



# **CyberFundamentals Framework Scheme Maintenance Procedure**

**Version : 10<sup>th</sup> January 2024**

## Document Change Log

Version	Reason for revision	Type of Revision
2024-01-10	New document	Complete document

# Table of Contents

<b>Introduction .....</b>	<b>4</b>
1. General remarks .....	4
2. Normative References .....	4
3. Definitions and acronyms .....	5
4. Disclaimer .....	5
<b>PART I Obligations for scheme owners .....</b>	<b>7</b>
1. General obligations .....	7
2. Clarification and complaints obligations .....	7
3. Review of the scheme .....	8
3.1. Phase 1: Technical adaptation of the CAS .....	8
3.2. Phase 2: Verification of the CAS by the AB's .....	9
<b>PART II Terms of Reference (ToR) of the Scheme Owner Group .....</b>	<b>10</b>
1. Status of the Scheme Owner Group and voting rights .....	10
2. CAS maintenance procedure: Expected contributions and timelines .....	10
2.1. Collecting information from Scheme owners .....	11
2.2. First proposal for changes to the CAS .....	11
2.3. Scheme Owner Group meeting to determine draft changes of the CAS .....	11
2.4. Public consultation on the draft changes of the CAS .....	12
2.5. Distribution of comments from public review .....	12
2.6. Scheme Owner Group meeting to decide on the changes of the CAS .....	12
2.7. Evaluation of the CAS by the AB's .....	13
3. Clarification and complaints procedure .....	13
3.1. Clarification process .....	14
3.2. Complaints process .....	14
<b>PART III Application and exclusion procedure .....</b>	<b>15</b>
1. Eligibility as scheme owner .....	15
2. Application process as a scheme owner .....	15
3. Exclusion procedure .....	15
<b>Annex A Application as a scheme owner .....</b>	<b>16</b>

# Introduction

## 1. General remarks



The CyberFundamentals Framework is a framework created by the Centre for Cybersecurity Belgium (CCB), operating under the authority of the Prime Minister of Belgium. The CCB maintains the documents of the scheme as Primary Scheme Owner.

In order to maintain the content of the scheme a Scheme Owners Group is composed by all competent authorities in the domain of cybersecurity that can supervise the operation of the scheme in their country (further detail provided in Part II of this document).

All competent authorities that have committed themselves to the rules of scheme owners can request the participation as scheme owners.

As Primary Scheme Owner, the Centre for Cybersecurity Belgium (CCB) is responsible for maintaining the content of the framework's related documents.

Changes to the scheme are decided in the Scheme Owner Group according to the Terms of Reference (ToR - see Part II) 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.

In order to achieve the objectives above and achieve acceptance of this Conformity Assessment Scheme (CAS), the criteria of IAF MD25 and EA 1/22 are followed.

*Note: Acceptance of the CAS by the AB, EA or IAF does not mean a judgement on the market value or usefulness of the technical requirements of the CAS.*

The CyberFundamentals Framework is available on [www.cyfun.eu](http://www.cyfun.eu).

The Scheme Owner Group is also available on [www.cyfun.eu](http://www.cyfun.eu).

## 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
EA 1/22	EA procedure and criteria for the evaluation of conformity assessment schemes by EA accreditation body members
IAF PL 3	Policies and Procedures on the IAF MLA Structure and for Expansion of the

# CyberFundamentals Framework

## Scheme Maintenance Procedure

	Scope of the IAF MLA
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.

AB	Accreditation Body
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 Belgian 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
hAB	Home AB, primary AB leading the evaluation procedure
NAB	National Accreditation Body (in Belgium: BELAC)
NCCA	National Cybersecurity Certification Authority
RD	Royal Decree
SO	Scheme owner
ToR	Terms of Reference
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.

## CyberFundamentals Framework Scheme Maintenance Procedure

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    Obligations for scheme owners

## 1. General obligations

1. In case a scheme owner (SO) provides any clarification on the Conformity Assessment Scheme (CAS) to any interested party, this information shall also be available to the Accreditation Bodies (AB) and Conformity Assessment Bodies (CAB) active within the CAS. This is done through clarification requests that are treated according to the complaints and clarification process as described in chapter 2.
2. The SO shall have a legally enforceable agreement with ABs and/or CABs in which it authorizes, as a minimum, that the ABs and/or CABs use the CAS as published by the SO, without any additions or reductions, and comply with SO rules for applying the symbol/statement/mark, as applicable.
3. The SO shall apply the complaints procedure (Chapter 2) for dealing with complaints relating to the CAS and shall ensure this not conflicts with complaints processes of CABs' clients, CABs and ABs. Investigation and decision on complaints shall not result in any discriminatory actions.
4. An arrangement describing the relationship and the terms of cooperation between the SO and the AB(s) shall be established and included in the CAS.
5. Collaboration with European AB's is established through the procedure EA 1/22 unless the scheme is accepted by IAF under procedure IAF PL3. In that case the Primary Scheme Owner is designated and authorized by the Scheme Owner Group to fulfil the obligations towards IAF taking into account the ToR of the Scheme Owner Group (see Part II)
6. If the SO monitors the CABs, it should consider cooperation with the ABs and have a feedback mechanism to provide information on the performance of the CABs to the ABs concerned.

## 2. Clarification and complaints obligations

All relevant stakeholders can request a clarification to a scheme owner.

Only impacted stakeholders can issue a complaint to the relevant scheme owner. In case of a complaint on the functioning of a scheme owner, the complaint can be received by any scheme owner.

# CyberFundamentals Framework

## Scheme Maintenance Procedure

The format of the complaint or clarification can be determined by the scheme owner. Each scheme owner is obliged to follow and contribute to the complaints and clarification process as described in the ToR (see Part II).

The output of the clarification process shall be formulated in the format determined by the clarification register. Scheme owners are responsible for transferring the information to the Primary Scheme Owner.

The output of the complaints procedure is not made publicly available. If the complaint results in the suggestion of a change to the CAS, the scheme owner is responsible to provide anonymised input.

More detail on clarification and complaints is available in Part II of this document.

### 3. Review of the scheme

The review of the scheme is done in 2 phases.

Phase	Action	Performed by
1	Technical adaptation of the scheme.	Scheme Owner Group
2	Verification of criteria for evaluation of conformity assessments schemes	Accreditation Bodies

#### 3.1. Phase 1: Technical adaptation of the CAS

The scheme owners will collect

- all remarks, complaints and clarification requests during the last period
- relevant changes in the level 1 to level 4 documents (IAF PL3) that require a change in the CAS
- relevant information from the practice of the scheme
- relevant information from cyberattacks
- relevant changes in the standards referred within the framework

The Scheme Owner Group will make a proposal for the scheme changes. Only the proposal for scheme change that have received approval according to the ToR (see Part II) will be communicated.

The Scheme Owner Group will communicate the proposal for the scheme change to the relevant stakeholders such as: competent authorities, Accreditation Bodies, Conformity Assessment Bodies, Users of the scheme. The users will receive 1 month to provide feedback to involve them in the maintenance of the scheme.

The feedback on the proposed scheme changes will be discussed within the Scheme Owner Group. Only the proposal for scheme change that have received approval according to the ToR (see Part II) will be approved for implementation.

Based on the impact of the changes, a transition delay will be decided by the Scheme Owner Group.



### 3.2. Phase 2: Verification of the CAS by the AB's

The Primary Scheme Owner will initiate the process of verification of the CAS by the Home AB (hAB) as defined in EA 1/22. Through this coordinated process AB's collaborate to the evaluation of the CAS.

The Primary Scheme Owner is responsible for sharing the feedback of the AB's with the Scheme Owner Group.

## PART II Terms of Reference (ToR) of the Scheme Owner Group

### 1. Status of the Scheme Owner Group and voting rights

The CCB maintains the documents of the scheme as Primary Scheme Owner. In order to maintain the scheme, a Scheme Owner Group is composed by all competent authorities in the domain of cybersecurity that can supervise the operation of the scheme in their country.

The Primary Scheme Owner is an entity that is legally responsible for its activities. It has the authority and obligation to establish and change the CAS with respect to the ToR and in collaboration with the Scheme Owner Group.

The Scheme Owner Group is responsible for

- monitoring the effectiveness of the scheme
- improving the effectiveness
- involving the interested parties, government initiatives and regulatory needs
- compliance of the CAS with the existing standards and rules on accreditation.

In this respect 2 elements will be crucial for the maintenance of the scheme:

- Relevant information from successful cyberattacks are extremely important as it is the means to validate changes in the scheme and keep the scheme as close as possible to real life situation
- Next to that the alignment with existing standards and accreditation rules are important to enable trust and mutual recognition of the scheme. With this respect, feedback of the AB's are to be taken into account.

Those elements are the leading factors to a general consensus oriented process to maintain the CAS.

Competent authorities from the same country can be member of the Scheme Owner Group. They will only have one vote as a member state. Different competent authorities of the same member state can make agreements on the voting status. In absence of this voting status the partial vote will be attributed based on the number of competent authorities of that member state (e.g. 2 competent authorities will both receive  $\frac{1}{2}$  of a vote).

### 2. CAS maintenance procedure: Expected contributions and timelines

The Primary Scheme Owner will plan a review and maintenance of the scheme. The planning might be determined by the alignment with existing standards and will include a timeline for:

- Collecting information from scheme owners
- Distribution deadline for the suggestions for change by the Primary Scheme Owner
- Planning of the Scheme Owner Group meeting (at least a week after the distribution of suggestions) to discuss the proposed suggestions
- Public review period of 4 weeks on the proposed changes
- Distribution of the comments from public review

# CyberFundamentals Framework

## Scheme Maintenance Procedure

- Planning of the Scheme Owner Group meeting (at least a week after the distribution of the comments)

### 2.1. Collecting information from Scheme owners

Scheme owners are expected to collect relevant information including

- Information from remarks, requests for clarification and complaints
- Relevant information on cyberattacks containing : anonymized description of the attack vectors used
- Relevant feedback on the operation of the scheme
- Relevant feedback of the AB

The scheme owner may suggest adaptations of the scheme including

- Change of key measures based on observed attack vectors
- Clarification of technical requirements (requirements, guidance, references)
- Changes to the CAS

The scheme owner will transfer the relevant information and, when applicable, the suggestions for adaptation in accordance with the Update planning provided by the Primary Scheme Owner.

### 2.2. First proposal for changes to the CAS

The Primary Scheme Owner will collect the information from the scheme owners and will make an initial proposal for adaptation of the scheme.

Suggestions from scheme owners are included in that proposal (note: multiple suggestions for change can be made).

The suggestions are distributed to the scheme owners at least one week before the Scheme Owner Group meeting.

### 2.3. Scheme Owner Group meeting to determine draft changes of the CAS

The proposals for change are discussed in the Scheme Owner Group in order to achieve a consensus agreement. Whenever a consensus is not possible a voting procedure may be initiated.

Proposals are accepted by a simple majority of votes of the scheme owners present in the meeting. Every member state represented receives one vote.

Only approved changes will be included in the draft changes of the scheme.

The approved changes of the scheme will be made available for a 4 weeks public consultation. The Primary Scheme Owner will determine the format of the feedback

### 2.4. Public consultation on the draft changes of the CAS

The approved changes of the scheme will be distributed through the scheme owners and be made available for public consultation. At least the following stakeholders should be notified:

- Users of the CAS (holders of the verification statements or certifications)
- CAB's
- AB's and competent authorities

The Primary Scheme Owner will determine the format of the feedback. Feedback will be collected by the Primary Scheme Owner who provides transparency to the Scheme Owner Group.

### 2.5. Distribution of comments from public review

The Primary Scheme Owner will collect the feedback and make a proposal for decision. The proposal can consist of maintaining the draft proposal, a new suggestion of change or proposal to withdraw the change.

The comments with suggestions are distributed to the Scheme Owner Group.

### 2.6. Scheme Owner Group meeting to decide on the changes of the CAS

The Scheme Owner Group will receive the comments, suggestions, and proposal for decision, at least a week before the Scheme Owner Group meeting.

The proposals for change are discussed in the Scheme Owner Group in order to achieve a consensus agreement. Whenever a consensus is not possible a voting procedure may be initiated.

Proposals for change are decided by a 2/3th majority of the votes of the scheme owners present in the meeting.

Proposals that did not receive a majority are not included in the update.

As an exception of the above voting rules, a simple majority is sufficient for approval when a change is induced by the changes to standards or rules related to accreditation. If no majority is reached the "elimination process" is initiated.

Note that excluding changes required as a result of changes in standards or rules related to accreditation may lead to a negative evaluation of the CAS. Therefore, a "Plurality with Elimination Voting"-process between draft proposals is possible if no consensus or majority can be reached.

#### "Plurality with Elimination Voting"-process

The plurality with elimination method requires voters to rank their preferences. If no draft proposal has a majority of first preferences, the least popular draft proposal is eliminated and its votes allocated according to second preferences. The process is repeated until a draft proposal has a majority.

A draft proposal has a plurality if it has the largest share of votes without reaching a majority, meaning more than 50%. Plurality with elimination uses multiple run-offs to eliminate draft proposals until one reaches majority.

## CyberFundamentals Framework Scheme Maintenance Procedure

A draft proposal has a majority when it has more than 50% of available votes. The plurality with elimination method uses multiple run-offs to eliminate lower-ranked draft proposals until one reaches a majority.

In case of an equal number of votes between 2 remaining proposals, the vote of the Primary Scheme Owner is decisive.

### 2.7. Evaluation of the CAS by the AB's

The final changes are transferred to the hAB, EA or IAF for final approval.

In case of EA evaluation, procedure EA 1/22 is initiated and followed-up by the Primary Scheme Owner.

In case of the IAF evaluation, IAF PL3 is applicable and managed by the Primary Scheme Owner. (Note that this procedure has to be initiated when a non-EA member requires participation and mutual recognition)

In both procedures the Primary Scheme Owner is responsible for the financial arrangements related to the evaluation procedure.

Remarks resulting from the evaluation process are distributed within the Scheme Owner Group. Changes to the CAS following these remarks are subject to approval. The Primary Scheme Owner drafts an answer to the remarks including a proposal for change to the CAS, and will issue a vote 'written procedure' or organize voting through a meeting.

Since the answer to the remarks can lead to a non-acceptance of the CAS, a simple majority of the expressed votes is required for approval. If no consensus can be reached, suggestions to adapt the answer and thus the proposal for change to the CAS are collected from the scheme owners and the voting process will start.

When no consensus can be reached, the under 2.6 above described "Plurality with Elimination Voting"-process has to be used.

The above results in a by consensus and agreed upon updated answer and proposal for change to the CAS. The "Evaluation of the CAS by the AB's"-process (this paragraph 2.7) will then be repeated.

### 3. Clarification and complaints procedure

All relevant stakeholders can request a clarification.  
Only impacted stakeholders can issue a complaint.

The format of the complaint or clarification can be determined by the scheme owner. Complaints and clarifications can be received by the relevant scheme owner. In case of a complaint on the functioning of a scheme owner, the complaint can be received by any scheme owner.

Note: not every explanation of a scheme is to be categorized as a clarification. A clarification is needed where the scheme leads to an ambiguous interpretation of the requirements.

### 3.1. Clarification process

1. Gathering information: the receiver will evaluate whether sufficient information is present and will request additional information as appropriate
2. Investigation: The scheme owner will investigate the issue and can seek further information and advice to have a clear view on the content in order to understand the issue
3. Proposal: The scheme owner will draft a proposal of decision and answer. Whenever the scheme owner evaluates that a clarification is required, he transfers the proposal for clarification to the Scheme Owner Group.  
Note: this clarification may include suggestions to change the CAS.
4. Validation: Validation is done by the Scheme Owner Group based on consensus. Whenever no consensus is reached, the clarification process ends.
5. Follow-up of the execution: The relevant scheme owners will follow-up the clarification process and report at regular intervals the status to the Primary Scheme Owner.

Results on clarifications are completed in the clarification register, managed by the Primary Scheme Owner on a publicly available website.

### 3.2. Complaints process

1. Gathering information: the receiving scheme owner will evaluate whether sufficient information is present and will request additional information as appropriate. The receiving scheme owner will evaluate whether they are the relevant scheme owner for this complaint and inform the complainant if this would not be the case. For the latter the scheme owner will also provide the complainant information what steps need to be followed.
2. Investigation: The relevant scheme owner will investigate the issue and can seek further information and advice to have a clear view on the content in order to understand the issue
3. Proposal: The relevant scheme owner will draft a proposal of decision and answer. Whenever the scheme owner evaluates that a clarification or change of the CAS is required, he transfers the proposal for clarification to the Scheme Owner Group.
4. Validation:
  - In the case of a complaint about the functioning of the scheme owner: Validation is done by the Scheme Owner Group based on consensus. Whenever no consensus is reached, the decision is taken by a vote where a simple majority is required.
  - In case of another complaint the scheme owner handling the complaint is responsible for the validation.
5. Follow-up of the execution
  - In the case of a complaint about the functioning of the scheme owner: The relevant scheme owner will follow-up the decision and report at regular intervals the result to the Primary Scheme Owner and debrief the Scheme Owner Group within the decided deadlines
  - In case of another complaint the relevant scheme owner handling the complaint is responsible for the follow-up of the complaint.

The outcome of the complaint-process is not publicly shared.

## PART III Application and exclusion procedure

### 1. Eligibility as scheme owner

In order to be eligible as a scheme owner, applicants shall demonstrate that:

- They are a governmental body (\*)
- They have authority in the domain of cybersecurity (\*)
- They are included in the implementation of the national cybersecurity strategy (\*)
- They have the authority to cooperate with their national accreditation body (\*)
- They are committed to accept the results from CAB's accredited by any AB which follows the requirements laid down in the CAS
- They shall restrict the use of the CAS to CAB's with which an agreement has been entered into. Such an agreement must guarantee at least that the CAB's will use the CAS as it is, without limitations and without additions.
- Will fulfil the obligations of the Scheme Owner as member of the Scheme Owner Group
- Is committed to collaborate with other scheme owners in a consensus building approach.

The above can be demonstrated through the signing of an application form (see Annex A) and the delivery of the evidence for the elements marked with an (\*)

### 2. Application process as a scheme owner

The application of a scheme owner is communicated to the Scheme Owner Group.

If no objection is received from the Scheme Owner Group within 2 weeks, the applicant is accepted. When a scheme owner has a question or an objection, a meeting will be organized within 2 weeks to discuss and reach a consensus.

In the event that no consensus can be reached, a voting procedure will require a 2/3 majority of all present votes during a voting procedure with the presence of 2/3 of all votes of the Scheme Owner Group.

### 3. Exclusion procedure

In the unlikely event that a scheme owner would not be fulfilling the obligations related to the operation of the CAS, any scheme owner can formulate a complaint.

If the complaint cannot be handled to the satisfaction of the complainant, the complainant can escalate to the Scheme Owner Group. In the Scheme Owner Group, a consensus will be sought to solve the issue.

In the event of repeated non fulfilment of the obligations a scheme owner can be expelled from the Scheme Owner Group. In that case a 2/3 majority of all present votes is required during a voting procedure with the presence of 2/3 of all votes of the Scheme Owner Group.

## Annex A Application as a scheme owner

Name Cybersecurity Authority	
Address	
Country	
Represented by:	
Function of the representative:	

Applicants shall demonstrate that:

OBLIGATIONS	EVIDENCE (or reference to evidences in annex)
The applicant is a governmental body	
The applicant is included in the implementation of the national cybersecurity strategy	
The applicant has authority in the domain of cybersecurity	
The applicant has the authority to cooperate with their national accreditation body	
The representative is entitled to make a commitment of the organization which he/she represents.	

As applicant as a scheme owner, the organization obliges itself

- to accept the results from CAB's accredited by any AB which follows the requirements laid down in the CAS
- to restrict the use of the CAS to CAB's with which an agreement has been entered into. Such an agreement must guarantee at least that the CAB's will use the CAS as it is, without limitations and without additions.
- to fulfil the obligations of the Scheme Owner as member of the Scheme Owner Group
- to be committed to collaborate with other scheme owners in a consensus building approach.

Representative	
Signature	
Date	

The form shall be sent to the Primary Scheme Owner ([certification@ccb.belgium.be](mailto:certification@ccb.belgium.be)), who initiates the application procedure.



## Annex B Acceptance as a scheme owner

The following Cybersecurity Authority is formally accepted as a scheme owner:

Name Cybersecurity Authority	
Address	
Country	

The Scheme Owner is accepted as member of the Scheme Owner Group and is included in the maintenance process of the CyberFundamentals Framework in accordance with the Scheme Maintenance Procedure

We welcome the above mentioned organisation as a new member of the Scheme Owner Group in our effort to maintain the CyberFundamentals as an effective and efficient tool to ensure a more cybersecure society.

On behalf of the Scheme Owner Group,

Representative      Johan Klykens  
Director Cybersecurity Certification Authority of CCB  
Representative of the Primary Scheme Owner

Signature

Date