CyFun®

CyberFundamentals Framework
Conformity Assessment Scheme

Clarifications

Version : 26 November 2025

Document Change Log

Version	Reason for revision & Changes	Type of Revision
2024-03-15	Creation of the document	Entire document
2025-03-07	Introduction	No change
	Demonstration of required competence of auditors, verifiers and reviewers active in the CyFun® CAS	No change
	Further course when misstatements are identified during verifications	New chapter
2025-11-26	Introduction	Update – see (*)
	Demonstration of required competence of auditors, verifiers and reviewers active in the CyFun® CAS.	Update – see (**)
	Further course when misstatements are identified during verifications	Update – see (***)
	Including the controls linked to the management aspects of the Assurance Level "Essential", which was originally part of the CyFun® CAS identifying these controls in CyFun®2023 and CyFun®2025.	New chapter

(*) Clarifying that this document constitutes an integral component of the CyFun® CAS.

(**) Adding that the training 'ISASecure® ISA/IEC 62443 for Product Suppliers and Assessors' (IC47 - 3 days) is an acceptable alternative for IC32.

(***) Clarification on the acceptance of a revised Self-Assessment as a result of the verification.

Table of Contents

Introduction

1. General remarks

This document provides additional information about the most recent version of the CyberFundamentals Framework Conformity Assessment Scheme (CyFun® CAS) and constitutes an integral component of that scheme.

The document is accessible to National Accreditation Bodies, Conformity Assessment Bodies (CABs), verified and certified entities, and all other users of the CyberFundamentals Framework. It is provided electronically through the official website: www.cyfun.eu.

This CyberFundamentals Framework Conformity Assessment Scheme Clarifications document is a collection of several descriptive topics. Every of these topics has a clear link to the respective part of the CyFun® CAS.

The application of newly introduced or adapted rules is always two (2) months after publication of the relevant version, if not specified otherwise. In case of a new CyberFundamentals Framework version, the rules apply at the moment the new version is applicable.

Conformity assessment bodies shall ensure that relevant CAB personnel are trained on the CyberFundamentals Framework Conformity Assessment Scheme Clarifications (this document) relevant with their function within the CAB before the clarifications become effective. Proof of this training shall be available on request.

2. Definitions and acronyms

For the purposes of this document, the terms and definitions given in the most recent version of ISO/IEC 17000 and the following apply.

BELAC	BELAC is the Belgian National Accreditation Body. It was established by the provisions of the Royal Decree of January 31, 2006, and is placed under the responsibility of the FPS Economy, S.M.E.s, Self-employed and Energy.
CAB	Conformity Assessment Body All Conformity Assessment Bodies operating in the scheme shall be accredited by the National Accreditation Body (NAB) operating according to EU Regulation 765/2008 unless otherwise determined by national legislation.
CAS	Conformity Assessment Scheme
CCB	Centre for Cybersecurity Belgium, established by Royal Decree on October 10, 2014.
Control	A measure that is modifying risk. (Note: controls include any process, policy, device, practice, or other actions that modify risk). [Source: ISO/IEC 27000]
CyFun®	CyberFundamentals Framework
ISMS	Information Security Management System
Measure	In this publication, measure and control are used interchangeably and the definition of "Control" applies to both.
NAB	National Accreditation Body (in Belgium: BELAC)
NC	Non-Conformity

NCCA	National Cybersecurity Certification Authority
Overlap time	Extra time provided to carry out the necessary verification or certification activities to enable the continuity of a label and its associated QR code.
RD	Royal Decree
Requirement	Since the CyberFundamentals Framework is linked to a conformity assessment scheme, the measures in this framework are also a requirement and these terms are considered interchangeable in this context.
SoA	Statement of Applicability
TLP	Traffic Light Protocol

3. Disclaimer

This document has been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Belgian Royal Decree of 10 October 2014.

All texts, layouts, designs and other elements of any nature in this document are subject to copyright law. Reproduction of extracts from this document is authorised for non-commercial purposes only and provided the source is acknowledged.

This document contains technical information written mainly in English. This information related to the security of networks and information systems is addressed to IT/OT services which use the English terms of computer language. A translation into Dutch, French or German of this technical information is available at the CCB.

The CCB is responsible for maintaining the content of the document in line with the objectives of the CyberFundamentals Framework to provide a tool for organisations to demonstrate the implementation of protective measures to mitigate cybersecurity risks.

Since the scheme requirements are of a general nature and does not specify particular situations, specific guidance or implementation tools may be issued by the scheme owner to facilitate the use of the scheme.

Topic 1 - Demonstration of required competence of auditors, verifiers and reviewers active in the CyFun® Conformity Assessment Scheme

1. CAS requirement

Part II A.4.2.1 & **B.4.2.1** Competence requirements of verifiers and reviewers
Part II C.5.2.1 Competence requirements of auditors and reviewers

Technical knowledge relevant for the level CyberFundamentals Basic/Important/Essential (ICT/OT knowledge, NIST-CSF knowledge, CIS controls, ISO/IEC 27001, ISO/IEC 27002, IEC 62433 series).

2. Clarification

ICT/OT knowledge

Demonstrated by training certificates or equivalent through demonstrable experience.

NIST-CSF knowledge

For NIST-CSF, there are few specific training courses. Here, internal training that discusses the general structure of NIST-CSF and its relationship with the CyberFundamentals Framework is sufficient. Materials are freely available on the NIST website and www.cyfun.eu.
Minimum demonstrable evidence: internal certificate

CIS controls

For CIS, there are few specific training courses. Here, in-house training that discusses the CIS Critical Controls and their relationship with the CyberFundamentals Framework is sufficient. Material is freely available on the CIS website and www.cyfun.eu (mapping)
Minimum demonstrable evidence: internal certificate

ISO/IEC 27001

ISO/IEC 27001 training shall cover all clauses of the standard.
Minimum demonstrable evidence: internal or external certificate depending on the assurance level (see table below).

ISO/IEC 27002

ISO/IEC 27002 training shall cover all information security controls of the standard.
Minimum demonstrable evidence: internal or external certificate depending on the assurance level (see table below).

IEC 62443 series

The following parts of IEC 62443 shall be part of the training as a minimum:

Part 1-1 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts & Models
Part 2-1 Security for Industrial Automation and Control Systems: Security program requirements for IACS asset owners
Part 3-3 Security for industrial automation and control systems: System security requirements and security levels

The above is part of ISA/IEC 62443 Cybersecurity Fundamentals Specialist training from ISA (International Society of Automation) and lasts 2 days (training code IC32).
The training 'ISASecure® ISA/IEC 62443 for Product Suppliers and Assessors' (IC47 - 3 days) is an acceptable alternative for IC32.

These training courses are provided as examples; other programs covering at least the elements listed above are equally acceptable.

This training is only required when the compliance assessment is performed in an OT environment.

3. Acceptability of a certificate/attestation of internally provided training and required training per assurance level

Training provider	**BASIC**	**IMPORTANT**	**ESSENTIAL**
Internally provided (*)	NIST-CSF **and** CIS **or** ISO 27001/27002	NIST-CSF **or** CIS	NIST-CSF **and** CIS
Externally provided	▨	ISO 27001/27002 (IEC 62443**)	ISO 27001/27002 (IEC 62443**)

(*) this training can also be provided by an external training organisation
(**) only required when the compliance assessment is performed in an OT environment

4. Training institute requirements

There are no specific requirements towards the training institutes to be chosen.

Topic 2- Further course when misstatements are identified during verifications

1. CAS requirement

Part II A.2.4 & **B.2.4** Verification process

2. Definition of a misstatement

If, during the verification of the self-assessment, the assessor finds that the maturity level assigned by the organisation is not consistent with the supporting documentation or with the assessor's findings on site, this is considered a misstatement.

3. Clarification on what to do when misstatements are identified during verification

An organisation claims conformity with the assurance level Basic or Important. Not per CyFun® control but with the entirety of the controls that make up an assurance level.

For the various CyFun® controls, the verifier checks whether the evidence presented sufficiently supports the maturity level claimed by the organisation for that specific control. If there is insufficient evidence, the verifier identifies a misstatement that also prevents the maturity level for that CyFun® control from being retained.

For each verification, the verifier shall assess the extent (materiality) of the insufficiency of the evidence (documentary or on-site finding). In other words, to what extent the claimed maturity differs from what the verifier estimates him/herself based on the evidence presented.

When a key measure is involved, such a misstatement could possibly result in the failure to meet the threshold for that key measure. This ultimately leads to the rejection of the claim stating that the organisation is conforming to the assurance level Basic or Important.

Any misstatement will impact the overall maturity level. Again, the extent (significance) of the cumulative misstatements on the overall maturity level will have to be assessed and whether or not, as a result, the claim as a whole has to be rejected. It is still possible that the cumulation of misstatements, when no key measures are involved, does not compromise the threshold of the overall maturity level (Basic or Important).

The limit as to whether or not the submitted evidence is acceptable can be freely determined by the verifier, as the specific condition of the organisation shall be taken into account in each case. Therefore, there are the competence requirements for technical verifiers and there is the verifier's professional judgment.

If the aggregate of misstatements identified does not impact the total maturity level threshold, organisations do not need to take action. If it does have an impact and leads to rejection of the claim, the organisation will have to adjust and apply for a new verification with new evidence.

4. Clarification on the acceptance of a revised Self-Assessment as a result of the verification

According to ISO/IEC 17029:2019 and the principles of conformity assessment, the verification outcome shall be based on objective evidence and the professional judgment of the verification body. When, during the audit, the originally submitted self-assessment is found to contain a misstatement (e.g. an incorrectly assigned maturity level), the auditor shall consider the materiality of the misstatement (ISO/IEC 17029:2019 clause 9.5.4 b) by reassessing the maturity level based on the evidence provided.

If the reassessed maturity level still meets the required threshold for the claim, the claim is not materially incorrect under ISO/IEC 17029:2019. However, for transparency and traceability, the audited organisation has to accept the revised self-assessment and formally replace the original version with a new version and date. This ensures that the verification statement accurately reflects the version of the self-assessment that was evaluated and validated.

The verification statement has to confirm that the claim is materially correct as of the verification date, based on:

- The organisation's completed self-assessment, including its version and completion date.
- Supporting objective evidence demonstrating implementation of the measures required for the declared CyberFundamentals assurance level, in accordance with the applicable version of the CyberFundamentals Framework.

Therefore, the version and date referenced in the verification statement shall correspond to the revised and accepted self-assessment, not the original submission. This requirement does not constitute consultancy, as the auditor does not provide advice or recommendations for improvement but merely ensures that the documentation reflects the verified reality.

For transparency and traceability, the verifier shall describe and motivate all the revised and reassessed maturity levels based on the available evidence and discussed and accepted by the audited organisation, in the verification report.

5. Clarification on formally reporting findings made during verifications

Findings made during verifications shall be formally reported as provided in the CAS Part II A/B.2.4.4. 'Verification execution: The verification execution shall result in a documented report' with a clear content including 'Whether or not the collected evidence supports the self-assessment result and other obligations of the verification scheme.'

6. Clarification regarding time the organisation has for correcting misstatements identified during verification

A verification of a claim involves the organisation submitting a CyFun® Self-Assessment along with supporting evidence. It is not the intention that the assessor should search for evidence him/herself. The organisation cannot change a maturity level or correct a material misstatement within the same verification period to prevent making a materially incorrect claim.

7. Clarification regarding the time the organisation has for submission of new evidence regarding misstatements identified during verification

In a verification, other than a certification, the verification statement reflects the situation at the time the verification activity was performed.

If misstatements lead to the rejection of the claim, a new verification will have to be requested.

If previously identified misstatements do not result in the rejection of the claim, any subsequent verification request may require an extended assessment period to review and address those discrepancies.

8. Clarification regarding the statement in case of an unconfirmed self-assessment

No negative statement is provided. The CyFun® CAS follows the provision of ISO/IEC 17029:2019 clause 9.7.1.4 without additions.

Topic 3 – Controls linked to the management aspects of the Assurance Level “Essential”

(New topic in this version of the CAS CyberFundamentals Clarifications)

1. CAS requirement

Part II C.2.3, C.3 & C.4 Certification process

In addition to the key measures, the controls linked to the management aspects shall be evaluated in every audit (initial audit, surveillance audit or recertification audit) for the assurance level “Essential”.

2. Review of any changes

Changes that may affect the capability of the management system to continue to fulfil the requirements of the CyberFundamentals Framework.

3. Use of marks and reference to certification

See CyFun® CAS PART III Assurance Level Labelling as appropriate.

4. Controls linked to the management aspects in CyFun®

The following controls are identified as controls linked to the management aspects in CyFun®. The various management aspects are grouped by topic, clearly indicating where this is covered in CyFun®2023 and CyFun®2025.

4.1. Internal audits

		CyFun® 2023	**CyFun® 2025**
1.a.	Internal audit	Applicable for CyFun® Through the self-assessment	
1.b.	The organization shall conduct specialised assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the organisation's critical systems.	DE.DP-5.2	ID.IM-03.9

4.2. Management review, continuing operational control and effectiveness of the management system

		CyFun® 2023	**CyFun® 2025**
2.a.1	Information security and cybersecurity roles, responsibilities and authorities within the	ID.AM-6.1	

		CyFun® 2023	CyFun® 2025
	organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.		
2.a.2	Information security and Cybersecurity roles, responsibilities and authorities for employees, suppliers, customers, and partners shall be documented, reviewed, authorised, kept up to date, communicated, and coordinated internally and externally.		GV.RR-02.1
2.b.1	The organization shall appoint an information security officer.	ID.AM-6.2	
2.b.2	The organisation shall appoint a senior-level executive information security officer.		GV.RR-02.2
2.c.1	Information security and cybersecurity risks shall be documented, formally approved, and updated when changes occur.	ID.GV-4.2	
2.c.2	Information and Cybersecurity risks shall be documented, as part of the enterprise risk management processes, formally approved by senior management, and updated when changes occur.		GV.RM-03.2
2.d.1	A cyber risk management process that identifies key internal and external stakeholders and facilitates addressing risk-related issues and information shall be created, documented, reviewed, approved, and updated when changes occur.	ID.RM-1.1	
2.d.2	Information and cybersecurity objectives shall be coherently established throughout the organisation and approved by senior management.		GV.RM-01.1
2.e.1	The organization shall clearly determine it's risk appetite.	ID.RM-2.1	
2.e.2	Risk appetite and risk tolerance statements shall be defined, documented, approved by senior management, communicated, and maintained.		GV.RM-02.1
2.f.1	The organization shall document, review, approve, update when changes occur, and implement a cyber supply chain risk management process that supports the identification, assessment, and mitigation of the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains.	ID.SC-1.1	
2.f.2	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes shall be documented, reviewed,		GV.SC-01.1

		CyFun® 2023	CyFun® 2025
	updated when changes occur, and approved by organisational stakeholders.		
2.g.	The organisation shall conduct and document risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and likelihood of their occurrence.	ID.RA-5.2	ID.RA-05.2
2.h.	Risk assessment results shall be disseminated to relevant stakeholders.	ID.RA-5.3	ID.RA-05.3
2.i.1	Capacity planning shall ensure adequate resources for organization's critical system information processing, networking, telecommunications, and data storage.	PR.DS-4.1	
2.i.2	Adequate resource capacity planning shall ensure that availability of organisation's critical system information processing, networking, telecommunications, and data storage is maintained.		PR.IR-04.1
2.j.1	Incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) shall be established, maintained, approved, and tested to determine the effectiveness of the plans, and the readiness to execute the plans.	PR.IP-9.1	
2.j.2	Contingency and continuity plans shall be established, communicated, maintained, tested, validated, and improved.		ID.IM-04.1
2.k.1	The organization shall coordinate the development and the testing of incident response plans and recovery plans with stakeholders responsible for related plans.	PR.IP-9.2	
2.k.2	The organisation shall coordinate the development and the testing of Incident Response Plans and other cybersecurity plans that affect operations with stakeholders to ensure that these plans align with overall organisational goals and enhance resilience.		ID.IM-04.2

4.3. Review of actions taken on non-conformities identified during the previous audit; Evaluation of execution of action plans for non-key measures for which an action plan was approved.

4.4. Complaints handling

		CyFun® 2023	CyFun® 2025
4.a.1	Negative impacts to organization’s operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.	DE.AE-4.1	
4.a.2	The organisation shall assess the negative impacts of detected events on its operations, assets, and individuals, and shall link these impacts to the results of its risk assessments.		DE.AE-04.1
4.b.1	The organization shall communicate recovery activities to predefined stakeholders, executive and management teams.	RC.CO-3.1	
4.b.2	Recovery activities and progress in restoring operational capabilities shall be communicated to designated internal and external stakeholders in accordance with established communication procedures.		RC.CO-03.1

4.5. Progress of planned activities aimed at continual improvement

		CyFun® 2023	CyFun® 2025
5.a.1	A comprehensive strategy shall be developed and implemented to manage risks to the organization’s critical systems, that includes the identification and prioritization of risk responses.	ID.RA-6.1	
5.a.2	Risk responses shall be identified, prioritised, planned, tracked and communicated.		ID.RA-06.1
5.b.	Improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned, shall be incorporated into detection process revisions.	DE.DP-5.1	(*)
5.c	The organization shall conduct specialized assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the organization's critical systems. *(also covering 1.b Internal Audits)*	DE.DP-5.2	ID.IM-03.9

(*) In CyFun®2025 the control DE.DP-5.1 from CyFun®2023 has been withdrawn and its intent has been embedded in the governance and improvement controls introduced at the Important and Essential assurance levels. The principle of integrating lessons learned and continuous improvement is addressed through:

- Governance measures that require oversight and review of cybersecurity performance.
- Improvement controls that mandate the incorporation of feedback and monitoring results into updated processes.
- Self-assessment tools that include spider diagrams and maturity indicators to track and improve detection capabilities over time.