CENTRE FOR CYBERSECURITY BELGIUM

CyberFundamentals Framework Conformity Assessment Scheme

Clarifications

Version : 28 October 2024

CENTRE FOR CYBERSECURITY BELGIUM

Document Change Log

Version	Reason for revision & Changes	Type of Revision
2024-03-15	Creation of the document	Entire document
2024-10-28	Introduction	No change
	Demonstration of required competence of auditors, verifiers and reviewers active in the CyFun® CAS	No change
	What happens when misstatements are identified during verifications	New chapter

CENTRE FOR CYBERSECURITY BELGIUM

Table of Contents

CENTRE FOR CYBERSECURITY BELGIUM

Introduction

1. General remarks

This document provides additional clarification to the CyberFundamentals Framework Conformity Assessment Scheme (CyFun® CAS) and is available to the National Accreditation Bodies, Conformity Assessment Bodies (CAB), verified and certified entities and all other users of the CyberFundamentals Framework. The document is made available electronically at www.cyfun.be or www.cyfun.eu.

This CyberFundamentals Framework Conformity Assessment Scheme Clarifications document is a collection of several descriptive documents. Every of these documents has a clear link to the respective part of the CyFun® CAS. For traceability reasons, every of these documents also has its own version.

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 is trained on the Introduced clarifications according to their function within the CAB before the rules come into force. A 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 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 and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

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.

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.be or 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.be (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 62433 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: Establishing an Industrial Automation and Control Systems Security Programme
Part 3-3 Security for industrial automation and control systems: System security requirements and security levels

The above are part of ISA/IEC 62443 Cybersecurity Fundamentals Specialist training from ISA (International Society of Automation) and lasts 2 days (training code IC32). This training is just an example, other training courses that include at least the above parts are perfectly 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.

CENTRE FOR CYBERSECURITY BELGIUM

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

For each audit, the assessor must 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 assessor 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 assessor, as the specific condition of the organisation must be taken into account in each case. Therefore, there are the competence requirements for technical assessors and there is the assessor'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 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.'

5. 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 does not have the opportunity to adjust in the time span of the same verification activity.

6. 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 misstatements do not lead to the rejection of the claim, a subsequent verification request may result in extending the assessment time to check what happened to the previously identified discrepancies.

7. 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.