Makes a Capability

A capability only exists when several elements come together:

1. Governance and ownership
2. Risk-based decision-making
3. Operational execution
4. Monitoring and feedback
5. Continuous improvement

Without all five:

- No capability
- Only isolated controls

Why Capability Is Central to NIS2

NIS2 explicitly requires:

- Risk-based security (Art. 21)
- Management responsibility (Art. 20)
  - *Effectiveness over time*
  - *Proportionality*

These requirements:

- Cannot be validated via controls alone
- **Can** be evaluated via capability maturity

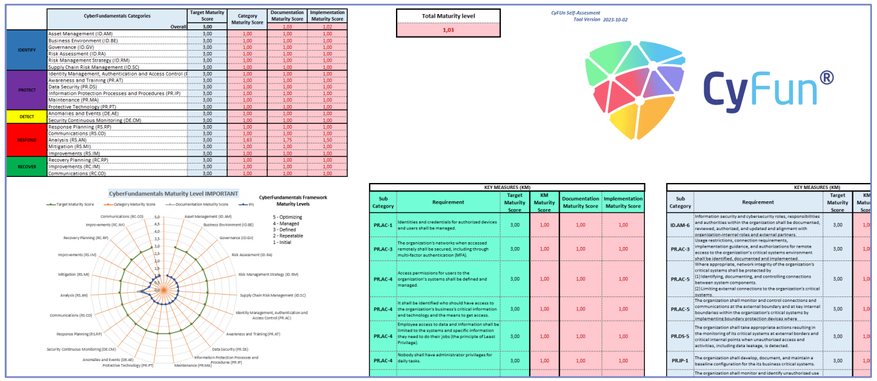
Capability Needs a Measure: Maturity

Capability alone is not enough.

Supervision also needs to answer:

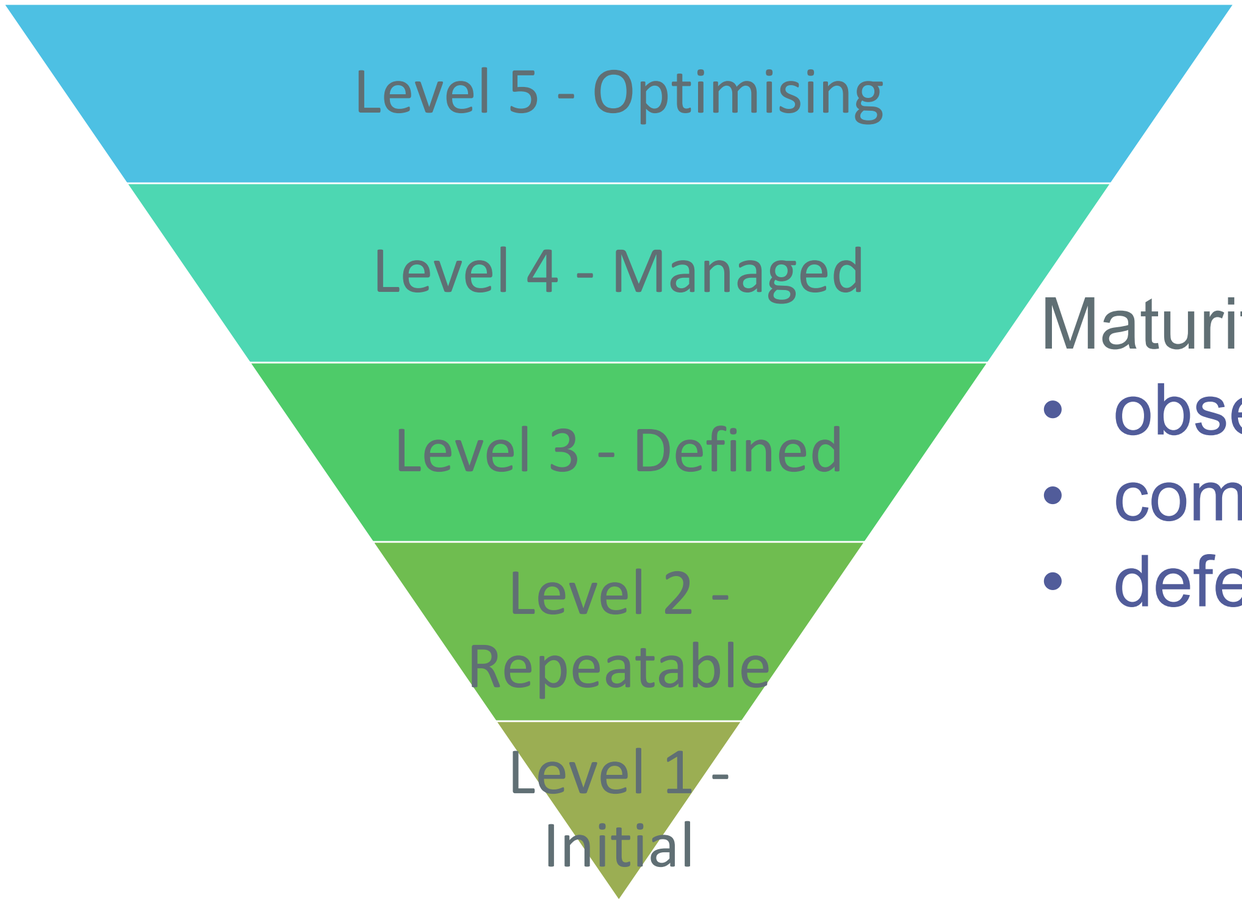
- *How robust is this capability?*
- *How well is it embedded?*
- *How dependent is it on individuals?*

This is where
maturity assessment
comes in.



Maturity in CyFun®

The CyFun® CAS uses a **uniform maturity scale**:



Maturity makes cyber resilience:

- observable
- comparable
- defensible in supervision

What CyFun® CAS Actually Assesses

CyFun® CAS does **not** assess:

- Tools
- Technologies
- Vendors

It assesses:

- How capabilities are organised
- How decisions are made
- How risk is controlled
- How improvement is driven

Organisational behaviour, not artifacts.

Example: Incident Response Plan

RS.MA-01.1 An incident response plan, including defined roles, responsibilities, and authorities, shall be executed during or after a cybersecurity event affecting the organisation's critical systems (CyFun® BASIC)

Low maturity:

- Incident response plan exists
- Roles and authorities unclear in practice
- Execution is ad hoc and reactive
- Response depends on individuals

Higher maturity:

- Clear ownership and decision authority
- Management involved according to defined escalation rules
- Incident response regularly tested and exercised
- Lessons learned drive updates to the plan and execution

Same “control”, different **capability maturity**

Why This Enables Objectivity

CyFun® CAS relies on:

- Observable practices
- Decision structures
- Evidence of consistency
- Management interaction

Result:

- Reduced assessor subjectivity
- Comparable outcomes
- Defensible assessments

From Capability Maturity to NIS2 Compliance

CENTRE FOR CYBERSECURITY BELGIUM

CyFun® provides a structured link between:

- NIS2 obligations (Art. 20 & 21)
- Observable organisational capabilities
- Maturity-based evidence of effectiveness

This enables:

- Consistent interpretation of NIS2 requirements
- Risk- and maturity-based supervision
- Defensible supervisory conclusions

What Regulators Gain

With CyFun®, authorities can:

- Compare entities fairly and consistently
- Supervise proportionally, based on risk and maturity
- Identify and prioritise weakest capabilities
- Track measurable improvement over time

Supervision shifts from:

“**Is this compliant?**”

to

“**Is this organisation cyber-resilient?**”

What Organisations Gain

Organisations gain:

- Clear expectations
- Structured improvement paths
- Management-level insight
- Defensible compliance position

Compliance becomes:

- Operational
- Measurable
- Strategic meaningful

Closing: The Core Message

- NIS2 compliance is not binary
- It is **capability-based**
- And must be evaluated through **maturity**

Cyber resilience is not about having controls.

It is about having mature capabilities.

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

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.