Assuring Cyber Resilience under NIS2
The CyFun® Audit Model and the Role of ISO/IEC 27001

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

.be

Version: 19 May 2026

Agenda

- CyberFundamentals (CyFun®) Conformity Assessment
- NIS2 Authorisation conditions for CABs

CENTRE FOR CYBERSECURITY BELGIUM

CyberFundamentals Conformity Assessment

CyFun® CAS – Part II: Assessment

CENTRE FOR CYBERSECURITY BELGIUM

CyFun®

- How CyFun® assessments are performed
- Differences between verification and certification
- What CABs are expected to do
- Why the Clarifications matter

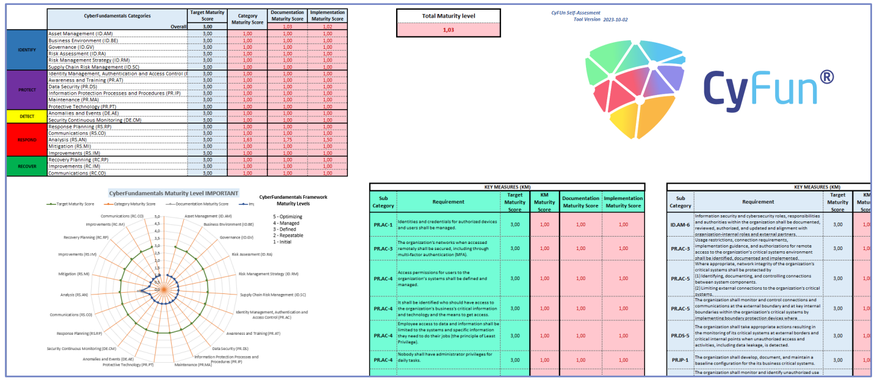
One Assessment Logic, Three Assurance Levels

CyFun® assurance levels

- **Basic** → Verification (ISO/IEC 17029)
- **Important** → Verification (ISO/IEC 17029)
- **Essential** → Certification (ISO/IEC 17021-1)

Common principle

- Assessment is always based on a **self-assessment + objective evidence**



The Central Role of the CyFun® Self Assessment

CENTRE FOR CYBERSECURITY BELGIUM

Self-assessment

- Mandatory input for every assessment
- Structured, maturity-based
- Covers documentation **and** implementation maturity

What CABs assess

- Plausibility of maturity scores
- Consistency with evidence
- Conformity with threshold values

Verification Process (CyFun® Basic & Important)

Applies to

- Assurance levels **Basic** and **Important**

Process steps

- Pre-engagement & scope definition
- Planning (full or limited verification)
- Documentary review
- On-site verification of **key measures**
- Verification report
- Independent review
- Verification statement

Strictly follows ISO/IEC 17029

+

CyFun® specific requirements

Full vs. Limited Verification

Full verification

- First-time verification, scope changes, material maturity changes
- All key measures on site

Limited verification

- Re-confirmation
- At least 50% of key measures
- Permitted only where the scope and maturity are stable

The choice must be motivated and documented by the CAB.

Verifications ➔ assessment of **all** controls
Verification requires a minimum of one day on site and may take longer when necessary.

Scope description

Pre-engagement (Ref. CyFun CAS A.2.4.1.)

The Conformity Assessment Body shall require the applicant to submit information sufficient to carry out a pre-engagement review (see A.2.1). The CAB shall make sure that the scope is documented and agreed upon, based on a precise description of the entity to be verified as well as the locations, services/products and processes.

scope: “Legal entity” ≠ OK

The CAB must have reviewed the scope and come to an agreement with the client ***before*** *accepting or refusing to carry out the verification.*

Handling Misstatements (Why Clarifications Exist)

Misstatement

- Claimed maturity not supported by evidence

CAB obligations

- Identify and assess materiality
- Re-score (⬇) where needed
- Decide if claim remains valid

📌 ***Defined in detail in CAS Clarifications***

Important

- The Organisation **cannot correct maturity scores during the same verification** to pass a threshold

Verification statement

Part II A/B 3

[NAME of conformity assessment body], acting as third party conformity assessment body, declares to have verified the following claim:

[NAME, ADDRESS of the organisation and COMPANY NUMBER] declares to satisfy the requirements of the CyberFundamentals assurance level "Basic" on [date] for the following scope: [scope].

[NAME of conformity assessment body] confirms that this claim is materially correct at [date of verification], based on the evaluation of the by [NAME of the organisation] completed self-assessment with version [version of the used self-assessment] on [date of completion of the self-assessment] and supporting objective evidence of the documentation and implementation of the measures required for the CyberFundamentals assurance level "Basic" in the CyberFundamentals Framework version [version of the applicable CyberFundamentals Framework].

Conformance is established against the conditions in the Conformity Assessment Scheme version [version of the applicable Conformity Assessment Scheme].

This verification statement reflects only the situation at the point in time it is issued.

The framework and the Conformity Assessment Scheme are publicly available on www.cyfun.eu

BELAC 2-405 CyberFundamentals version R1-2026

Verification activities for the CyberFundamentals assurance levels Basic/Important **shall be performed under accreditation**. A verification statement may therefore **be issued only after accreditation has been formally granted for the relevant activity**. No verification statement may be issued prior to the accreditation decision, **even not** without reference to accreditation.

Certification Process CyFun® Essential

CENTRE FOR CYBERSECURITY BELGIUM

Applies to

- Assurance level **Essential**

Certification characteristics

- Management system–oriented
- 3-year cycle
- Initial → Surveillance → Recertification audits

Here, the focus shifts explicitly from "controls" to ***manageable capabilities****.*

Why CyFun® CAS Clarifications Are Integral (Not Optional)

CAS Clarifications define

- Required auditor / verifier competence
- How misstatements are handled
- How revised self-assessments are accepted
- Which **management-related controls** apply at AL Essential

Rule

- Clarifications are an **integral part of the CAS**
- CAB staff must be trained on them

Verifications & Audits: assessment of all controls

CENTRE FOR CYBERSECURITY BELGIUM

CyFun® Basic & Important (verification)

Key references
CAS Part II – Annex A & B
- *A.2.2 / B.2.2 Full verification program*
- *A.2.4.4 / B.2.4.4 Verification execution*

- Verification is **always based on the complete self-assessment**
- **All included controls are assessed** (no sampling approach)
- Any change in maturity score ⇒ **re-assessment of all affected controls**
- Key measures: always on-site; other controls: appropriate off-site/on-site verification

CyFun® Essential (audit / certification)

Key references
- CAS Annex C – C.2.2.2 *Planning*
- CAS Clarifications – Topic 3, §1 *CAS requirement*

- Initial and recertification audits **shall cover the complete CyberFundamentals set of requirements**
- **Management-related controls are mandatory in every audit**
  (initial, surveillance, and recertification)

Key takeaway

Under the CyFun® CAS there is **no selective assessment of controls**:

- Verifications (Basic/Important) → **all controls in the self-assessment**
- Audits (Essential) → **the full set of controls, including management aspects**

What This Means for CABs

For CABs already accredited for CyFun®

- Align procedures with Part II + Clarifications
- Ensure **competence** evidence is complete
- Apply consistent judgement across clients
- See points for “prospective” CABs

For prospective CABs

- Accreditation required
- Clear separation from consultancy
- Impartiality
- Annual reporting to the scheme owner

CyFun® CAS is a fully-fledged scheme under accreditation, not a lightweight framework.

Policy for Witnessing & Assessment Programme

Ref: BELAC 2-405 CyberFundamentals R1-2026

General

- The accreditation programme **always includes on-site witnessing** of CAB activities.
- Witnessing is **cluster-based** and covers both **verification (Basic/Important)** and **certification (Essential)** activities.

Initial accreditation

- **At least one witnessing per cluster**:
  - **ISO/IEC 17029 (Basic/Important)**: witnessing of a **full verification** (CAS A.2.2 / B.2.2).
  - **ISO/IEC 17021-1 (Essential)**: witnessing of **Stage 1 and Stage 2** of the certification audit. ➔ **Stage 1 witnessing shall be conducted on-site.**

Policy for Witnessing & Assessment Programme

Ref: BELAC 2-405 CyberFundamentals R1-2026

During the accreditation cycle

- **Minimum one witness audit per cluster per full accreditation cycle** (3 or 5 years), regardless of whether it concerns:
  - a **verification** (Basic/Important), or
  - a **certification audit** (Essential).
- For shorter accreditation cycles, the assessment programme is **defined case-by-case** by the NAB.

Extension of scope

- **Additional cluster(s)**: **at least one witness audit (≥ 1 day) per added cluster**.
- Extension **to or from Essential ↔ Basic & Important**:
  - appropriate witnessing (full verification or certification stages 1 & 2),
  - supplemented with technical and/or management-system audits as applicable.

Policy for Witnessing & Assessment Programme

Ref: BELAC 2-405 CyberFundamentals R1-2026

Extension of assurance level (CyFun® Basic/Important ⇔ CyFun® Essential)

- A CAB already accredited for CyFun® Basic/Important applying for accreditation for CyFun® Essential must undergo a **full accreditation audit with one witness present**.
- If the assessment is positive, the clusters already included in the scope of accreditation for CyFun® Basic/Important may also be included in the scope for CyFun® Essential.
- The same applies in the opposite direction.

Witnessing under CyFun® is systematic, cluster based and risk covering, with clear minimum requirements for initial accreditation, the accreditation cycle, and scope extensions.

CENTRE FOR CYBERSECURITY BELGIUM

NIS2 Authorisation conditions for CABs

Authorisation conditions for CABs

Authorisation conditions for Conformity Assessment Bodies (CABs) Version 02 February 2026

- How CABs obtain authorisation
- Which accreditation tracks are recognised
- What authorisation legally entails
- Ongoing obligations once authorised

Legal Context

Why Authorisation Is Required

- Belgian NIS2 Law (26 April 2024)
- Royal Decree NIS2 (09 June 2024)

Key principle

- Accreditation is necessary, but **not sufficient**.
- Authorisation by the CCB is mandatory.

Two Step Requirement

Accreditation + Authorisation

1. Accreditation

- By a National Accreditation Body
- Under EU Regulation 765/2008
- Operating under the IAF MLA

2. Authorisation

- Granted by the CENTRE FOR CYBERSECURITY BELGIUM
- Based on documented procedures and commitments

Recognised CAB Categories

Three Authorisation Tracks

- **Part I** – CyberFundamentals (CyFun®) accredited CABs
- **Part II** – ISO/IEC 27001 accredited CABs
- **Part III** – CABs accredited to other IT/OT standards

Each track:

- Has **specific authorisation conditions**
- Requires a **formal agreement with the** CENTRE FOR CYBERSECURITY BELGIUM

Common Core Conditions (All Tracks)

Applies to Every CAB

- Valid accreditation certificate
- Branch established in an EU NIS2 country
- That branch included in accreditation scope
- Legally binding agreement with the CCB
- CCB allowed to verify accreditation with the NAB
- Obligation to cooperate with CCB supervision
- Confidential handling of NIS2-related information

Authorisation Conditions

CAB must:

- Be accredited against the requirements of **ISO/IEC 17029** (in case of B/I) and the requirements of **ISO/IEC 17021-1** (in case of E), in combination with the requirements of the **CyFun® CAS**, including the **Clarifications**
- Use the scheme **without modification**
- Report annually to the CCB:
  - Verification statements
  - Refused claims
  - Complaints & appeals
  - Revised statements

Mandatory Procedures (CyFun® CABs)

What CABs Must Document

- Procedure to ensure **correct scope definition**
- Assessment must cover the **entire organisation**
- Exceptions only when IT/OT environments are:
  - Physically or technically separated
  - Proven not to affect in-scope risks
- Scope demarcation must be explicit and documented

Part II: ISO/IEC 27001 CABs

Why ISO/IEC 27001 Is Recognised

- ISO/IEC 27001 certification can support NIS2 compliance
- Included as an option in the BE NIS2 legislation

Authorisation Conditions

- **Accreditation** for ISO/IEC 17021-1, in combination with ISO/IEC 27006-1 for ISO/IEC 27001 certification is mandatory
  - **NAB** must operate under EU 765/2008 + IAF MLA + based in a country where the NIS 2 Directive applies.

- The CAB shall have a **branch** established in a country where the NIS 2 Directive applies.
  - The activities of that branch shall be included in the accreditation scope.

Additional Obligations for ISO/IEC 27001 CABs

Working in a NIS2 context goes beyond Standard Certification

CAB must:

- Upload each NIS2-related certificate + SoA to the CCB database
- Report annually on certificates, refusals, complaints, appeals
- Provide a **scope-definition procedure** (same logic as CyFun®)

See also BELAC 2-405 ISMS R5-2026 Chapter 5 Specific requirements applicable to the conformity assessment body related to the Belgian NIS2 regulation

SoA Equivalence Requirement (ISO Track)

Critical NIS2 Condition

ISO/IEC 27001 CABs must have a procedure ensuring that:

- The **Statement of Applicability**
- Demonstrates **equivalence** with CyFun®:
  - Basic
  - Important
  - Essential
- Assurance level determined via **risk analysis**
- **CyFun® Selection Tool is the preferred method**

Part III: Other IT / OT Standards

Applies to CABs accredited to:

- ISO/IEC 17029 or ISO/IEC 17021-1
- For IT/OT standards other than ISO/IEC 27001

Conditions largely mirror Part II:

- Accreditation + EU presence
- Annual reporting
- Uploading certificates
- Scope and SoA equivalence procedures required

Supervision & Enforcement

What Happens If Conditions Are Not Met

- Failure to cooperate → warning
- Repeated failures → warning
- Confirmed violations:
  - Formal notice
  - Suspension or revocation of authorisation

What Authorisation Really Means

Key Take-aways for CABs

- Authorisation is **regulatory trust**
- CABs act within a **national supervisory framework**
- Transparency and cooperation are mandatory
- Scope control and equivalence proof are non-negotiable

Authorisation is not a formality.
It is the condition that makes CAB activities
legally usable for NIS2 supervision.

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.