

CyberFundamentals Framework Conformity Assessment Scheme

Version : 20 November 2023

Document Change Log

Version	Reason for revision	Type of Revision
2023-11-20	New document - Document created in consultation with BELAC	Full document

Table of Contents

Introduction	4
1. General remarks	4
2. Normative References	5
3. Definitions and acronyms	5
4. Disclaimer	6
PART I CyberFundamentals Framework Requirements	7
1. Assurance levels	7
2. Key measures	7
3. Location and applicable version	7
PART II Assessment of the CyberFundamentals Framework	8
1. General remarks	8
2. CyberFundamentals assessment Overview	8
Annex A Assessment of the CyberFundamentals Framework Assurance Level “BASIC”	9
Annex B Assessment of the CyberFundamentals Framework Assurance Level “IMPORTANT”	17
Annex C Assessment of the CyberFundamentals Framework Assurance Level “ESSENTIAL”	25
Annex D Self-Assessment tool	35
Annex E Assessment time chart	37
Annex F Requirements for the National Accreditation Body (NAB)	39
Annex G (informative) Mapping towards ISO/IEC 17029 and ISO/IEC 17021-1	41
PART III Assurance Level Labelling	46
1. General remarks	46
2. CyberFundamentals labelling overview	46
Annex A CyberFundamentals Framework Assurance Level “BASIC” label	47
Annex B CyberFundamentals Framework Assurance Level “IMPORTANT” label	49
Annex C CyberFundamentals Framework Assurance Level “ESSENTIAL” label	51
Annex D Eligibility for labelling through ISO/IEC 27001 certification	53
Annex E Rules on the use of CyberFundamentals labels	54
PART IV Key Measures of the CyberFundamentals Framework	56

Introduction

1. General remarks

The CyberFundamentals Framework is a framework owned by the Centre for Cybersecurity Belgium (CCB), operating under the authority of the Prime Minister of Belgium.

By Royal Decree of 16 October 2022 the CCB is designated as the National Cybersecurity Certification Authority (NCCA). The operational activities of the NCCA are carried out by the CCB Certification Authority, a department of the CCB.

As scheme owner, the Centre for Cybersecurity Belgium (CCB) is responsible for maintaining the content of the framework's related documents in line with the following objectives:

- For the assurance level “Basic” and “Important”, achieve trust towards customers, suppliers and regulators through an independent and technically correct assessment of the statement regarding the cybersecurity measures taken.
- For the assurance level “Essential” achieve trust towards customers, suppliers and regulators through an independent and technically correct assessment of the implementation of a management system to manage and adjust the tangible and implemented cybersecurity measures.

Since the requirements of the framework are general in nature and do not specify specific situations, the owner of the framework may issue specific guidelines or implementation tools to facilitate the use of the framework.

The framework is available for voluntary as well as mandatory use.

- In case of voluntary use, it shall be considered in combination with this conformity assessment program as National Conformity Assessment Scheme for Cybersecurity in execution of the CCB's legal mission (RD 10 Oct 2014, Art. 3 8°).
- For mandatory use of the conformity assessment scheme, the laws and regulations imposing the mandatory use shall apply.

Conformity assessment of the CyberFundamentals Framework shall be performed by an accredited conformity assessment body operating according to EU Regulation 765/2008 setting out the requirements for accreditation and market surveillance unless otherwise determined by national legislation.

The scheme owner evaluates and manages the scheme with relevant stakeholders in accordance with IAF MD 25.

The CyberFundamentals Framework is available on www.cyfun.be .

2. Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17000	Conformity assessment - Vocabulary and general principles
ISO/IEC 17021-1	Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements
ISO/IEC 17029	Conformity Assessment - General principles and requirements for validation and verification bodies
ISO 19011	Guidelines for auditing management systems
ISO/IEC 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary
ISO/IEC 27001	Information security, cybersecurity and privacy protection - Information security management systems - Requirements
ISO/IEC 27002	Information security, cybersecurity and privacy protection - Information security controls
ISO/IEC 27006	Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing
IEC 62433	The IEC 62443 series of standards define requirements and processes for securing industrial automation and control systems (IACS) throughout their lifecycle.
IAF ID 1	IAF Informative Document for QMS and EMS Scopes of Accreditation
IAF MD 2	IAF Mandatory document for the transfer of accredited certification of management systems.
IAF MD 25	IAF Mandatory Document - Criteria for evaluation of conformity assessment schemes.

3. 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

4. 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.

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.

PART I CyberFundamentals Framework Requirements

1. Assurance levels

The CyberFundamentals Requirements are available for three assurance levels:

Basic

The assurance level Basic contains the standard information security measures for all enterprises. These provide an effective security value with technology and processes that are generally already available. Where justified, the measures are tailored and refined.

Important

The assurance level Important is designed to minimise the risks of targeted cyber-attacks by actors with common skills and resources in addition to known cyber security risks.

Essential

The assurance level Essential goes one step further and is designed to address the risk of advanced cyber-attacks by actors with extensive skills and resources.

2. Key measures

The key measures are an essential element of the CyberFundamentals Framework. Part IV of this Conformity Assessment Scheme provides an overview of the key measures for assurance level “Basic”, assurance level “Important” and assurance level “Essential”. For assurance level “Essential” a specific set of controls is defined that are linked to the management aspects. The latter shall be audited during every audit.

Key measures build up as the assurance level increases. This means that for assurance level important, the key measures of level basic must also be met. For assurance level essential, the key measures of levels basic and important must also be met.

3. Location and applicable version

The CyberFundamentals Framework is only available online on the website www.cyfun.be. Guidance documents and tools are included in the CyFun-Toolbox available online on the website www.cyfun.be.

Conformity assessment will always be done against the latest version published on www.cyfun.be. Unless a transition regulation decides otherwise, which will be communicated on www.cyfun.be.

PART II Assessment of the CyberFundamentals Framework

1. General remarks

The requirements in Annex A and B of Part II shall be read by the Conformity Assessment Body in addition to the requirements of ISO/IEC 17029 (General principles and requirements for validation and verification bodies).

The requirements in Annex C of Part II shall be read by the Conformity Assessment Body in addition to the requirements of ISO/IEC 17021-1 (Requirements for bodies providing audit an certification of management systems).

2. CyberFundamentals assessment Overview

	BASIC	IMPORTANT	ESSENTIAL
Type of assessment	Verification	Verification	Certification
Assessment method	Verification of self-assessment	Verification of self-assessment	Certification audit
Assessment performed by	Accredited CAB	Accredited CAB	Accredited CAB
Accreditation standard	ISO/IEC 17029	ISO/IEC 17029	ISO/IEC 17021-1
Frequency	The verification statement reflects only the situation at the point in time it is issued. There is no repetitive cycle.		3yrs repetitive cycle Year 0: Complete Year 1&2: partial (surveillance)
Assurance evidence	Verified Claim	Verified Claim	Certificate

Annex A Assessment of the CyberFundamentals Framework Assurance Level “BASIC”

A.1. Type of Claim

The claim shall be provided in the form of a statement and a completed self-assessment. The statement shall declare the organizations conformance with the requirements of the CyberFundamentals assurance level “Basic” in accordance with the conditions specified in clause ‘A.2.4.4 Verification Execution’ of the CyberFundamentals Conformity Assessment Scheme.

To this end, the claim shall include:

- The organizations name, address and company number. The organization is the object of the verification. The conformance with the requirements for the CyberFundamentals assurance level “Basic” can only be claimed for the organization as a whole and no activities or processes can be excluded (see NOTE);
- The cluster and IAF code applicable to the organisation's activities;
- The organisation's statement that its operation meets the requirements of the CyberFundamentals assurance level “Basic”;
- The version of the self-assessment that is subject of the claim and date of completion of the self-assessment;
- The version of the CyberFundamentals Framework that is subject of the claim;
- The version of the applicable CyberFundamentals Conformity Assessment Scheme.

NOTE: In principle, the conformity assessment involves an organization as a whole, unless IT/OT environments are physically and/or technically separated. The separation shall be performed in such a way that the environments out of scope do not influence the risks of the environment in scope. In any case, this shall be clarified in the scope of the conformity assessment.

A.2. Verification program

A.2.1. Input for the verification

The input for a verification activity to be provided by the applicant to the Conformity Assessment Body (CAB) shall consist of the following:

- The claim as detailed in A.1. above.
- The Self-assessment report for assurance level “Basic” (output of the Self-Assessment tool further detailed in Part II-Annex D) that demonstrates a total maturity level higher than or equal to 2,5/5 and a maturity level for each key measure higher than or equal to 2,5/5.
- Appropriate evidence to support the maturity self-assessment. The submitted evidence includes the completed ‘details’ tab from the Self-Assessment tool (see Part II-Annex D), and information or reference thereto regarding the verification of key measures.
- Maximum 1 CyberFundamentals measure that the organisation wants to exclude from the scope of the claim; Can not be excluded: Key measures as defined in clause A in part IV of this CAS;
- Motivation for the from the scope excluded CyberFundamentals measure (maximum 1).
- Objective evidence or reference to the verification regarding the use of symbols/logo’s/marks;

- Objective evidence or reference to the verification collected by the applicant during onsite verification on the key measures to be verified. The verifier shall have access to the relevant information;
- The verification report of the previous verification.

A.2.2. Full verification program

Full verification is carried out by a Conformity Assessment Body (CAB) based on documentary verification of the self-assessment and applicable supporting documentation, and on-site verification of all key measures.

The verification shall take at least 1,5 person-days, of which at least 1 day (8 hours) shall be conducted on site. More detail on verification time is provided in Part II-Annex E.

A full verification program shall be carried out every 3 years.

The self-assessment results in a maturity score. Any change in that maturity score compared to the previous self-assessment assessed by the CAB shall trigger an extension of verification to all changes in the self-assessment, regardless of whether those changes have a positive or negative impact. The assessment time is extended by the time needed to assess that changed maturity score.

The Conformity Assessment Body shall determine the location of the verification (off site or on site) to ensure appropriate verification.

A.2.3. Limited verification program

The baseline of a limited verification program is a fully verified claim that is not older than 30 months (2,5 years).

The verification statement may be renewed by the same Conformity Assessment Body on the basis of a limited verification program, by documentary verification of the updated self-assessment of which the total maturity level is not lower than the previous self-assessment or has a total maturity level higher than 3,5/5.

A limited verification program can only be applied to an environment that is neither physically nor technically modified, except for improvements that do not negatively impact the risks of the environment in scope. In any case, any change in scope will trigger a full verification.

The limited verification shall consider at least half of the key measures. Those key measures shall be selected, after review of the previous verification report, on the basis of the following criteria:

- Each key measure involved in a change
- For unchanged scores, priority is given to those key measures not verified in the previous verification. This implies that the Conformity Assessment Body (CAB) shall maintain a verification plan.

All verification activities are performed by a Conformity Assessment Body .

The minimal duration of the limited verification will be 0,5 person-day and will be extended to cover changed key measures. More detail on verification time is provided in Part II-Annex E.

The Conformity Assessment Body shall determine the location of the verification (off site or on site) to ensure appropriate verification.

A.2.4. Verification process

A.2.4.1. Pre-engagement

The Conformity Assessment Body shall require the applicant to submit information sufficient to carry out a pre-engagement review. 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.

A.2.4.2. Engagement

The Conformity Assessment Body shall have a legally enforceable agreement with the applicant that includes an agreement on confidentiality of the information that is subject of the verification activities.

The latter implies that the information exchanged between the applicant and the CAB is labelled according to the TLP protocol.

The agreement shall include, as appropriate, the required security clearance.

The retention period for the obtained information shall be agreed upon but shall not be shorter than the minimum retention period as described below.

The agreement shall include a statement that reports and other evidence may be requested by the Centre for Cybersecurity Belgium.

A.2.4.3. Planning

The CAB shall plan the verification of the claim and determine what activities are needed to collect the necessary evidence to complete the verification. Based on this, a verification plan shall be drawn up.

The Conformity Assessment Body shall, where relevant, communicate the required security clearance to the team taking into account the requirements of the National Security Authority.

A.2.4.4. Verification execution

The CAB shall perform the verification execution activities in accordance with the verification plan.

During the verification following information is collected:

- Objective evidence or reference to the verification on the use of marks/logo's/symbols.
- Objective evidence or reference to the verification collected by the verifier during onsite verification on the key measures to be verified. The verifier shall have access to the relevant information.

- When during a limited verification there is a reasonable doubt on the validity of the claim, a specific verification can be performed on site or via remote verification on the elements of doubt.
- Verification of the result of the maturity self-assessment with the obtained information. The verification verifies the fulfilment of the requirement as well as the scoring of the relevant element(s) in the self-assessment.

The claim can only be confirmed as successfully verified at the assurance level “Basic” when the following conditions are met:

Key Measures	13*
	≥ 2,5/5 for each key measure
Total Maturity level	≥ 2,5/5 (see self-assessment tool – summary tab)

(*) See Part IV of this CAS

For the measures excluded from the scope, the values are assigned as described in Part II - Annex D.3

The verification execution shall result in a documented report, the verification report, containing at least the following:

- Points of evaluation and evaluation results.
- Reference to the objective evidence.
- The completed maturity self-assessment that was used as input for the verification activity.
- Whether or not the collected evidence supports the self-assessment result and other obligations of the verification scheme.
- Location, date, time and duration of the verification on site and remote.
- Verification result of the motivation for exclusion for maximum 1 requirement.
- A conclusion stating whether or not the claim is materially correct at a given point in time, for the predefined scope and based on the evaluation of objective evidence, and meets the requirements for the CyberFundamentals assurance level “Basic”.

A.2.4.5. Review

The review of the verification report shall be carried out by persons who have not been involved in the verification, and who meet the competence requirements in A.4.2.

The review activities consist of an independent review of the verification report and shall be documented including at least the following:

- Date
- Reviewers
- Outcome of the review
- Review of the appointed verifiers (including the confirmation of competence and impartiality).

A.2.4.6. Decision and issue of the verification statement

Upon completion of the verification review the decision shall be made on whether or not to confirm the claim.

The decision shall be made by persons who have not been involved in the verification execution and who meet the competence requirements in A.4.2.

The decision shall be documented including at least the following:

- Date
- Decision makers
- result of the decision-making process including
 - Whether or not a verification statement can be issued.
 - Motivation of the decision taken.
 - The review of the appointed reviewers and verifiers (including the confirmation of competence and impartiality).

The issue of the verification statement is discussed in A.3.

A.2.4.7. Retention of verification documents

The verification statements, input, output, reporting, review and decision shall be retained for a minimum of 5 years by the Conformity Assessment Body .

A.3. Verification statement

A successful full (A.2.2) or limited verification (A.2.3) leads to a verification statement for which the following wording shall be used:

[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 be conform with 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.be

The verification statement shall include:

- Name, address and company number of the Conformity Assessment Body;
- The relevant sector and subsector to which the organisation to which the verification applies belongs and referred to in A.4.2.1 and governing legislation, as applicable;
- The date and the unique identification of the statement;

- Conformity Assessment Body mark/logo/symbol;
- National Accreditation Body mark/logo/symbol and the accreditation certificate number, as prescribed by the NAB.

All logo's and marks shall be of the same or comparable size and they shall not be misleading or ambiguous.

A.4. Requirements for verifiers, reviewers and decision makers

A.4.1. Impartiality requirements

In addition to the normative requirements, the personnel involved in the review process (verifiers, reviewers and decision makers) shall not have been involved in consultancy for that organization for a period of 5 years.

Consultancy includes, but is not limited to, the following activities:

- In-house, specific or dedicated training on policies or security measures other than generic training (see below)
- Engineering of policies and security measures
- Technical assistance from conception through implementation of policies and/or security measures

Consultancy does not include:

- Use of shared information and resources (for example: the same vulnerability database,...)
- Generic training (from a public list of pre-established training) carried out for multiple organizations, without specific case studies of the organization involved.

Note: internal audit is not considered as consultancy, but it is not compatible with the activities of independent third-party assessments.

The internal auditor shall not be employed or hired by the Conformity Assessment Body to reduce the risk of familiarity and impartiality (internal auditor's relationship with verifiers).

Where a consultant is or was involved in the implementation of the security measures or the security program during the last two years, and that consultant is also employed by or has a contract with the Conformity Assessment Body, the Conformity Assessment Body may not accept the verification request.

No part of the verification shall be outsourced.

Records shall be retained by the conformity assessment body for a minimum of five years after the last assessment of the audit client.

A.4.2. Competence requirements

In addition to the normative requirements in ISO/IEC 17029, the following requirements are also applicable.

A.4.2.1. Competence requirements of verifiers and reviewers

The verifiers and reviewers of the CyberFundamentals Framework shall have demonstrated competence in:

- Technical knowledge relevant for the level CyberFundamentals Basic (ICT/OT knowledge, NIST-CSF knowledge, CIS controls, ISO/IEC 27001, ISO/IEC 27002, IEC 62433 series)
- Auditing skills according to ISO 19011 and Chapter 7 of ISO/IEC 27007
- The business context of the verified company

The knowledge of the business requirements is determined according to the following clustering (in accordance with IAF ID1):

Cluster	IAF Code	Description of economic sector / activity
Production/ products	All other	
Transport	31	Transport, storage and communication
Supply	25	Electricity supply
	26	Gas supply
	27	Water supply
Services	34	Engineering services
	32	Financial intermediation, real estate, renting
	35	Other services
	36	Public administration
	37	Education
	38	Health and social services
	39	Other social services
Information technology	33	Information technology
Nuclear	11	Nuclear fuel
Aerospace	21	Aerospace

It is accepted that the qualification on the business context can be obtained through other schemes operating under accreditation.

Where a team of verifiers performs the verification, the lead verifier shall have full competence. Other verifiers in the team shall only verify security measures for which they are technically competent.

Verifiers shall be monitored on the CyberFundamentals Framework for at least 1 verification per year (onsite + documentary). When they are qualified for different business contexts, they shall be monitored for each cluster at least once every 5 years. For the monitoring related to the business context also other schemes can be used when the assessment is performed under accreditation.

Records shall be retained by the conformity assessment body for a minimum of five years after the last assessment of the audit client.

A.4.2.2. Competence requirements of decision makers

The decision makers shall have competence on

- The business context of cybersecurity
- The CyberFundamentals Framework (in general)

Where the decision making is done by a group, the competences shall be present as a group.

Records shall be retained by the conformity assessment body for a minimum of five years after the last assessment of the audit client.

A.4.2.3. Security clearance

Where relevant, security clearance applies to the verifier, reviewer and decision-makers, as they shall have access to the full documentation of the verification program. Where a security clearance applies, all parties involved act in accordance with the clearance level and the requirements of the National Security Authority.

A.5. Collaboration between the scheme owner and the Conformity Assessment Body

The Centre for Cybersecurity Belgium is the scheme owner.

Conformity Assessment Bodies are required to have a legally binding agreement with the scheme owner. This agreement will enforce the use of the scheme without limitations or additions and will require collaboration with the scheme owner.

The Conformity Assessment Bodies are required to provide a yearly report to the scheme owner with the following data:

- List of verification statements + contact
- List of refused claims
- Complaints (received, treated)
- Revised verification statements

The Conformity Assessment Body is obliged to cooperate on any request from the CCB regarding the verification activities. If security clearance is required to access the information, the CCB will take the necessary steps to apply the required measures.

Annex B Assessment of the CyberFundamentals Framework Assurance Level “IMPORTANT”

B.1. Type of Claim

The claim shall be provided in the form of a statement and a completed self-assessment. The statement shall declare the organizations conformance with the requirements of the CyberFundamentals assurance level “Important” in accordance with the conditions specified in clause ‘B.2.4.4 Verification Execution’ of the CyberFundamentals Conformity Assessment Scheme.

To this end, the claim shall include:

- The organizations name, address and company number. The organization is the object of the verification. The conformance with the requirements for the CyberFundamentals assurance level “Important” can only be claimed for the organization as a whole and no activities or processes can be excluded (see NOTE);
- The cluster and IAF code applicable to the organisation's activities;
- The organisation's statement that its operation meets the requirements of the CyberFundamentals assurance level “Important”;
- The version of the self-assessment that is subject of the claim and date of completion of the self-assessment;
- The version of the CyberFundamentals Framework that is subject of the claim;
- The version of the applicable CyberFundamentals Conformity Assessment Scheme.

NOTE: In principle, the conformity assessment involves an organization as a whole, unless IT/OT environments are physically and/or technically separated. The separation shall be performed in such a way that the environments out of scope do not influence the risks of the environment in scope. In any case, this shall be clarified in the scope of the conformity assessment.

B.2. Verification program

B.2.1. Input for the verification

The input for a verification activity to be provided by the applicant to the Conformity Assessment Body (CAB) shall consist of the following:

- The claim as detailed in A.1. above.
- The Self-assessment report for assurance level “Important” (output of the Self-Assessment tool further detailed in Part II-Annex D) that demonstrates a total maturity level higher than or equal to 3/5 and a maturity level for each key measure higher than or equal to 3/5.
- Appropriate evidence to support the maturity self-assessment. The submitted evidence includes the completed ‘details’ tab from the Self-Assessment tool (see Part II-Annex D), and information or reference thereto regarding the verification of key measures.
- Maximum 3 CyberFundamentals measures that the organisation wants to exclude from the scope of the claim; Can not be excluded: Key measures as defined in clauses A and B in part IV of this CAS;
- Motivation for each of the from the scope excluded CyberFundamentals measures (maximum 3).

- Objective evidence or reference to the verification regarding the use of symbols/logo's/marks;
- Objective evidence or reference to the verification collected by the applicant during onsite verification on the key measures to be verified. The verifier shall have access to the relevant information;
- The verification report of the previous verification.

B.2.2. Full verification program

Full verification is carried out by a Conformity Assessment Body (CAB) based on documentary verification of the self-assessment and applicable supporting documentation, and on-site verification of all key measures.

The verification shall take at least 1,5 person-days, of which at least 1 day (8 hours) shall be conducted on site. More detail on verification time is provided in Part II-Annex E.

A full verification program shall be carried out every 3 years.

The self-assessment results in a maturity score. Any change in that maturity score compared to the previous self-assessment assessed by the CAB shall trigger an extension of verification to all changes in the self-assessment, regardless of whether those changes have a positive or negative impact. The assessment time is extended by the time needed to assess that changed maturity score.

The Conformity Assessment Body shall determine the location of the verification (off site or on site) to ensure appropriate verification.

B.2.3. Limited verification program

The baseline of a limited verification program is a fully verified claim that is not older than 30 months (2,5 years).

The verification statement may be renewed by the same Conformity Assessment Body on the basis of a limited verification program, by documentary verification of the updated self-assessment of which the total maturity level is not lower than the previous self-assessment or has total maturity level higher than 4/5.

A limited verification program can only be applied to an environment that is neither physically nor technically modified, except for improvements that do not negatively impact the risks of the environment in scope. In any case, any change in scope will trigger a full verification.

The limited verification shall consider at least half of the key measures. Those key measures shall be selected, after review of the previous verification report, on the basis of the following criteria:

- Each key measure involved in a change
- For unchanged scores, priority is given to those key measures not verified in the previous verification. This implies that the Conformity Assessment Body (CAB) shall maintain a verification plan.

All verification activities are performed by a Conformity Assessment Body .

The minimal duration of the limited verification will be 0,5 person-day and will be extended to cover changed key measures. More detail on verification time is provided in Part II-Annex E.

The Conformity Assessment Body shall determine the location of the verification (off site or on site) to ensure appropriate verification.

B.2.4. Verification process

B.2.4.1. Pre-engagement

The Conformity Assessment Body shall require the applicant to submit information sufficient to carry out a pre-engagement review. 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.

B.2.4.2. Engagement

The Conformity Assessment Body shall have a legally enforceable agreement with the applicant that includes an agreement on confidentiality of the information that is subject of the verification activities.

The latter implies that the information exchanged between the applicant and the CAB is labelled according to the TLP protocol.

The agreement shall include, as appropriate, the required security clearance.

The retention period for the obtained information shall be agreed upon but shall not be shorter than the minimum retention period as described below.

The agreement shall include a statement that reports and other evidence may be requested by the Centre for Cybersecurity Belgium.

B.2.4.3. Planning

The CAB shall plan the verification of the claim and determine what activities are needed to collect the necessary evidence to complete the verification. Based on this, a verification plan shall be drawn up.

The Conformity Assessment Body shall, where relevant, communicate the required security clearance to the team taking into account the requirements of the National Security Authority.

B.2.4.4. Verification execution

The CAB shall perform the verification execution activities in accordance with the verification plan.

During the verification following information is collected:

- Objective evidence or reference to the verification on the use of marks/logo's/symbols.
- Objective evidence or reference to the verification collected by the verifier during onsite verification on the key measures to be verified. The verifier shall have access to the relevant information.

- When during a limited verification there is a reasonable doubt on the validity of the claim, a specific verification can be performed on site or via remote verification on the elements of doubt.
- Verification of the result of the maturity self-assessment with the obtained information. The verification verifies the fulfilment of the requirement as well as the scoring of the relevant element(s) in the self-assessment.

The claim can only be confirmed as successfully verified at the assurance level “Important” when the following conditions are met:

Key Measures	13 (Basic) + 8 (Important)*
	≥ 3/5 for each key measure
Total Maturity level	≥ 3/5 (see self-assessment tool – summary tab Important)

(*) See Part IV of this CAS

For the measures excluded from the scope, the values are assigned as described in Part II - Annex D.3

The verification execution shall result in a documented report, the verification report, containing at least the following:

- Points of evaluation and evaluation results.
- Reference to the objective evidence.
- The completed maturity self-assessment that was used as input for the verification activity.
- Whether or not the collected evidence supports the self-assessment result and other obligations of the verification scheme.
- Location, date, time and duration of the verification on site and remote.
- Verification result of the motivation for exclusion for maximum 3 measures.
- A conclusion stating whether or not the claim is materially correct at a given point in time, for the predefined scope and based on the evaluation of objective evidence, and meets the requirements for the CyberFundamentals assurance level “Important”.

B.2.4.5. Review

The review of the verification report shall be carried out by persons who have not been involved in the verification, and who meet the competence requirements in A.4.2.

The review activities consist of an independent review of the verification report and shall be documented including at least the following:

- Date
- Reviewers
- Outcome of the review
- Review of the appointed verifiers (including the confirmation of competence and impartiality).

B.2.4.6. Decision and issue of the verification statement

Upon completion of the verification review the decision shall be made on whether or not to confirm the claim.

The decision shall be made by persons who have not been involved in the verification execution and who meet the competence requirements in B.4.2.

The decision shall be documented including at least the following:

- Date
- Decision makers
- result of the decision-making process including
 - Whether or not a verification statement can be issued.
 - Motivation of the decision taken.
 - The review of the appointed reviewers and verifiers (including the confirmation of competence and impartiality).

The issue of the verification statement is discussed in B.3.

B.2.4.7. Retention of verification documents

The verification statements, input, output, reporting, review and decision shall be retained for a minimum of 5 years by the Conformity Assessment Body.

B.3. Verification statement

A successful full (B.2.2) or limited verification (B.2.3) leads to a verification statement for which the following wording shall be used :

[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 be conform with the requirements of the CyberFundamentals assurance level “Important” 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 “Important” 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.be

The verification statement shall include:

- Name, address and company number of the Conformity Assessment Body;
- The relevant sector and subsector to which the organisation to which the verification applies belongs and referred to in B.4.2.1 and governing legislation, as applicable;
- The date and the unique identification of the statement;

- Conformity Assessment Body mark/logo/symbol;
- National Accreditation Body mark/logo/symbol and the accreditation certificate number, as prescribed by the NAB.

All logo's and marks shall be of the same or comparable size and they shall not be misleading or ambiguous.

B.4. Requirements for verifiers, reviewers and decision makers

B.4.1. Impartiality requirements

In addition to the normative requirements, the personnel involved in the review process (verifiers, reviewers and decision makers) shall not have been involved in consultancy for that organization for a period of 5 years.

Consultancy includes, but is not limited to, the following activities:

- In-house, specific or dedicated training on policies or security measures other than generic training (see below)
- Engineering of policies and security measures
- Technical assistance from conception through implementation of policies and/or security measures

Consultancy does not include:

- Use of shared information and resources (for example: the same vulnerability database,...)
- Generic training (from a public list of pre-established training) carried out for multiple organizations, without specific case studies of the organization involved.

Note: internal audit is not considered as consultancy, but it is not compatible with the activities of independent third-party assessments.

The internal auditor shall not be employed or hired by the Conformity Assessment Body to reduce the risk of familiarity and impartiality (internal auditor's relationship with verifiers).

Where a consultant is or was involved in the implementation of the security measures or the security program during the last two years, and that consultant is also employed by or has a contract with the Conformity Assessment Body, the Conformity Assessment Body may not accept the verification request.

No part of the verification shall be outsourced.

Records shall be retained by the conformity assessment body for a minimum of five years after the last assessment of the audit client.

B.4.2. Competence requirements

In addition to the normative requirements in ISO/IEC 17029, the following requirements are also applicable.

B.4.2.1. Competence requirements of verifiers and reviewers

The verifiers and reviewers of the CyberFundamentals Framework shall have demonstrated competence in:

- Technical knowledge relevant for the level CyberFundamentals Important (ICT/OT knowledge, NIST-CSF knowledge, CIS controls, ISO/IEC 27001, ISO/IEC 27002, IEC 62433 series)
- Auditing skills according to ISO 19011 and Chapter 7 of ISO/IEC 27007
- The business context of the verified company

The knowledge of the business requirements is determined according to the following clustering (in accordance with IAF ID1):

Cluster	IAF Code	Description of economic sector / activity
Production/ products	All other	
Transport	31	Transport, storage and communication
Supply	25	Electricity supply
	26	Gas supply
	27	Water supply
Services	34	Engineering services
	32	Financial intermediation, real estate, renting
	35	Other services
	36	Public administration
	37	Education
	38	Health and social services
	39	Other social services
Information technology	33	Information technology
Nuclear	11	Nuclear fuel
Aerospace	21	Aerospace

It is accepted that the qualification on the business context can be obtained through other schemes operating under accreditation.

Where a team of verifiers performs the verification, the lead verifier shall have full competence. Other verifiers in the team shall only verify security measures for which they are technically competent.

Verifiers shall be monitored on the CyberFundamentals Framework for at least 1 verification per year (onsite + documentary). When they are qualified for different business contexts, they shall be monitored for each cluster at least once every 5 years. For the monitoring related to the business context also other schemes can be used when the assessment is performed under accreditation.

Records shall be retained by the conformity assessment body for a minimum of five years after the last assessment of the audit client.

B.4.2.2. Competence requirements of decision makers

The decision makers shall have competence on

- The business context of cybersecurity
- The CyberFundamentals Framework (in general)

Where the decision making is done by a group, the competences shall be present as a group.

Records shall be retained by the conformity assessment body for a minimum of five years after the last assessment of the audit client

B.4.2.3. Security clearance

Where relevant, security clearance applies to the verifier, reviewer and decision-makers, as they shall have access to the full documentation of the verification program. Where a security clearance applies, all parties involved act in accordance with the clearance level and the requirements of the National Security Authority.

B.5. Collaboration between the scheme owner and the Conformity Assessment Body

The Centre for Cybersecurity Belgium is the scheme owner.

Conformity Assessment Bodies are required to have a legally binding agreement with the scheme owner. This agreement will enforce the use of the scheme without limitations or additions and will require collaboration with the scheme owner.

The Conformity Assessment Bodies are required to provide a yearly report to the scheme owner with the following data:

- List of verification statements + contact
- List of refused claims
- Complaints (received, treated)
- Revised verification statements

The Conformity Assessment Body is obliged to cooperate on any request from the CCB regarding the verification activities. If security clearance is required to access the information, the CCB will take the necessary steps to apply the required measures.

Annex C Assessment of the CyberFundamentals Framework Assurance Level “ESSENTIAL”

C.1. Type of certificate

The certificate in this context is the attestation of conformity of an organization’s management system including the cybersecurity policies and security measures at the assurance level CyberFundamentals “Essential” for a scope to be mentioned in the certificate.

To this end, the certification request shall include :

- The organizations name, address and company number. The organization is the scope of certification. The conformance with the requirements for the CyberFundamentals assurance level “Essential” can only be certified for the organization as a whole and no activities or processes can be excluded (see NOTE);
- The cluster and IAF code applicable to the organisation’s activities;
- The organisation’s statement that its operation meets the requirements of the CyberFundamentals assurance level “Essential”;
- The identification of maximum 5 CyberFundamentals measures that the organisation wants to exclude from the certification scope; Can not be excluded: Key measures as defined in clauses A, B and C in part IV of this CAS, nor controls linked to the management aspects as defined in clause D in part IV of this CAS;
- The version of the self-assessment that is part of the certification scope and date of completion of the self-assessment;
- The version of the applicable CyberFundamentals Framework;
- The version of the CyberFundamentals Conformity Assessment Scheme.

NOTE: In principle, the conformity assessment involves an organization as a whole, unless IT/OT environments are physically and/or technically separated. The separation shall be performed in such a way that the environments out of scope do not influence the risks of the environment in scope. In any case, this shall be clarified in the scope of the conformity assessment.

C.2. Certification program

C.2.1. Certification cycle and certification agreement

Certification is carried out by a Conformity Assessment Body (CAB).

The certification can be obtained for 3 years, with a yearly surveillance audit.

A legally enforceable certification agreement shall:

- Not exceed 3 years and can be discontinued considering a 3 months’ notice
- Include a statement that certifications are not eligible for transfer.
- Include confidentiality requirements including requirements on security clearance
- Foresee treatment of information using the TLP protocol.
- Include the statement that reports and other evidence may be requested by the Centre for Cybersecurity Belgium.

NOTE: Transfer in this context means as referred to in ISO/IEC 17021-1:2015 Clause 8.5.3 and subsequent clause 9.6.3.1.3 and not as referred to in IAF MD 2:2017.

C.2.2. Pre-certification activities

C.2.2.1. Application

The application review to be provided by the applicant to the Conformity Assessment Body (CAB) shall include:

- The Self-assessment report for assurance level “Essential” (output of the Self-Assessment tool further detailed in Part II-Annex D) that demonstrates a total maturity level higher than or equal to 3,5/5, a maturity level for each category higher than or equal to 3/5, and a maturity level for each key measure higher than or equal to 3/5;
- Appropriate evidence, including the completed ‘details’ tab from the Self-Assessment tool (see Part II-Annex D), to support the maturity self-assessment. The submitted evidence includes information or reference thereto regarding the self-assessment of key measures and controls linked to the management aspects of the Assurance Level “Essential” (see Part IV of this CAS);
- Motivation for each of the from the scope excluded CyberFundamentals measures (maximum 5);
- Objective evidence or reference to the verification regarding the use of symbols/logo’s/marks.

The CAB shall make sure that the scope is documented and agreed upon, based on the information provided in the certification request (Ref. C.1 above).

C.2.2.2. Planning

The initial and recertification audit program shall cover the complete CyberFundamentals set of requirements for assurance level “Essential”.

During the surveillance audits only the key measures and changes thereto are audited. Therefore, the auditor shall always review the previous report before planning an audit.

When an integrated certification audit is done with another by the applicant chosen technical standard, the time on-site of the integrated certification audit shall not be lower than the audit time as determined by the applicable technical standard or by this scheme whichever is the largest. This measure allows a complete audit for each scheme. The rounding rules apply as mentioned in IAF MD 5.

Temporary sites are to be considered in the audit program when they contain controls that cannot be verified at the main site.

The audit team shall be appointed in conformance with the requirements in section C.5 below, the rules specified in ISO/IEC 27006 and the normative requirements in ISO/IEC 17021-1.

C.2.3. Initial audits, surveillance audits and re-certification audits

C.2.3.1. Initial audits

The initial audit has two stages.

In addition to the objectives of a stage 1 audit identified in ISO/IEC 17021-1, the stage 1 audit shall include a documentary audit on the maturity self-assessment for assurance level “Essential” and

appropriate evidence to support this maturity self-assessment, that is submitted in the application (Ref. C.2.2.1).

The total maturity level of the, as a result of the stage 1 audit, eventually revised self-assessment shall not be below 2,5/5 to pass to a stage 2 assessment.

The stage 2 audit shall include at least the following onsite evaluation of the implementation, including effectiveness of:

- Measures taken in relation to the requirements of CyberFundamentals assurance level “Essential” that contribute to the respective Category Maturity levels;
- Measures taken in relation to the in the self-assessment documented Key Measure Maturity levels;
- Measures taken in relation to the controls linked to the management aspects of the Assurance Level “Essential” (see Part IV – Clause D of this CAS). Part IV – D. Controls linked to the management aspects of the Assurance Level “Essential”;
- The organisation’s management system ability and its performance regarding meeting of applicable statutory, regulatory and contractual requirements.

The minimum audit time for initial audits is 50% of the minimum audit time calculated according to the rules of ISO 27006, Annex B and C. This minimum audit time can only be applied if the maturity self-assessment for assurance level “Essential” is completed with appropriate evidence to support this maturity self-assessment and the information on the self-assessment of key measures is detailed enough to reach an audit conclusion. More detail on audit time can be found in Part II-Annex E.

C.2.3.2. Surveillance audits

The baseline of surveillance audits is an updated maturity self-assessment for assurance level “Essential” that is not older than 4 months. This updated maturity self-assessment for assurance level “Essential” has to be provided by the applicant to the Conformity Assessment Body (CAB) in due time before the start of the surveillance audit, including evidence on changed maturity of key measures and controls linked to the management aspects of the Assurance Level “Essential” (see Part IV of this CAS).

The timely delivery referred to above means that this has to enable the CAB to prepare the audit.

The minimal audit time will be 1 person-day taking into account the rules of ISO/IEC 27006, and shall include:

- The elements included in Part IV – Clause D Controls linked to the management aspects of the Assurance Level “Essential”.
- 1/3th of the key measures. These key measures will be selected giving priority to the controls that have not been audited in the previous surveillance audits.

The minimal audit time of 1 person-day shall be extended to audit:

- Key measures where a change has occurred or the score dropped below or is equal to 3/5
- Measures where scores result in category averages below 3/5
- Individual non-key measure scores that have a revised score below 2/5

More detail on audit time can be found in Part II-Annex E.

C.2.3.3. Re-certification audits

The baseline of recertification audit is an updated maturity self-assessment for assurance level “Essential” that is not older than 4 months. This updated maturity self-assessment for assurance level “Essential” has to be provided by the applicant to the Conformity Assessment Body (CAB) in due time before the start of the surveillance audit, including evidence on changed maturity of key measures and controls linked to the management aspects of the Assurance Level “Essential” (see Part IV of this CAS).

Providing information regarding the changed maturity of key measures and controls linked to the management aspects of the Assurance Level “Essential” only applies when the same CAB continues the certification. When another CAB takes over, the provisions of C.2.2.1 apply.

The timely delivery referred to above means that this has to enable the CAB to prepare the audit.

The recertification audit has two stages in situations where there have been significant changes to the organization, or the context in which the organization is operating (e.g. changes to legislation).

In addition to the objectives of a stage 1 audit identified in ISO/IEC 17021-1, the stage 1 audit shall include a documentary audit on the updated maturity self-assessment for assurance level “Essential” and appropriate evidence to support this maturity self-assessment.

When there is a stage 1 audit, the total maturity level of the, as a result of the stage 1 audit, eventually revised self-assessment shall not be below 2,5/5 to pass to a stage 2 assessment.

The stage 2 audit shall include at least the following onsite evaluation of the implementation, including effectiveness of:

- Measures taken in relation to the requirements of CyberFundamentals assurance level “Essential” that contribute to the respective Category Maturity levels in the light of internal and external changes and its continued relevance and applicability to the scope of certification;
- Measures taken in relation to the in the self-assessment documented Key Measure Maturity levels;
- Measures taken in relation to the controls linked to the management aspects of the Assurance Level “Essential” (see Part IV – Clause D of this CAS). Part IV – D. Controls linked to the management aspects of the Assurance Level “Essential”;
- The organisation’s management system ability and its performance regarding meeting of applicable statutory, regulatory and contractual requirements.

The minimum audit time for initial audits is 50% of the minimum audit time calculated according to the rules of ISO 27006, Annex B and C. This minimum audit time can only be applied if the maturity self-assessment for assurance level “Essential” is completed with appropriate evidence to support this maturity self-assessment and the information on the self-assessment of key measures is detailed enough to reach an audit conclusion.

The minimal audit time shall be extended to audit:

- Key measures where a change has occurred
- Measures where scores result in category averages below 3/5
- Individual non-key measure scores that have a revised score below 2/5

More detail on audit time can be found in Part II-Annex E.

C.2.3.4. Non-conformance handling

In addition to the general certification rules as explained in ISO/IEC 17021-1 the following rules shall apply:

Non-conformances are categorized as follows:

	Major non-conformance Maturity Level	Minor non-conformance Maturity Level
Each Key Measure	< 3/5	
Each Management Controls *	< 3/5	
Each Category	< 3/5	
Total Maturity Level	< 3.5/5	
All other controls		< 2/5

(*) controls linked to the management aspects defined in Part IV of the CAS

Major non-conformances are to be re-evaluated before proceeding to a certification decision. This re-evaluation can be based on a documentary, remote or onsite evaluation.

Minor non-conformances shall be subject of an action plan that shall be approved by the auditor and shall be integrated into the audit report. The approval shall also give an indication of the revised score when the action plan will be successfully implemented.

C.2.3.5. Special audits

Changes that occur in the organization that lead to a situation where key measures or controls linked to the management aspects defined in Part IV of this CAS, result in a revised self-assessment score lower than 3/5 or when a category average drops below 3/5, have to be flagged to the CAB. The CAB shall evaluate the situation and as appropriate decide to perform a special audit.

C.2.3.6. Audit conclusion

The maturity self-assessment score, which may be updated as a result of the findings during the audit, shall meet the values below to be eligible for certification:

Key Measures	13 (Basic) + 8 (Important) + 8 (Essential)*
	≥ 3/5 for each key measure
Category Maturity	≥ 3/5 for each category
Total Maturity level	≥ 3,5/5 (see self-assessment tool – summary tab Important)

(*) See Part IV of this CAS

For the measures excluded from the scope, the values are assigned as described in Part II – Annex D.3

The maturity self-assessment updated as a result of the findings during the audit shall not take into account the results of the action plans of the minor non-conformities (as they do not yet reflect the current situation of the certified organisation).

C.3. Certification decision making process

C.3.1. Certification output

The certification audits shall result in an audit report containing at least the following:

- Documented objective evidence or reference to that evidence that confirms or not the self-assessment result and other obligations of the conformity assessment scheme.
- Points of evaluation and evaluation results.
- Location, date, time and duration of the audit activities on site.
- Non-conformance reports and the evaluation of the actions or action plans.
- Evaluation and the result thereof of the motivation to exclude maximum 5 measures

When supplementary evaluation of major non-conformances is required, the result of this evaluation shall be documented including:

- Documented objective evidence or reference to that evidence regarding the evaluated major non-conformance.
- Location, date, time, nature of that evaluation
- The evaluation result.

C.3.2. Review

The review shall be carried out by persons who have not been involved in the certification audit and are conform with the requirements section C.5 below.

Each audit report shall be reviewed. Documentation of the independent review shall include at least the following:

- date
- result of review
- review of the appointed audit team (including the confirmation of competence and impartiality)

C.3.3. Decision

The decision shall be made by persons who have not been involved in the certification audit and who are conform with the requirements section C.5 below.

Each reviewed audit report shall be followed by a formal decision on attributing, maintaining, renewing or changing the certificate.

The decision shall be documented including at least the following:

- date
- decision makers
- result of the decision-making process including
 - the review of the appointed reviewer.
 - motivation of the decision taken.

C.4. Certification documents

C.4.1. Certification Statement

A successful (re)certification audit leads to a certification statement for which the following wording shall be used :

[NAME of conformity assessment body] declares to have successfully certified the management system, including policies and security measures, of [NAME, ADDRESS of organisation and COMPANY NUMBER] for the CyberFundamentals assurance level “Essential” on [date] for the following scope: [scope].

[NAME of conformity assessment body] confirms that the certification is 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 “Essential” 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].

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

The certification statement shall include:

- The date and the unique identification of the statement;
- Validity period of the certificate;
- The relevant sector and subsector to which the organisation covered by the certification belongs and referred to in C.5.2.1 and governing legislation, as applicable
- Name, address and company number of the Conformity Assessment Body;
- Conformity Assessment Body mark/logo/symbol;
- National Accreditation Body mark/logo/symbol and the accreditation certificate number, as prescribed by the NAB.

All logo’s and marks shall be of the same or comparable size and they shall not be misleading or ambiguous.

C.4.2. Retention of documentation

The certification audit documentation, input, output, reporting, review and decision shall be retained for a minimum of 2 certification cycles by the Conformity Assessment Body .

C.5. Requirements for auditors, reviewers, decision makers and the certification body

C.5.1. Impartiality requirements

In addition to the normative requirements, the personnel involved in the certification audit process (auditors, reviewers and decision makers) shall not have been involved in consultancy for that organization for a period of 5 years.

Consultancy includes, but is not limited to, the following activities:

- In-house, specific or dedicated training on policies or security measures other than generic training (see below)
- Engineering of policies and security measures
- Technical assistance from conception through implementation of policies and/or security measures

Consultancy does not include:

- Use of shared information and resources (for example: the same vulnerability database,...)
- Generic training (from a public list of pre-established training) carried out for multiple organizations, without specific case studies of the organization involved.

Note: internal audit is not considered as consultancy, but it is not compatible with the activities of independent third-party assessments.

The internal auditor shall not be employed or hired by the Conformity Assessment Body to reduce the risk of familiarity and impartiality (internal auditor's relationship with verifiers).

Where a consultant is or was involved in the implementation of the security measures or the security program during the last two years, and that consultant is also employed by or has a contract with the Conformity Assessment Body, the Conformity Assessment Body may not accept the certification request.

No part of the certification shall be outsourced.

Records shall be retained by the conformity assessment body for a minimum of five years after the last assessment of the audit client

C.5.2. Competence requirements

In addition to the normative requirements in ISO/IEC 17021-1, and the rules specified in ISO/IEC 27006, the following requirements are applicable:

C.5.2.1. Competence requirements of auditors and reviewers

The auditors and reviewers of the CyberFundamentals Framework shall have demonstrated competence in:

- Technical knowledge relevant for the level CyberFundamentals 'Essential' (ICT/OT knowledge, NIST-CSF knowledge, CIS controls, ISO/IEC 27001, ISO/IEC 27002, IEC 62433 series)
- Auditing skills according to ISO 19011 and Chapter 7 of ISO/IEC 27007
- The business context of the assessed company

The knowledge of the business requirements is determined according to the following clustering (in accordance with IAF ID1):

Cluster	IAF Code	Description of economic sector / activity
Production/ products	All other	
Transport	31	Transport, storage and communication
Supply	25	Electricity supply
	26	Gas supply
	27	Water supply
Services	34	Engineering services
	32	Financial intermediation, real estate, renting
	35	Other services
	36	Public administration
	37	Education
	38	Health and social services
	39	Other social services
Information technology	33	Information technology
Nuclear	11	Nuclear fuel
Aerospace	21	Aerospace

It is accepted that the qualification on the business context can be obtained through other schemes operating under accreditation.

Where an audit team performs the certification, the lead auditor shall have full competence. Other auditors in the team shall only audit security measures for which they are technically competent.

Auditors shall be monitored on the CyberFundamentals Framework for at least 1 audit per year (onsite + documentary). When they are qualified for different business contexts, they shall be monitored for each cluster at least once every 5 years. For the monitoring related to the business context also other schemes can be used when the assessment is performed under accreditation.

Records shall be retained by the conformity assessment body for a minimum of five years after the last assessment of the audit client.

C.5.2.2. Competence requirements of decision makers

The decision makers shall have competence on

- The business context of cybersecurity
- The CyberFundamentals Framework (in general)

Where the decision making is done by a group, the competences shall be present as a group.

Records shall be retained by the conformity assessment body for a minimum of five years after the last assessment of the audit client

C.5.2.3. Security clearance

Where relevant, security clearance applies to the auditor, reviewer and decision-makers, as they shall have access to the full documentation of the certification audit. Where a security clearance applies, all parties involved act in accordance with the clearance level and the requirements of the National Security Authority.

C.6. Collaboration between the scheme owner and the Certification Body

The Centre for Cybersecurity Belgium is the scheme owner.

Conformity Assessment Bodies are required to have a legally binding agreement with the scheme owner. This agreement will enforce the use of the scheme without limitations or additions and will require collaboration with the scheme owner.

The Conformity Assessment Bodies are required to provide a yearly report to the scheme owner with the following data:

- List of active certificates + name of entities + Company registration number (when available) + contact
- List of refused or revoked certifications
- List of certificates currently suspended
- Complaints (received, treated)

The Conformity Assessment Body is obliged to cooperate on any request from the CCB regarding the certification activities. If security clearance is required to access the information, the CCB will take the necessary steps to apply the required measures.

Annex D Self-Assessment tool

D.1. General

In support of the 'CyberFundamentals Framework' the Centre for Cybersecurity Belgium has developed a tool in MS[®] Excel.

The self-assessment tool takes into account the measures for assurance level "Basic", assurance level "Important" and assurance level "Essential" of a specific version of the framework as well as the requirements identified in the Conformity Assessment Scheme (CAS). The versions of the CyberFundamentals framework and CAS with which the tool is aligned, are identified in the tool. For this reason, the tool shall not be modified as part of any verification or certification activity.

Organisations submitting a self-assessment to a Conformity Assessment Body (CAB) according to the Conformity Assessment Scheme (CAS) shall use this tool.

The self-assessment tool is electronically available in the toolbox on the website: www.cyfun.be

D.2. Tool layout

The self-assessment tool in MS[®] Excel includes several tabs, each with its own function. Besides introduction, maturity levels and references, there are the tabs with the controls for assurance level "Basic", "Important" and "Essential" ('details' tab) and for each assurance level a summary ('summary' tab).

The controls are assessed through two angles:

Documentation Maturity: The Documentation Maturity evaluation measures how well your written rules and procedures satisfy the controls of the CyberFundamentals Framework.

Implementation Maturity: The Implementation Maturity evaluation assess how mature your actual operational practices are in relation to the CyberFundamentals Framework.

The table below shows the different maturity levels and the definitions used to assess maturity from both perspectives:

Maturity level	Documentation	Documentation Maturity score	Implementation	Implementation Maturity score
Initial (Level 1)	No Process documentation or not formally approved by management		Standard process does not exist .	
Repeatable (Level 2)	Formally approved Process documentation exists but not reviewed in the previous 2 years		Ad-hoc process exists and is done informally .	
Defined (Level 3)	Formally approved Process documentation exists, and exceptions are documented and approved . Documented & approved exceptions < 5% of the time		Formal process exists and is implemented. Evidence available for most activities. Less than 10% process exceptions.	
Managed (Level 4)	Formally approved Process documentation exists, and exceptions are documented and approved. Documented & approved exceptions < 3% of the time		Formal process exists and is implemented. Evidence available for all activities. Detailed metrics of the process are captured and reported. Minimal target for metrics has been established. Less than 5% of process exceptions.	
Optimizing (Level 5)	Formally approved Process documentation exists, and exceptions are documented and approved. Documented & approved exceptions < 0,5% of the time		Formal process exists and is implemented. Evidence available for all activities. Detailed metrics of the process are captured and reported. Minimal target for metrics has been established and continually improving . Less than 1% of process exceptions.	

D.3. Calculation method

A sub-category may consist of several controls and each of those controls shall be assessed for documentation and implementation according to the maturity table above. A value from 1 to 5 has to be entered per control in the ‘details’ tab of the applicable assurance level.

For the measures excluded from the scope, the following values are entered in the “details tab” of the respective measures:

	Documentation Maturity Level	Implementation Maturity Level
BASIC	2,5	2,5
IMPORTANT	3	3
ESSENTIAL	3	3

The tool calculates an arithmetic average for documentation and implementation per sub-category (e.g. ID.AM-1) to then calculate another arithmetic average for documentation and implementation per category (e.g. ID.AM).

These calculated values are visible in the ‘details’ tab of the applicable assurance level.

D.4. Self-Assessment Report

The ‘summary’ tab for the respective CyberFundamentals assurance levels is the report to be made available to the CAB and contains:

- 1) An overall maturity level (‘Total Maturity Level’) calculated as an arithmetic mean of the maturity levels of the categories.
- 2) A summary of the different maturity levels for each category using the respective values of the arithmetic averages of what was calculated in the ‘details’ tab.
- 3) A listing of the key measures to be met, the data for which is taken from the values entered in the ‘details’ tab.
- 4) A radar chart (spider chart) is also displayed based on the data from the summary of categories.

Determining conformity with the Conformity Assessment Scheme (CAS)

The overview includes the target scores as determined for the specific assurance levels as described in the CAS. It is against these target scores that the values of the self-assessment are assessed.

When the values colour red one is not conforming to the required maturity level, green shows conformance.

Annex E Assessment time chart

The following normative references apply to determine the assessment time:

- ISO/IEC 17021-1: 2012 Clause 9.1.4 Determining audit time
- ISO/IEC 27006:2015 Annex B Audit time

The table below shows the minimum assessment time and the situations where additional assessment time shall be scheduled, indicated by a '+' sign. The amount of additional assessment time is determined based on the lead auditor's professional judgement. This shall take into account the normative references above.

	BASIC		IMPORTANT		ESSENTIAL	
	Verification	Limited Verification	Verification	Limited Verification	Initial or Recert	Follow-up
Min Assessment time*	1.5	0.5	1.5	0.5	50% of the time calculation using ISO/IEC 27006	1 day
Min assessment time on site (as part of the total min assessment time)	1		1			
Adjustment of audit time						
Changes in more than 2 key measures		+ (time to be planned in verification plan)		+ (time to be planned in verification plan)		+ (time to be planned in audit plan)
Changes in non-key measures resulting in maturity score change > 1		+ (time to be planned in verification plan)		+ (time to be planned in verification plan)		+ (time to be planned in audit plan)
Significant Doubt about evidence provided by the organization	+ (time to be planned in verification plan)	+ (time to be planned in verification plan)	+ (time to be planned in verification plan)	+ (time to be planned in verification plan)		+ (time to be planned in audit plan)
Evidence lacking regarding use of symbols/logo's/marks	+ 2hrs (on or off site)					
Changes relevant to the ISMS					+ (time following ISO/IEC 27006)	+ (time following ISO/IEC 27006)
Follow-up of NC's of previous assessments					Min. 1 hr / major NC	+ Min. 1 hr / major NC
					Min. 0.5 hr / minor NC	+ Min. 0.5 hr / minor NC
					(time planned in audit plan)	(time planned in audit plan)

(*) This minimum assessment time can only be applied if the maturity self-assessment for the appropriate assurance level is completed and accompanied by appropriate objective evidence to support this maturity self-assessment, including evidence or accessible reference to evidence for key measures and significantly changed non-key measures.

The assessment time is time needed to plan and accomplish a complete and effective assessment of the client's claim (verification) or client organization's management system (certification).

This includes:

- Preparing the assessment off-site;
- Performing the document review on site and off site;
- Collecting and verifying information;
- Performing the assessment (verification or certification);
- Conducting the opening and closing meeting;
- Communicating during the assessment;
- Generating assessment findings;
- Preparing assessment conclusions (including assessment report).

Annex F Requirements for the National Accreditation Body (NAB)

F.1. Accreditation scope

The NAB will require the conformity assessment body to be accredited, to identify in its accreditation application the technical cluster, as defined in Part II – A.4.2.1, B.4.2.1 and C.5.2.1, in which it wishes to operate:

Cluster	IAF Code	Description of economic sector / activity
Production/ products	All other	
Transport	31	Transport, storage and communication
Supply	25	Electricity supply
	26	Gas supply
	27	Water supply
Services	34	Engineering services
	32	Financial intermediation, real estate, renting
	35	Other services
	36	Public administration
	37	Education
	38	Health and social services
	39	Other social services
Information technology	33	Information technology
Nuclear	11	Nuclear fuel
Aerospace	21	Aerospace

Also, the conformity assessment body to be accredited shall indicate whether it has assessors active in that cluster.

F.2. Assessment programme for assessing the conformity assessment body activities during the accreditation cycle

The program for assessing the conformity assessment body activities during the accreditation cycle shall include on-site witnessing as follows:

- For initial accreditation audits, a field follow-up will be done per cluster of which
 - At least 1 witnessing covering a full verification as meant in Part II – A.2.2 and B.2.2
 - At least 1 witnessing covering phases 1 and 2 of the certification audit.
- For further cycles, witnessing per cluster during the full accreditation cycle covering at least 3 years is sufficient. For shorter accreditation cycles, a case-by-case definition of the assessment program can be determined by the NAB.

F.3. Competencies of NAB staff

- Technical Assessors: qualification for the relevant accreditation standard, supplemented by technical knowledge such as that for auditors (Part II – A.4.2.1, B.4.2.1 and C.5.2.1) and accreditation-oriented training provided by the scheme owner.
- Lead Assessors: qualification for the relevant accreditation standard, supplemented by accreditation-oriented training provided by the scheme owner.
- NAB staff other than (lead) assessors: accreditation-focused training provided by the scheme owner.

Annex G (informative) Mapping towards ISO/IEC 17029 and ISO/IEC 17021-1

G.1. Mapping from the Conformity Assessment Scheme towards ISO/IEC 17029:2019 and ISO/IEC 17021-1:2015

	ISO/IEC 17029:2019 Clauses	ISO/IEC 17021-1:2015 Clauses
Introduction		
1. General remarks	Introduction, 1, 11	Introduction, 1, 10
2. Normative references	2	2
3. Definitions and acronyms	3	3
4. Disclaimer		
PART I CyberFundamentals Framework Requirements		
1. Assurance levels	Introduction, 1, 11	Introduction, 1, 10
2. Key measures	Introduction, 1, 11	Introduction, 1, 10
3. Location and applicable version		
Part II Assessment of the CyberFundamentals Framework		
1. General remarks	Introduction, 1, 11	Introduction, 1, 10
2. CyberFundamentals assessment overview	Introduction, 1	Introduction, 1
Annex A Assessment of the CyberFundamentals Framework Assurance Level "BASIC"		
A.1 Type of claim	3.1, 3.3	
A.2 Verification program	6.2, 8, 9, 9.8, 9.9, 9.10	
A.2.1. Input for verification	9.2	
A.2.2. Full verification program	6.2, 8, 9	
A.2.3. Limited verification program	6.2, 8, 9	
A.2.4. Verification process	4.2.2, 4.3.7, 9	
A.2.4.1. Pre-engagement	9.2	
A.2.4.2. Engagement	5.4, 6.1, 9.3, 9.11, 10.4	
A.2.4.3. Planning	7, 9.4	
A.2.4.4. Verification Execution	4.2.3, 9.5	
A.2.4.5. Review	9.6	
A.2.4.6. Decision and issue of the verification statement	9.7	
A.2.4.7. Retention of verification documents	9.11, 11.6.2	
A.3 Verification statement	5.2, 9.7.2, 10	
A.4 Requirements for verifiers, reviewers, and decision makers	4.3, 5.3, 6.1, 7, 9.6, 9.7.1, 9.11	
A.5 Collaboration between the scheme owner and the Conformity Assessment Body	6.1	
Annex B Assessment of the CyberFundamentals Framework Assurance Level "IMPORTANT"		
B.1 Type of claim	3.1, 3.3	
B.2 Verification program	6.2, 8, 9, 9.8, 9.9, 9.10	

	ISO/IEC 17029:2019 Clauses	ISO/IEC 17021-1:2015 Clauses
B.2.1. Input for verification	9.2	
B.2.2. Full verification program	6.2, 8, 9	
B.2.3. Limited verification program	6.2, 8, 9	
B.2.4. Verification process	4.2.2, 4.3.7, 9	
B.2.4.1. Pre-engagement	9.2	
B.2.4.2. Engagement	5.4, 6.1, 9.3, 9.11, 10.4	
B.2.4.3. Planning	7, 9.4	
B.2.4.4. Verification Execution	4.2.3, 9.5	
B.2.4.5. Review	9.6	
B.2.4.6. Decision and issue of the verification statement	9.7	
B.2.4.7. Retention of verification documents	9.11, 11.6.2	
B.3 Verification statement	5.2, 9.7.2, 10	
B.4 Requirements for verifiers, reviewers, and decision makers	4.3, 5.3, 6.1, 7, 9.6, 9.7.1, 9.11	
B.5 Collaboration between the scheme owner and the Conformity Assessment Body	6.1	
Annex C Assessment of the CyberFundamentals Framework Assurance Level "ESSENTIAL"		
C.1 Type of certificate		8.2, 8.3, 9.6.3
C.2 Certification program		9
C.2.1. Certification cycle and certification agreement		5.1.2, 9.1.3, 9.2.3
C.2.2. Pre-certification activities		9.1
C.2.2.1. Application		9.1.1, 9.1.2
C.2.2.2. Planning		9.1.3, 9.1.4
C.2.3. Initial audits, surveillance audits and re-certification audits		9.2, 9.3, 9.6
C.2.3.1. Initial audits		9.3
C.2.3.2. Surveillance audits		9.6.2
C.2.3.3. Re-certification audits		9.6.3
C.2.3.4. Non-conformance handling		9.4.9, 9.4.10
C.2.3.5. Special audits		9.6.4
C.2.3.6. Audit conclusion		9.6.5
C.3 Certification decision making process		9.5
C.3.1. Certification Output		9.5
C.3.2. Review		9.5
C.3.3. Decision		9.5
C.4 Certification documents		8
C.4.1. Certification statement		8.3
C.4.2. Retention of documentation		9.9, 10
C.5 Requirements for auditors, reviewers, and decision makers and the certification body		4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 5, 7, Annex A
C.5.1. Impartiality requirements		4.2, 5.2

	ISO/IEC 17029:2019 Clauses	ISO/IEC 17021-1:2015 Clauses
C.5.2. Competence requirements		4.3, 7.1, 7.2, 7.5, 9.1.2, 9.2.2, 9.4, Annex A
C.6 Collaboration between the scheme owner and the Certification Body		10
Annex D Self-assessment tool		
	8, 9	8, 9
Annex E Assessment time chart		
	9.2, 9.4	9.1.4
Annex F Requirements for the National Accreditation Body (NAB)		
Part IV Key Measures of the CyberFundamentals Framework		
A. Key measures for Assurance Levels “Basic”, “Important” and “Essential”	9.2, 9.3, 9.4, 9.5, 9.6, 9.7	9.1, 9.2, 9.3, 9.4, 9.5, 9.6
B. Additional Key measures for Assurance Levels “Important” and “Essential”	9.2, 9.3, 9.4, 9.5, 9.6, 9.7	9.1, 9.2, 9.3, 9.4, 9.5, 9.6
C. Additional Key measures for the Assurance Level “Essential”		9.1, 9.2, 9.3, 9.4, 9.5, 9.6
D. Controls linked to the management aspects of the Assurance Level “Essential”		9.3, 9.4, 9.6

G.2. Mapping from ISO/IEC 17029:2019 towards the Conformity Assessment Scheme

ISO/IEC 17029:2019 Clauses	CyFun CAS Reference
3. Terms and definitions	Introduction – 3, Part II – A.1 & B.1
4. Principles	
4.1 General	Part II – 1
4.2 Principles for the validation/verification process	Part II – A.2.4 & B.2.4
4.3 Principles for validation/verification bodies	Part II – A.2.4 , A.4 & B.2.4, B.4
5. General requirements	
5.1 Legal entity	Part II – C.1, C.4.1
5.2 Responsibility for validation/verification statements	Part II – A.3 & B.3
5.3 Management of impartiality	Part II – A.4 & B.4
5.4 Liability	Part II – A.2.4.2 & B.2.4.2
6. Structural requirements	
6.1 Organizational structure and top management	Part II – A.2.4.2, A.4, A.5 & B.2.4.2, B.4, A.5
6.2 Operational control	Part II – A.2 & B.2
7. Resource requirements	Part II – A.2.4.3 & B.2.4.3
7.1 General	
7.2 Personnel	Part II – A.4 & B.4 & F.1
7.3 Management process for the competence of personnel	Part II – A.4.2 & B.4.2
7.4 Outsourcing	Part II – A.4 & B.4
8. Validation/verification program	Part II – A.2, D & B.2, D

ISO/IEC 17029:2019 Clauses	CyFun CAS Reference
9. Process requirements	Part II – A.2, D & B.2, D
9.1 General	Part II – A.2.4 & B.2.4
9.2 Pre-engagement	Part II – A.2.1, A.2.4.1. & B.2.1, B.2.4.1.& E & Part IV.A, B
9.3 Engagement	Part II – A.2.4.2 & B.2.4.2 & Part IV.A, B
9.4 Planning	Part II – A.2.4.3 & B.2.4.3 & E & Part IV.A, B
9.5 Validation/verification execution	Part II – A.2.4.4 & B.2.4.4 & Part IV.A, B
9.6 Review	Part II – A.2.4.5, A.4 & B.2.4.5, B.4 & Part IV.A, B
9.7 Decision and issue of the validation/verification statement	Part II – A.2.4.6, A.3, A.4 & B.2.4.6, B.3, B.4 & Part IV.A, B
9.8 Facts discovered after the issue of the validation/verification statement	Part II – A.2 & B.2
9.9 Handling of appeals	Part II – A.2 & B.2
9.10 Handling of complaints	Part II – A.2 & B.2
9.11 Records	Part II – A.2.4.2, A.2.4.7, A.4 & B.2.4.2, B.2.4.7, B.4
10 Information requirements	
10.1 Publicly available information	Covered through ISO/IEC 17029 accreditation of the CAB.
10.2 Other information to be available	Part II – A.5 & B.5
10.3 Reference to validation/verification and use of marks	Part II – A.3 & B.3
10.4 Confidentiality	Part II – A.2.4.2 & B.2.4.2
11 Management system requirements	
11.1 General	
11.2 Management review	
11.3 Internal audits	Covered through ISO/IEC 17029 accreditation of the CAB.
11.4 Corrective action	
11.5 Actions to address risks and opportunities	
11.6 Documented information	Part II – A.2.4.7 & B.2.4.7

G.3. Mapping from ISO/IEC 17021-1:2015 towards the Conformity Assessment Scheme

ISO/IEC 17021-1:2015	CyFun CAS Reference
3. Terms and definitions	Introduction – 3
4. Principles	
4.1 General	Covered through ISO/IEC 17021-1 accreditation of the CAB.
4.2 Impartiality	Part II – C.5
4.3 Competence	Part II – C.5
4.4 Responsibility	Part II – C.5
4.5 Openness	Part II – C.5
4.6 Confidentiality	Part II – C.5
4.7 Responsiveness to complaints	Part II – C.5

4.8 Risk-based approach	Covered through ISO/IEC 17021-1 accreditation of the CAB.
5. General requirements	Part II – C.5
5.1 Legal and contractual matters	Part II – C.2.1
5.2 Management of impartiality	Part II – C.5.1
5.3 Liability and financing	Covered through ISO/IEC 17021-1 accreditation of the CAB.
6. Structural requirements	
6.1 Organizational structure and top management	Covered through ISO/IEC 17021-1 accreditation of the CAB.
6.2 Operational control	Covered through ISO/IEC 17021-1 accreditation of the CAB.
7. Resource requirements	Part II – C.5
7.1 Competence of personnel	Part II – C.5.2
7.2 Personnel involved in the certification activities	Part II – C.5.2
7.3 Use of individual external auditors and external technical experts	Part II – C.5.2
7.4 Personnel records	Part II – C.5.2
7.5 Outsourcing	Part II – C.5.2
8. Information requirements	Part II – C.4 & D
8.1 Public information	Covered through ISO/IEC 17021-1 accreditation of the CAB.
8.2 Certification documents	Part II – C.1
8.3 Reference to certification and use of marks	Part II – C.1, C.4.1
8.4 Confidentiality	Part II – A.4.2 & B.4.2
8.5 Information exchange between a certification body and its clients	Part II – A.2.1 & B.2.1
9 Process requirements	Part II – C.2 & D
9.1 Pre-certification activities	Part II – C.2.1, C.2.2, C.5.2 & E & Part IV.B, C
9.2 Planning audits	Part II – C.2.1, C.2.3 & Part IV.A, B, C
9.3 Initial certification	Part II – C.2.3 & Part IV.A, B, C, D
9.4 Conducting audits	Part II – C.2.3, C.5.2 & Part IV.A, B, C, D
9.5 Certification decision	Part II – C.3 & Part IV.A, B, C
9.6 Maintaining certification	Part II – C.1, C.2.3, C.2.3.5, C.2.3.6 & Part IV.A, B, C, D
9.7 Appeals	Covered through ISO/IEC 17021-1 accreditation of the CAB.
9.8 Complaints	
9.9 Client records	Part II – C.4.2
10 Management system requirements for certification bodies	Covered through ISO/IEC 17021-1 accreditation of the CAB.
10.1 Options	
10.2 Option A: General management system requirements	
10.3 Option B: Management system requirements in accordance with ISO/IEC 9001	
Annex A (normative) Required knowledge and skills	Part II – C.5

PART III Assurance Level Labelling

1. General remarks

For verification and certification activities Part II of this CAS is applicable.

Labels are granted by the CCB Certification Authority based on a self-assessment assessed by a Conformity Assessment Body (CAB).

The self-assessment to be submitted can be found in the self-assessment tool uploaded in the toolbox on the CyFun website (www.cyfun.be).







An ISO/IEC 27001 certificate with the suitable scope and statement of applicability (SoA) is presumed to conform to the measures of the framework. For further detail see Part III -Annex D

For every assurance level of the CyberFundamentals Framework (Basic, Important, Essential) an organization can do a self-declaration based on a completed self-assessment for the respective assurance level considering the required maturity levels including key measures as specified in the table above.

The assessment can be performed by an internal auditor. It is also possible that the self-assessment is carried out in the context of regional initiatives to improve cybersecurity (Flanders: VLAIO - Wallonia KIS - ADP).

A self-declaration by itself without verification (AL Basic & AL Important) or certification (AL Essential) by an independent third-party Conformity Assessment Body (CAB) does not entitle an organization to obtain a label.

2. CyberFundamentals labelling overview

	BASIC	IMPORTANT	ESSENTIAL
Type of assessment	Verification	Verification	Certification
Assessment method	Verification of self-assessment	Verification of self-assessment	Certification audit
Assessment performed by	Accredited CAB	Accredited CAB	Accredited CAB
Assurance evidence	Verified Claim	Verified Claim	Certificate
Label	 	 	 

Annex A CyberFundamentals Framework Assurance Level “BASIC” label

A.1. CyberFundamentals “Basic” Assessment

An entity can opt for a verification assessment in order to obtain a label with associated QR code CyberFundamentals ‘Basic’. The modalities are stipulated in Part II – Annex A.

A.2. Rules to obtain and use of the label CyberFundamentals “Basic”

A completed self-assessment for assurance level “Basic” (see Part II - Annex D) and a verification statement (see Part II – Annex A.3) by an independent third-party Conformity Assessment Body (CAB) entitles an organization to obtain a label with associated QR code.

The organisation shall be a Belgian legal entity (this includes public entities), which will be controlled in the application process by a limited automated verification of their legal status (name of the organisation, company registration number and legal situation).

Eligibility to obtain a label is determined by achieving the following, and assessed by a CAB:

Key Measures	13*
	≥ 2,5/5 for each key measure
Total Maturity level	≥ 2,5/5 (see self-assessment tool – summary tab)

(*) See Part IV of this CAS

The assessed self-assessment and a verification statement issued by the same CAB is provided by the organisation to the CCB via the SafeOnWeb@Work portal, where it is reviewed that the requirements for each key measure have been met and that the overall maturity level has been achieved. The CCB Certification Authority can request additional information.

When the organization is eligible for the use of the label with associated QR code, the CCB will provide a label and QR code CyberFundamentals ‘Basic’ containing:

- The name of the organization
- The organization’s registration number
- The scope
- The overall maturity level and respective values for policy and implementation maturity as declared
- The notion that the label is substantiated by a self-assessment evaluated during a verification assessment, and the corresponding label may be used for a maximum period of 12 months + 1 month overlap time from the date of the self-assessment.

The label and QR code are sent to the e-Box of the organization. The organization obliges itself to use this label and QR code in an unchanged way and in accordance with the Rules on the use of CyberFundamentals labels (see Part III - Annex E).

A.3. Facts discovered after the issue of the label

If new facts or information that could materially affect the use of the label CyberFundamentals 'Basic' are discovered after the issue date, the CCB Certification Authority shall:

- take into account that a verification statement is a statement that represents only the situation at the moment of verification.
- communicate the matter as soon as practicable to the client and the Conformity Assessment Body who issued the verification statement that was used to obtain the label;
- take appropriate action, including the following:
 - Discuss the matter with the client and the Conformity Assessment Body who issued the verification statement that was used to obtain the label;
 - Consider if the label has to be withdrawn. If it is decided to withdraw the label, it shall not be used for any purpose and shall be removed where appropriate.

Annex B CyberFundamentals Framework Assurance Level “IMPORTANT” label

B.1. CyberFundamentals ‘Important’ Assessment

An entity can opt for a verification assessment in order to obtain a label with associated QR code CyberFundamentals ‘Important’. The modalities are stipulated in Part II – Annex B.

B.2. Rules to obtain and use of the label CyberFundamentals “Important”

A completed self-assessment for assurance level “Important” (see Part II - Annex D) and a verification statement (see Part II – Annex B.3) by an independent third-party Conformity Assessment Body (CAB) entitles an organization to obtain a label with associated QR code.

The organisation shall be a Belgian legal entity (this includes public entities), which will be controlled in the application process by a limited automated verification of their legal status (name of the organisation, company registration number and legal situation).

Eligibility to obtain a label is determined by achieving the following, and assessed by a CAB:

Key Measures	13 (Basic) + 8 (Important)*
	≥ 3/5 for each key measure
Total Maturity level	≥ 3/5 (see self-assessment tool – summary tab Important)

(*) See Part IV of this CAS

The assessed self-assessment and a verification statement issued by the same CAB is provided by the organisation to the CCB via the SafeOnWeb@Work portal, where it is reviewed that the requirements for each key measure have been met and that the overall maturity level has been achieved. The CCB Certification Authority can request additional information.

When the organization is eligible for the use of the label with associated QR code, the CCB will provide a label and QR code CyberFundamentals ‘Important’ containing:

- The name of the organization
- The organization’s registration number
- The scope
- The overall maturity level and respective values for policy and implementation maturity as declared
- The notion that the label is substantiated by a self-assessment evaluated during a verification assessment, and the corresponding label may be used for a maximum period of 12 months + 1 month overlap time from the date of the self-assessment.

The label and QR code are sent to the e-Box of the organization. The organization obliges itself to use this label and QR code in an unchanged way and in accordance with the Rules on the use of CyberFundamentals labels (Part III - Annex E).

B.3. Facts discovered after the issue of the label

If new facts or information that could materially affect the use of the label CyberFundamentals 'Important' are discovered after the issue date, the CCB Certification Authority shall:

- take into account that a verification statement is a statement that represents only the situation at the moment of verification.
- communicate the matter as soon as practicable to the client and the Conformity Assessment Body who issued the verification statement that was used to obtain the label;
- take appropriate action, including the following:
 - Discuss the matter with the client and the Conformity Assessment Body who issued the verification statement that was used to obtain the label;
 - Consider if the label has to be withdrawn. If it is decided to withdraw the label, it shall not be used for any purpose and shall be removed where appropriate.

Annex C CyberFundamentals Framework Assurance Level “ESSENTIAL” label

C.1. CyberFundamentals ‘Essential’ Assessment

An entity can opt for a certification in order to obtain a label with associated QR code CyberFundamentals ‘Essential’. The modalities are stipulated in Part II – Annex C.

C.2. Rules to obtain and use of the label CyberFundamentals “Essential”

A completed self-assessment for assurance level “Essential” (see Part II - Annex D) and a certificate (see Part II – Annex C.4.1) by an independent third-party Conformity Assessment Body (CAB) entitles an organization to obtain a label with associated QR code.

The organisation shall be a Belgian legal entity (this includes public entities), which will be controlled in the application process by a limited automated verification of their legal status (name of the organisation, company registration number and legal situation).

Eligibility to obtain a label is determined by achieving the following, and assessed by a CAB:

Key Measures	13 (Basic) + 8 (Important) + 8 (Essential)* ≥ 3/5 for each key measure
Category Maturity	≥ 3/5 for each category
Total Maturity level	≥ 3,5/5 (see self-assessment tool – summary tab Important)

(*) See Part IV of this CAS

The assessed self-assessment and certificate issued by the same CAB is provided by the organisation to the CCB via the SafeOnWeb@Work portal, where it is reviewed that the requirements for each key measure have been met and that the overall maturity level has been achieved. Evidence of successful implementation of key measures must be provided together with the self-assessment. The evidence to be provided for each key measure consists of an explanation (1-pager) with demonstrable evidence of how the measure has been rolled out. The CCB Certification Authority can request additional information.

When the organization is eligible for the use of the label with associated QR code, the CCB will provide a label and QR code CyberFundamentals ‘Essential’ containing:

- The name of the organization
- The organization’s registration number
- The scope
- The overall maturity level and respective values for policy and implementation maturity as declared
- The notion that the label is substantiated by a self-assessment evaluated during a certification audit (initial, surveillance or recertification), and the corresponding label may be used for a maximum period of 12 months + 1 month overlap time from the date of the self-assessment.

The label and QR code are sent to the e-Box of the organization. The organization obliges itself to use this label and QR code in an unchanged way and in accordance with the Rules on the use of CyberFundamentals labels (Part III - Annex D).

C.3. Facts discovered after the issue of the label

If new facts or information that could materially affect the use of the label CyberFundamentals 'Essential' are discovered after the issue date, the CCB Certification Authority shall:

- communicate the matter as soon as practicable to the client and the Conformity Assessment Body who issued the certification statement that was used to obtain the label;
- take appropriate action, including the following:
 - Discuss the matter with the client and the Conformity Assessment Body who issued the certification statement that was used to obtain the label;
 - Consider if the label has to be withdrawn. If it is decided to withdraw the label, it shall not be used for any purpose and shall be removed where appropriate.

Annex D Eligibility for labelling through ISO/IEC 27001 certification

When an ISO/IEC 27001 certification is chosen to obtain a CyberFundamentals label (Basic, Important or Essential), the following procedure applies to obtain that label:

- The CyberFundamentals label shall be requested by the applicant (private or public entity), through the SafeOnWeb@Work portal by uploading the ISO/IEC 27001 certificate issued by a CAB, and the Statement of Applicability.
- The applicant must clearly indicate the level of assurance (Basic, Important or Essential) for which the applicant wishes to obtain a label using an ISO/IEC 27001 certification.
- CCB will verify the eligibility the same way as described in the respective rules to obtain and use of a CyberFundamentals label (Part III – Annex A, B & C). In practice, this means that the Statement Of Applicability that is part of the ISO/IEC 27001 certification must include the requirements of the respective CyberFundamentals assurance level.

The label with associated QR code will be sent to the e-Box of the evaluated organization.

Organizations oblige themselves to use this label with associated QR code in an unchanged way and in accordance with the “Rules on the use of CyberFundamentals labels” as detailed in Part III – Annex E.

Demonstrating conformance with the requirements of the CyberFundamentals Framework based on an ISO/IEC 27001 certification is only possible for obtaining a CyberFundamentals label. A CyberFundamentals label cannot be used to obtain an ISO/IEC 27001 certification. Conformance to the requirements of the CyberFundamentals framework may although support ISO/IEC 27001 certification.

Annex E Rules on the use of CyberFundamentals labels

The requirements are based on the guidelines of ISO/IEC 17030 and describe the Use policy of the Centre for Cybersecurity Belgium (CCB) assurance level labels CyberFundamentals “Basic”, CyberFundamentals “Important” and CyberFundamentals “Essential”. In the following, label also includes the associated QR code.

General Rules regarding the use of a CyberFundamentals label

The CyberFundamentals label is considered a third-party mark of conformity owned and protected by the Centre for Cybersecurity Belgium (CCB). The following rules shall apply:

- By applying for the CyberFundamentals label, the entity is legally bound to the rules as stipulated in the use of CyberFundamentals labels.
- In addition, the rules on the use of CyberFundamentals labels shall be referred to in the legally enforceable agreement between the requester and the Conformity Assessment Body for the labels Basic, Important and Essential.
- The label will contain or be accompanied by a link to the conformity assessment statement (verification or certification).
- The user shall not register, try to register nor claim ownership of the label during or after the period of use of the label.
- Since the label is not related to product conformity assessment, the label shall not be displayed on the product or product packaging. Nor shall the label be used on test reports, and calibration certificates.
- The label can be used on digital media (e.g. website).
- A reference to the label may also be used on other media such as letters, business cards, promotional material for the period as stipulated in the scheme and within the scope of the label.
- The label shall not be used in a way that leads to misinterpretation or abuse of the label. This includes unauthorized use, wrong use or misleading use of the label (e.g. suggest that a customer service of an entity is certified).
- Possible sanctions on the abuse of a label include the sanctions related to abuse of the reference to verification, certification and accreditation as stipulated in the applicable legislation. (Code of Economic Law)
- The label is intended to indicate a level of performance verified by the method related to the specific label. It shall not transfer liability on compliance requirements from the requester of the label to the owner of the label or the Conformity Assessment Body (CAB).

Reasonable doubt about the legitimacy of a used CyberFundamentals label

- When during the period of use of the label, there is reasonable doubt about the legitimacy of the fixed label, the scheme owner has the right to recall the permission to use the label. The user of the label shall stop all use of the label within 5 working days of the recall.
- Possible sanctions on the abuse of a CyberFundamentals label are imposed by the scheme owner and may include a formal warning, an obligation to inform impacted parties on the abuse of the label, a decision to recall the use of the label and/or a decision to cancel the eligibility to use the label for a period up to 3 years. The sanction shall be made public by the CCB.

Merger of an organization

In case of a merger of an organization the right to use the label is not automatically transferred to a new entity. For the CyberFundamentals Essential, the Conformity Assessment Body shall be notified to evaluate the validity of the current certification.

Complaints regarding the use of the CyberFundamentals label

Complaints regarding the use of the label for the labels granted after verification and certification are dealt with in cooperation with the conformity assessment bodies and/or the CCB Certification Authority.

Information provision regarding the CyberFundamentals label

The user of the label is obliged to provide upon request information that explains the meaning of the label. In order to contribute to the information for interested parties, the CCB CyberFundamentals Framework is published on the website of the Centre for Cybersecurity Belgium (CCB).

Specific information about the maturity assessment shall not be made available to requesters unless required by law or court.

For all files, the information related to the maturity assessment is considered to fall under the exception Art. 6 §1 of the government information act (11 April 1994), namely the confidential character of the organization's data delivered to the government.

Possible changes regarding the use of CyberFundamentals labels

The Centre for Cybersecurity Belgium (CCB) reserves the right to change the rules related to the use of labels and will inform users of these changes.

The change of rules will be subject to the provision of scheme management that will include stakeholder consultation.

PART IV Key Measures of the CyberFundamentals Framework

The key measures are defined based on market surveillance information, the national cybersecurity strategy and successful attack methods that the operational services of the CCB have detected. Key measures will be updated regularly to ensure the framework remains relevant, focusing on those controls that contribute most to the cybersecurity of the framework's users.

A. Key measures for Assurance Levels “Basic”, “Important” and “Essential”

The following controls are key measures mutual for all assurance levels:

	Sub-category	Requirement
1.	PR.AC-1	Identities and credentials for authorized devices and users shall be managed.
2.	PR.AC-3	The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).
3.	PR.AC-4	Access permissions for users to the organization's systems shall be defined and managed.
4.	PR.AC-4	It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.
5.	PR.AC-4	Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (the principle of Least Privilege).
6.	PR.AC-4	Nobody shall have administrator privileges for daily tasks.
7.	PR.AC-5	Firewalls shall be installed and activated on all the organization's networks.
8.	PR.AC-5	Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.
9.	PR.IP-4	Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.
10.	PR.MA-1	Patches and security updates for Operating Systems and critical system components shall be installed.
11.	PR.PT-1	Logs shall be maintained, documented, and reviewed.
12.	DE.AE-3	The activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.
13.	DE.CM-4	Anti-virus, -spyware, and other -malware programs shall be installed and updated.

B. Additional Key measures for Assurance Levels “Important” and “Essential”

In addition to the key measures defined for the three assurance levels, the following key measures are added for the assurance levels “Important” and “Essential”:

Sub-category		Requirement
1.	ID.AM-6	Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.
2.	PR.AC-3	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization’s critical systems environment shall be identified, documented and implemented.
3.	PR.AC-5	Where appropriate, network integrity of the organization's critical systems shall be protected by (1) Identifying, documenting, and controlling connections between system components. (2) Limiting external connections to the organization's critical systems.
4.	PR.AC-5	The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.
5.	PR.DS-5	The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.
6.	PR.IP-1	The organization shall develop, document, and maintain a baseline configuration for the its business critical systems.
7.	DE.CM-1	The organization shall monitor and identify unauthorized use of its business critical systems through the detection of unauthorized local connections, network connections and remote connections.
8.	RS.AN-5	The organization shall implement vulnerability management processes and procedures that include processing, analysing and remedying vulnerabilities from internal and external sources.

C. Additional Key measures for the Assurance Level “Essential”

In addition to the key measures defined under sections A and B above, the following key measures are added for the assurance level “Essential”:

Sub-category		Requirement
1.	ID.SC-3	Contractual ‘information security and cybersecurity’ requirements for suppliers and third-party partners shall be implemented to ensure a verifiable flaw remediation process, and to ensure the correction of flaws identified during ‘information security and cybersecurity’ testing and evaluation.
2.	ID.SC-3	The organization shall establish contractual requirements permitting the organization to review the ‘information security and cybersecurity’ programs implemented by suppliers and third-party partners.
3.	PR.AC-7	The organization shall perform a documented risk assessment on organization’s critical system transactions and authenticate users, devices, and other assets (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks).
4.	PR.MA-1	The organization shall prevent the unauthorized removal of maintenance equipment containing organization’s critical system information.
5.	PR.MA-1	Maintenance tools and portable storage devices shall be inspected when brought into the facility and shall be protected by anti-malware solutions so that they are scanned for malicious code before they are used on organization’s systems.
6.	PR.MA-1	The organization shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.
7.	PR.PT-2	Portable storage devices containing system data shall be controlled and protected while in transit and in storage.
8.	DE.AE-1	The organization shall ensure that a baseline of network operations and expected data flows for its critical systems is developed, documented and maintained to track events.

D. Controls linked to the management aspects of the Assurance Level “Essential”

In addition to the key measures, the following elements shall be evaluated in every audit (initial audit, surveillance audit or recertification audit) for the assurance level “Essential”:

1. Internal audits

1.a.	internal audit (e.g. self-assessment)	
1.b.	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.	Sub-category: DE.DP-5

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

2.a.	<ul style="list-style-type: none"> Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners. The organization shall appoint an information security officer. 	Sub-category: ID.AM-6
2.b.	Information security and cybersecurity risks shall be documented, formally approved, and updated when changes occur.	Sub-category: ID.GV-4
2.c.	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.	Sub-category: ID.RM-1
2.d.	The organization shall clearly determine its risk appetite.	Sub-category: ID.RM-2
2.e.	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.	Sub-category: ID.SC-1
2.f.	<ul style="list-style-type: none"> The organization shall conduct and document risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence. Risk assessment results shall be disseminated to relevant stakeholders. 	Sub-category: ID.RA-5
2.g.	Capacity planning shall ensure adequate resources for organization's critical system information processing, networking, telecommunications, and data storage.	Sub-category: PR.DS-4
2.h.	<ul style="list-style-type: none"> 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. The organization shall coordinate the development and the testing of incident response plans and recovery plans with stakeholders responsible for related plans. 	Sub-category: PR.IP-9

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. Complaints handling

4.a.	Negative impacts to organization's operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.	Sub-category: DE.AE-4
4.b.	The organization shall communicate recovery activities to predefined stakeholders, executive and management teams.	Sub-category: RC.CO-3

5. Progress of planned activities aimed at continual improvement

5.a.	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.	Sub-category: ID.RA-6
5.b.	<ul style="list-style-type: none"> • Improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned, shall be incorporated into detection process revisions. • 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. 	Sub-category: DE.DP-5

6. Review of any changes

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

7. Use of marks and reference to certification

See PART III Assurance Level Labelling.

E. Mapping to ISO/IEC 17021-1 (informative)

See Part II, Annex G of this CAS.