CENTRE FOR CYBERSECURITY BELGIUM

Authorisation conditions for Conformity Assessment Bodies (CAB)

Version : 27 September 2024

Document Change Log

Version	Reason for revision	Type of Revision
2024-07-05	Creation of the document	New document
2024-09-20	Clarification	Adding: In Introduction: 4. Confidentiality of information In PART II and PART III: Uploading information in the database of the certification authority of the Centre for Cybersecurity Belgium (CCB)
2024-09-27	Clarification of accreditation requirements	The NAB operates under EU Regulation 765/2008, operates under the IAF MLA and is based in a country where the NIS2 regulation apply.

Table of Contents

Introduction

1. Legal basis

In the context of the implementation of the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of public security interest – transposing in Belgium the European directive (EU) 2022/2555 (known as the NIS2 law) and its royal decree of 09 June 2024, Conformity assessment bodies wishing to assess compliance with the Belgian NIS2 legislation shall have an accreditation, granted by the National Accreditation Body, and an authorisation granted by the CCB. Regardless if the conformity assessment is voluntary or mandatory for the entity concerned.

This document explains the different conditions for receiving such an authorisation.

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/IEC 27001	Information security, cybersecurity and privacy protection - Information security management systems - Requirements
IAF PL 3	Policies and Procedures on the IAF MLA Structure and for Expansion of the scope of the IAF MLA

3. Definitions and acronyms

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

BELAC	The Belgian National Accreditation Body according to the Royal Decree of 31 January 2006, establishing the BELAC accreditation system for conformity assessment bodies. BELAC is attached to the Belgian 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 (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, unless otherwise determined by national legislation.
CAS	Conformity Assessment Scheme
CCB	Centre for Cybersecurity Belgium, federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister. Designated as National cybersecurity authority by the NIS2 law and RD.

CyFun	CyberFundamentals Framework
IAF	International Accreditation Forum
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MLA	Multilateral Recognition Arrangement
NAB	National Accreditation Body (in Belgium: BELAC)
NIS2 law	Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of public security interest.
NIS2 RD	Royal Decree of 09 June 2024 executing the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of public security interest.
TLP	Traffic Light Protocol

4. Confidentiality of information

All information obtained or created during the performance of the supervision activities of the certification authority of the Centre for Cybersecurity Belgium (CCB) under the NIS2 Act shall be treated as confidential, except where derogation is required by legal provisions.

PART I Authorisation conditions for CyberFundamentals accredited CABs

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.

Assessment of the CyberFundamentals Framework, whether the conformity assessment is voluntary or mandatory for the entity concerned, is performed as described in the CyberFundamentals Conformity Assessment Scheme by CABs that are accredited for assessing this scheme by a NAB (e.g. BELAC).

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

The CyberFundamentals Conformity Assessment Scheme is available on www.cyfun.eu.

The acronym “CyFun” stands for “The CyberFundamentals Framework” and is a registered trademark owned by the CCB.

The use of the acronym CyFun® and/or parts of this document are authorised, as long as the source is clearly mentioned.

2. Authorisation conditions

According to articles 14 and 15 of the RD NIS2 of 09 June 2024, the following conditions shall be met for obtaining an authorisation:

- The CAB shall be accredited in accordance with the CyberFundamentals Conformity Assessment Scheme by a NAB (e.g. BELAC), and has to present a valid accreditation certificate. The CCB can request details from the NAB regarding this accreditation to support its authorisation decision.

- A legally binding agreement, as in the NIS2 Authorisation Request on www.cyfun.eu , shall be in place between the CAB and the CCB:
  - This agreement enforces the use of the scheme without limitations or additions and will require collaboration with the scheme owner.
  - The agreement includes the obligation for the CAB to provide a yearly report to the CCB with the following data:

    For CABS operating for assurance levels ‘Basic’ and ‘Important’

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

For CABS operating for assurance level 'Essential'

- 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)
- Appeals (received, treated)

- The agreement includes the obligation for the CAB to cooperate on any request from the CCB regarding the verification or certification activities.
  - Failure to respond to any request from the CCB will lead to a warning.
  - Repeated insufficient response to a request from the CCB might lead to a warning.
  - When the inspection service of the national cybersecurity authority establishes a violation of the authorisation conditions referred to in this document, the inspection service may, through the procedure referred to in Section 1 of Chapter 2 of Title 4 of the NIS2 law, give notice to the conformity assessment body to put an end to the violation. Otherwise, the national cybersecurity authority may suspend or revoke the authorisation.

PART II Authorisation conditions for ISO/IEC 27001 accredited CABs

1. General remarks

This chapter concerns CABs accredited to certify management systems in conformance with ISO/IEC 27001 according to ISO/IEC 17021-1.

The accreditation of the CAB is granted by a NAB that :

- Operates according to the EU Regulation 765/2008 setting out the requirements for accreditation and market surveillance.

And

- Operates under the IAF Multilateral Recognition Arrangement (MLA) as described in IAF PL 3.

And

- Is based in a country where the NIS2 regulation apply.

2. Authorisation conditions

According to articles 14 and 15 of the NIS2 RD, the following conditions shall be met for obtaining an authorisation:

- The CAB shall be accredited to certify management systems in conformance with ISO/IEC 27001 according to ISO/IEC 17021-1 and has to present a valid accreditation certificate.
  The CCB can request details from the NAB regarding this accreditation to support its authorisation decision.

- A legally binding agreement, as in the NIS2 Authorisation Request on www.cyfun.eu , shall be in place between the CAB and the CCB, including
  - The obligation for the CAB to provide a yearly report to the CCB with the following data:
    - List of active ISO 27001 certificates in a NIS2 compliancy context + name of entities + Company registration number (when available) + contact
    - List of refused or revoked certifications
    - List of certificates currently suspended
    - Complaints (received, treated)
    - Appeals (received, treated)
  - Uploading information in the database of the certification authority of the Centre for Cybersecurity Belgium (CCB) in the context of ISO/IEC 27001 certification
    - The authorised conformity assessment body (CAB) shall upload each ISO/IEC 27001 certificate and the associated Statement Of Applicability granted in a NIS2 context into the database of the certification authority of the Centre for Cybersecurity Belgium (CCB). For this purpose, the certification authority of the Centre for Cybersecurity Belgium (CCB) will provide the necessary instructions.
    - Entities that opt for the use of an ISO/IEC 27001 certification to obtain a presumption of conformity with NIS2 are, as stipulated in the Royal Decree of 09 June 2024 (Royal Decree implementing the Law of 26 April 2024 establishing a framework for the cyber

security of network and information systems of general interest for public security) Art 22 §1 2° obliged to provide the CCB with the scope and Statement of Applicability.

- The agreement includes the obligation for the CAB to cooperate on any request from the CCB regarding the above certification activities.
  - Failure to respond to any request from the CCB will lead to a warning.
  - Repeated insufficient response to a request from the CCB might lead to a warning.
  - When the inspection service of the national cybersecurity authority establishes a violation of the authorisation conditions referred to in this document, the inspection service may, through the procedure referred to in Section 1 of Chapter 2 of Title 4 of the NIS2 Act, give notice to the conformity assessment body to put an end to the violation. Otherwise, the national cybersecurity authority may suspend or revoke the authorisation.

PART III Authorisation conditions for CABs accredited to other IT/OT related standards

1. General remarks

This chapter concerns CABs accredited to ISO/IEC 17029 or ISO/IEC 17021-1 verifying or certifying entities against IT/OT related standards other than ISO/IEC 27001.

The accreditation of the CAB is granted by a NAB that :

- Operates according to the EU Regulation 765/2008 setting out the requirements for accreditation and market surveillance.

And

- Operates under the IAF Multilateral Recognition Arrangement (MLA) as described in IAF PL 3.

And

- Is based in a country where the NIS2 regulation apply.

2. Authorisation conditions

According to articles 14 and 15 of the NIS2 RD, the following conditions shall be met for obtaining an authorisation:

- The CAB shall be accredited to ISO/IEC 17029 or ISO/IEC 17021-1 and has to present a valid accreditation certificate.
  The CCB can request details from the NAB regarding this accreditation to support its authorisation decision.

- A legally binding agreement, as in the NIS2 Authorisation Request on www.cyfun.eu , shall be in place between the CAB and the CCB:
  - The agreement includes the obligation for the CAB to provide a yearly report to the CCB with the following data:

    For CABS accredited to ISO/IEC 17029

    - List of verification statements in a NIS2 compliancy context + contact
    - List of refused claims
    - Complaints (received, treated)
    - Appeals (received, treated)
    - Revised verification statements

    For CABS accredited to ISO/IEC 17021-1

    - List of active certificates in a NIS2 compliancy context + name of entities + Company registration number (when available) + contact
    - List of refused or revoked certifications
    - List of certificates currently suspended
    - Complaints (received, treated)

    - Appeals (received, treated)
  - Uploading information in the database of the certification authority of the Centre for Cybersecurity Belgium (CCB)
    - The authorised conformity assessment body (CAB) shall upload each certificate and the associated information granted in a NIS2 context into the database of the certification authority of the Centre for Cybersecurity Belgium (CCB). For this purpose, the certification authority of the Centre for Cybersecurity Belgium (CCB) will provide the necessary instructions.

- The agreement includes the obligation for the CAB to cooperate on any request from the CCB regarding the verification or certification activities.
  - Failure to respond to any request from the CCB will lead to a warning.
  - Repeated insufficient response to a request from the CCB might lead to a warning.
  - When the inspection service of the national cybersecurity authority establishes a violation of the authorisation conditions referred to in this document, the inspection service may, through the procedure referred to in Section 1 of Chapter 2 of Title 4 of the NIS2 Act, give notice to the conformity assessment body to put an end to the violation. Otherwise, the national cybersecurity authority may suspend or revoke the authorisation.