CENTRE FOR CYBERSECURITY BELGIUM

# Autorisatievoorwaarden voor conformiteitsbeoordelingsinstanties (CAB)

**Versie : 27 september 2024**

# Logboek documentwijzigingen

| Versie | Reden voor herziening | Type herziening |
|---|---|---|
| 2024-07-05 | Creatie van het document | Nieuw document |
| 2024-09-20 | Verduidelijking | Toevoeging van:<br>In Inleiding: 4. Vertrouwelijkheid van informatie<br>In DEEL II en DEEL III: Opladen van informatie in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB) |
| 2024-09-27 | Verduidelijking van de accreditatievoorwaarden | De NAB werkt volgens de EU-verordening 765/2008, werkt onder de IAF MLA en is gevestigd in een land waar de NIS2 regelgeving van toepassing is. |

# Inhoudsopgave

# Inleiding

## 1. Wettelijke basis

In het kader van de uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid – het omzetten in België van de Europese richtlijn (EU) 2022/2555 (bekend als de NIS2-wet) en het koninklijk besluit van 9 juni 2024, moeten conformiteitsbeoordelingsinstanties die de naleving van de Belgische NIS2-wetgeving willen beoordelen, een accreditatie hebben, toegekend door de Nationale Accreditatie-instantie, en een autorisatie, toegekend door het CCB. Ongeacht of de conformiteitsbeoordeling vrijwillig of verplicht is voor de betrokken entiteit .

In dit document worden de verschillende voorwaarden voor het verkrijgen van een dergelijke autorisatie uitgelegd.

## 2. Normatieve referenties

De volgende documenten waarnaar wordt verwezen, zijn onmisbaar voor de toepassing van dit document. Voor gedateerde referenties geldt alleen de genoemde editie. Voor ongedateerde referenties geldt de laatste editie van het document waarnaar wordt verwezen (inclusief eventuele amendementen).

| | |
|---|---|
| ISO/IEC 17000 | Conformiteitsbeoordeling - Woordenlijst en algemene principes |
| ISO/IEC 17021-1 | Conformiteitsbeoordeling - Eisen voor instanties die audits uitvoeren en certificatie van managementsystemen - Deel 1: Eisen |
| ISO/IEC 17029 | Conformiteitsbeoordeling - Algemene principes en eisen voor validatie- en verificatie-instellingen |
| ISO/IEC 27001 | Informatiebeveiliging, cyberveiligheid en privacybescherming - Beheersystemen voor informatiebeveiliging - Eisen |
| IAF PL 3 | Beleid en procedures inzake de IAF MLA-structuur en voor uitbreiding van het toepassingsgebied van de IAF MLA |

## 3. Definities en acroniemen

In dit document zijn de termen en definities uit ISO/IEC 17000 en het volgende van toepassing.

| | |
|---|---|
| BELAC | De Belgische Nationale Accreditatie-instantie volgens het Koninklijk Besluit van 31 januari 2006 tot oprichting van het BELAC-accreditatiesysteem voor conformiteitsbeoordelingsinstanties. BELAC is verbonden aan de Belgische FOD Economie, KMO, Middenstand en Energie. |
| CAB | Conformiteitsbeoordelingsinstantie<br>Alle conformiteitsbeoordelingsinstanties die in het kader van het schema actief zijn, worden geaccrediteerd door de Nationale Accreditatie-instantie (NAB) die werkt overeenkomstig EU-Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, tenzij in de nationale wetgeving anders is bepaald. |
| CAS | Conformiteitsbeoordelingschema |

| | |
|---|---|
| CCB | Centrum voor Cybersecurity België, federale administratie opgericht bij Koninklijk Besluit van 10 oktober 2014 en onder de bevoegdheid van de Eerste Minister. Aangewezen als Nationale autoriteit voor cyberbeveiliging door de NIS2 wet en KB. |
| CyFun | CyberFundamentals Kader |
| IAF | Internationaal accreditatieforum |
| IEC | Internationale Elektrotechnische Commissie |
| ISO | Internationale Organisatie voor Standaardisatie |
| MLA | Multilaterale Erkenningsregeling |
| NAB | Nationale Accreditatie-instantie (in België: BELAC) |
| NIS2-wet | Wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerken en informatiesystemen die van belang zijn voor de openbare veiligheid. |
| NIS2 RD | Koninklijk besluit van 09 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerken en informatiesystemen van openbaar belang. |
| TLP | Verkeerslichten Protocol |

## 4. Vertrouwelijkheid van informatie

Alle informatie die is verkregen of gecreëerd tijdens het uitvoeren van de supervisieactiviteiten van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB) in het kader van de NIS2-wet, wordt als vertrouwelijk behandeld, behalve wanneer hier door wettelijke bepalingen van moet worden afgeweken.

# DEEL I Autorisatievoorwaarden voor volgens CyberFundamentals geaccrediteerde CABs

## 1. Algemene opmerkingen

Het CyberFundamentals Raamwerk is een raamwerk dat eigendom is van het Centrum voor Cybersecurity België (CCB), dat opereert onder de autoriteit van de Eerste Minister van België.

De beoordeling van het CyberFundamentals Framework, of de conformiteitsbeoordeling nu vrijwillig of verplicht is voor de betrokken entiteit, wordt uitgevoerd zoals beschreven in het CyberFundamentals Conformiteitsbeoordelingschema voor CABs die geaccrediteerd zijn voor de beoordeling van dit schema door een NAB (bijv. BELAC).

Het CyberFundamentals Raamwerk is beschikbaar op www.cyfun.eu.

Het CyberFundamentals Conformiteitsbeoordelingschema is beschikbaar op www.cyfun.eu.

Het acroniem "CyFun" staat voor "The CyberFundamentals Framework" en is een geregistreerd handelsmerk van het CCB.



## 2. Autorisatievoorwaarden

Volgens de artikelen 14 en 15 van het KB NIS2 van 9 juni 2024 moet aan de volgende voorwaarden worden voldaan om een autorisatie te verkrijgen:

- De CAB moet geaccrediteerd zijn in overeenstemming met het CyberFundamentals Conformiteitsbeoordelingschema door een NAB (bv. BELAC) en moet een geldig accreditatiecertificaat voorleggen. Het CCB kan de NAB om details vragen over deze accreditatie ter ondersteuning van haar autorisatiebeslissing.

- Tussen de CAB en het CCB moet een juridisch bindende overeenkomst bestaan, zoals in het NIS2 Autorisatieverzoek op www.cyfun.eu :
  - Deze overeenkomst vereist het gebruik van het schema zonder beperkingen of toevoegingen en vereist samenwerking met de eigenaar van het systeem.
  - De overeenkomst bevat de verplichting voor de CAB om jaarlijks een verslag in te dienen bij het CCB met de volgende gegevens:

    Voor CABs die werken voor zekerheidsniveaus 'Basic' en 'Important'.

    - Lijst van verificatieverklaringen + contact
    - Lijst van geweigerde claims
    - Klachten (ontvangen, behandeld)
    - Beroepen (ontvangen, behandeld)
    - Herziene verificatieverklaringen

Voor CABs die werken voor zekerheidsniveau 'Essential'.

- Lijst van actieve certificaten + naam van entiteiten + registratienummer bedrijf (indien beschikbaar) + contactpersoon
- Lijst van geweigerde of ingetrokken certificeringen
- Lijst van certificaten die momenteel zijn geschorst
- Klachten (ontvangen, behandeld)
- Beroepen (ontvangen, behandeld)

- De overeenkomst omvat de verplichting voor de CAB om mee te werken aan elk verzoek van het CCB met betrekking tot de verificatie- of certificeringsactiviteiten.
  - Bij het niet reageren op een verzoek van het CCB, volgt een waarschuwing.
  - Herhaaldelijk onvoldoende antwoord op een verzoek kan leiden tot een waarschuwing
  - Wanneer de inspectiedienst van de nationale autoriteit voor cyberbeveiliging een schending van de in dit hoofdstuk bedoelde autorisatievoorwaarden vaststelt, kan de inspectiedienst volgens de procedure van titel 4, hoofdstuk 2, afdeling 1, van de Wet NIS2 de conformiteitsbeoordelingsinstantie aanmanen een einde te maken aan de schending. Zo niet, dan kan de nationale autoriteit voor cyberbeveiliging de autorisatie schorsen of intrekken.

# DEEL II Autorisatievoorwaarden voor ISO/IEC 27001 geaccrediteerde CABs

## 1. Algemene opmerkingen

Dit hoofdstuk heeft betrekking op CABs die geaccrediteerd zijn om managementsystemen te certificeren conform /IEC 27001 volgens ISO/IEC 17021-1.

De accreditatie van de CAB wordt verleend door een NAB die :

- Werkt volgens de EU-verordening 765/2008 waarin de vereisten voor accreditatie en markttoezicht zijn vastgelegd.

En

- Werkt onder de IAF Multilaterale Erkenningsregeling (MLA) beschreven in IAF PL 3.

En

- Gevestigd is in een land waar de NIS2 regelgeving van toepassing is.

## 2. Autorisatievoorwaarden

Volgens de artikelen 14 en 15 van het KB NIS2 moet aan de volgende voorwaarden worden voldaan om een autorisatie te verkrijgen:

- De CAB moet geaccrediteerd zijn om managementsystemen te certificeren conform ISO/IEC 27001 volgens ISO/IEC 17021-1 en moet een geldig accreditatiecertificaat voorleggen. Het CCB kan de NAB om details vragen over deze accreditatie ter ondersteuning van zijn autorisatiebeslissing.

- Tussen de CAB en het CCB moet een juridisch bindende overeenkomst van kracht zijn, zoals opgenomen in het NIS2 autorisatieverzoek op www.cyfun.eu , die het volgende omvat
  - De verplichting voor de CAB om jaarlijks een verslag in te dienen bij het CCB met de volgende gegevens:
    - Lijst van actieve ISO 27001-certificaten in een NIS2-context + naam van entiteiten + bedrijfsregistratienummer (indien beschikbaar) + contactpersoon
    - Lijst van geweigerde of ingetrokken certificaten
    - Lijst van certificaten die momenteel zijn geschorst
    - Klachten (ontvangen, behandeld)
    - Beroepen (ontvangen, behandeld)
  - Opladen van informatie in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB) in het kader van ISO/IEC 27001 certificatie
    - De geautoriseerde conformiteitsbeoordelingsinstantie (CAB) zal elk ISO/IEC 27001 certificaat en de daaraan verbonden toepasselijkheidsverklaring (‘Statement Of Applicability’) dat werd verleend in een NIS2 context opladen in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB). Hiervoor zal de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB) de nodige instructies verstrekken.

- Entiteiten die opteren voor het gebruik van een ISO/IEC 27001 certificatie om een vermoeden van conformiteit t.o.v. NIS2 (‘presumption of conformity’) te verkrijgen zijn zoals bepaald in het KB van 09 juni 2024 (Koninklijk besluit tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid) Art 22 §1 2° verplicht het toepassingsgebied en de toepasselijkheidsverklaring aan het CCB te bezorgen.

- De overeenkomst omvat de verplichting voor de CAB om mee te werken aan elk verzoek van het CCB met betrekking tot de bovengenoemde certificeringsactiviteiten.
  - Bij het niet reageren op een verzoek van het CCB, volgt een waarschuwing.
  - Herhaaldelijk onvoldoende beantwoorden van een verzoek kan leiden tot een waarschuwing.
  - Wanneer de inspectiedienst van de nationale autoriteit voor cyberbeveiliging een overtreding van de in dit document bedoelde autorisatievoorwaarden vaststelt, kan de inspectiedienst volgens de procedure van titel 4, hoofdstuk 2, afdeling 1, van de NIS2-wet de conformiteitsbeoordelingsinstantie aanmanen om een einde te maken aan de overtreding. Anders kan de nationale autoriteit voor cyberbeveiliging de autorisatie schorsen of intrekken.

# DEEL III Toelatingsvoorwaarden voor CABs die geaccrediteerd zijn volgens andere IT/OT-gerelateerde normen

## 1. Algemene opmerkingen

Dit hoofdstuk heeft betrekking op CABs die zijn geaccrediteerd volgens ISO/IEC 17029 of ISO/IEC 17021-1 en die entiteiten verifiëren of certificeren tegen andere IT/OT-gerelateerde normen dan ISO/IEC 27001.

De accreditatie van het CAB wordt verleend door een NAB die :

- Werkt volgens de EU-verordening 765/2008 waarin de vereisten voor accreditatie en markttoezicht zijn vastgelegd.

En

- Werkt onder de IAF Multilaterale Erkenningsregeling (MLA) beschreven in IAF PL 3.

En

- Gevestigd is in een land waar de NIS2 regelgeving van toepassing is.

## 2. Autorisatievoorwaarden

Volgens de artikelen 14 en 15 van het KB NIS2 moet aan de volgende voorwaarden worden voldaan om een autorisatie te verkrijgen:

- De CAB moet geaccrediteerd zijn volgens ISO/IEC 17029 of ISO/IEC 17021-1 en moet een geldig accreditatiecertificaat voorleggen.
  Het CCB kan de NAB om details vragen over deze accreditatie om zijn autorisatiebeslissing te ondersteunen.

- Tussen de CAB en het CCB moet een juridisch bindende overeenkomst bestaan, zoals opgenomen in het NIS2 autorisatieverzoek op www.cyfun.eu :
  - ➢ De overeenkomst bevat de verplichting voor de CAB om jaarlijks een verslag in te dienen bij het CCB met de volgende gegevens:

    Voor CABS geaccrediteerd volgens ISO/IEC 17029

    - Lijst van verificatieverklaringen in een NIS2-context + contactpersoon
    - Lijst van geweigerde claims
    - Klachten (ontvangen, behandeld)
    - Beroepen (ontvangen, behandeld)
    - Herziene verificatieverklaringen

    Voor CABs geaccrediteerd volgens ISO/IEC 17021-1

    - Lijst van actieve certificaten in een NIS2-context + naam van entiteiten + bedrijfsregistratienummer (indien beschikbaar) + contactpersoon
    - Lijst van geweigerde of ingetrokken certificaties
    - Lijst van certificaten die momenteel zijn geschorst

- Klachten (ontvangen, behandeld)
- Beroepen (ontvangen, behandeld)

➢ Opladen van informatie in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB)

- De geautoriseerde conformiteitsbeoordelingsinstantie (CAB) zal elk certificaat en de daaraan verbonden informatie dat werd verleend in een NIS2 context opladen in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB). Hiervoor zal de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB) de nodige instructies verstrekken.

- De overeenkomst omvat de verplichting voor het CAB om mee te werken aan elk verzoek van het CCB met betrekking tot de verificatie- of certificeringsactiviteiten.
  - ➢ Bij het niet reageren op een verzoek van het CCB, volgt een waarschuwing.
  - ➢ Herhaaldelijk onvoldoende beantwoorden van een verzoek kan leiden tot een waarschuwing.
  - ➢ Wanneer de inspectiedienst van de nationale autoriteit voor cyberbeveiliging een schending van de in dit hoofdstuk bedoelde autorisatievoorwaarden vaststelt, kan de inspectiedienst volgens de procedure van titel 4, hoofdstuk 2, afdeling 1, van de Wet NIS2 de conformiteitsbeoordelingsinstantie aanmanen een einde te maken aan de schending. Zo niet, dan kan de nationale autoriteit voor cyberbeveiliging de autorisatie schorsen of intrekken.