CENTRE FOR
CYBERSECURITY
BELGIUM

Conditions d'autorisation des organismes d'évaluation de la conformité (CAB)

Version : 27 septembre 2024

Journal des modifications du document

Version	Motif de la révision	Type de révision
2024-07-05	Création du document	Nouveau document
2024-09-20	Clarification	Addition de : Dans Introduction : 4. Confidentialité des informations Dans PARTIE II et PARTIE III : Téléchargement d'informations dans la base de données de l'autorité de certification du Centre pour la Cybersécurité Belgique (CCB)
2024-09-27	Clarification des exigences en matière d'accréditation	Le NAB fonctionne conformément au règlement 765/2008 de l'UE, opère dans le cadre de l'IAF MLA et est basé dans un pays où la réglementation NIS2 s'applique.

Table des matières

Introduction

1. Base juridique

Dans le cadre de la mise en œuvre de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique - transposant en Belgique la directive européenne (UE) 2022/2555 (connue sous le nom de loi NIS2) et de son arrêté royal du 9 juin 2024, les organismes d'évaluation de la conformité souhaitant évaluer la conformité à la législation belge NIS2 doivent disposer d'une accréditation, accordée par l'Organisme national d'accréditation, et d'une autorisation accordée par le CCB. Que l'évaluation de la conformité soit volontaire ou obligatoire pour l'entité concernée .

Ce document explique les différentes conditions pour recevoir une telle autorisation.

2. Références normatives

Les documents de référence suivants sont indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition du document référencé (y compris les amendements éventuels) qui s'applique.

ISO/IEC 17000	Évaluation de la conformité - Vocabulaire et principes généraux
ISO/IEC 17021-1	Évaluation de la conformité - Exigences pour les organismes d'audit et la certification des systèmes de management - Partie 1 : Exigences
ISO/IEC 17029	Évaluation de la conformité - Principes généraux et exigences pour organismes de validation et de vérification
ISO/IEC 27001	Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de gestion de la sécurité de l'information - Exigences
IAF PL 3	Politiques et procédures relatives à la structure IAF MLA et à l'extension du champ d'application de l'IAF MLA

3. Définitions et acronymes

Aux fins du présent document, les termes et définitions figurant dans la norme ISO/CEI 17000 et dans les documents suivants s'appliquent.

BELAC	L'organisme national belge d'accréditation conformément à l'arrêté royal du 31 janvier 2006 établissant le système d'accréditation BELAC pour les organismes d'évaluation de la conformité. BELAC est rattaché au SPF Economie, P.M.E., Indépendants et Energie.
CAB	Organisme d'évaluation de la conformité Tous les organismes d'évaluation de la conformité opérant dans le cadre du système doivent être accrédités par l'organisme national d'accréditation (ONA) fonctionnant conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93, sauf dispositions contraires prévues par la législation nationale.
CAS	Système d'évaluation de la conformité

CCB	Centre pour la Cybersécurité Belgique, administration fédérale créée par l'arrêté royal du 10 octobre 2014 et placée sous l'autorité du Premier ministre. Désigné comme autorité nationale de cybersécurité par la loi NIS2 et l'AR.
CyFun	CyberFundamentals Framework (Cadre des CyberFondamentaux)
IAF	Forum international de l'accréditation
CEI	Commission électrotechnique internationale
ISO	Organisation internationale de normalisation
MLA	Arrangement de reconnaissance multilatérale
NAB	Organisme national d'accréditation (en Belgique : BELAC)
Loi NIS2	Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.
NIS2 RD	Arrêté royal du 09 juin 2024 portant exécution de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.
TLP	Protocole des feux de signalisation

4. Confidentialité des informations

Toutes les informations obtenues ou créées au cours de l'exercice des activités de supervision de l'autorité de certification du Centre pour la Cybersécurité Belgique (CCB) en vertu de la loi NIS2 sont traitées de manière confidentielle, sauf si une dérogation est requise par les dispositions légales.

PARTIE I Conditions d'autorisation pour les OEC accrédités par CyberFundamentals

1. Remarques générales

Le CyberFundamentals Framework est un cadre appartenant au Centre for Cybersecurity Belgium (CCB), qui opère sous l'autorité du Premier ministre belge.

L'évaluation du cadre des principes fondamentaux du cyberespace, qu'elle soit volontaire ou obligatoire pour l'entité concernée, est effectuée selon le schéma d'évaluation de la conformité des principes fondamentaux du cyberespace par des OEC accrédités pour l'évaluation de ce schéma par un organisme d'évaluation national (par exemple BELAC).

Le CyberFundamentals Framework est disponible sur le site www.cyfun.eu.

Le schéma d'évaluation de la conformité des principes CyberFundamentals est disponible sur le site www.cyfun.eu.

L'acronyme "CyFun" signifie "The CyberFundamentals Framework" et est une marque déposée appartenant au CCB.

L'utilisation de l'acronyme CyFun® et/ou de parties de ce document est autorisée, à condition que la source soit clairement mentionnée.

2. Conditions d'autorisation

Conformément aux articles 14 et 15 de l'AR NIS2 du 9 juin 2024, les conditions suivantes doivent être remplies pour obtenir une autorisation :

- Le CAB doit être accrédité conformément au système d'évaluation de la conformité des CyberFundamentals par un NAB (par exemple BELAC) et doit présenter un certificat d'accréditation valide. Le CCB peut demander au NAB des détails concernant cette accréditation afin d'étayer sa décision d'autorisation.

- Un accord juridiquement contraignant, comme inclus dans la demande d'autorisation NIS2 sur www.cyfun.eu, doit être mis en place entre le CAB et le CCB :
  - Cet accord impose l'utilisation du schéma sans limitations ni ajouts et nécessitera une collaboration avec le propriétaire du schéma.
  - L'accord prévoit l'obligation pour le CAB de fournir un rapport annuel au CCB avec les données suivantes :

    Pour les CABS fonctionnant aux niveaux d'assurance 'Basic' et 'Important'.

    - Liste des déclarations de vérification + contact
    - Liste des demandes refusées
    - Plaintes (reçues, traitées)
    - Appels (reçus, traités)
    - Déclarations de vérification révisées

Pour les CABS opérant au niveau d'assurance 'Essential'.

- Liste des certifications actifs + nom des entités + numéro d'enregistrement de la société (si disponible) + contact
- Liste des certifications refusées ou révoquées
- Liste des certifications actuellement suspendus
- Plaintes (reçues, traitées)
- Appels (reçus, traités)

- L'accord prévoit l'obligation pour le CAB de coopérer à toute demande du CCB concernant les activités de vérification ou de certification.
  - L'absence de réponse à une demande du CCB entraînera un avertissement.
  - Une réponse insuffisante répétée à une demande du CCB peut entraîner un avertissement.
  - Lorsque le service d'inspection de l'autorité nationale de cybersécurité constate une violation des conditions d'autorisation visées dans le présent document, le service d'inspection peut, par la procédure prévue dans la section 1 du chapitre 2 du titre 4 de la loi NIS2, mettre en demeure l'organisme d'évaluation de la conformité de faire cesser la violation. Dans le cas contraire, l'autorité nationale de cybersécurité peut suspendre ou révoquer l'autorisation.

PARTIE II Conditions d'autorisation pour CABs accrédités ISO/IEC 27001

1. Remarques générales

Le présent chapitre concerne les CAB accrédités pour certifier les systèmes de management conformes à la norme ISO/CEI 27001 selon la norme ISO/CEI 17021-1.

L'accréditation du CAB est accordée par un NAB qui :

- Fonctionne conformément au règlement (CE) n° 765/2008 de l'UE fixant les exigences en matière d'accréditation et de surveillance du marché.

Et

- Opère dans le cadre de l'Arrangement IAF de reconnaissance multilatérale (MLA), décrit dans le IAF PL 3.

Et

- Est basé dans un pays où la réglementation NIS2 s'applique.

2. Conditions d'autorisation

Conformément aux articles 14 et 15 de l'AR NIS2, les conditions suivantes doivent être remplies pour obtenir une autorisation :

- Le CAB doit être accrédité pour certifier les systèmes de management en conformité avec ISO/IEC 27001 conformément à la norme ISO/IEC 17021-1 et doit présenter un certificat d'accréditation valide. Le CCB peut demander au NAB des détails sur cette accréditation pour étayer sa décision d'autorisation.

- Un accord juridiquement contraignant, comme inclus dans la demande d'autorisation NIS2 sur www.cyfun.eu, doit être mis en place entre le CAB et le CCB :
  - L'obligation pour le CAB de fournir un rapport annuel au CCB avec les données suivantes:
    - Liste des certifications ISO 27001 actifs dans un contexte de conformité NIS2 + nom des entités + numéro d'enregistrement de la société (si disponible) + contact
    - Liste des certifications refusées ou révoquées
    - Liste des certifications actuellement suspendus
    - Plaintes (reçues, traitées)
    - Appels (reçus, traités)
  - Téléchargement d'informations dans la base de données de l'autorité de certification du Centre pour la Cybersécurité Belgique (CCB) dans le cadre de la certification ISO/IEC 27001
    - L'organisme d'évaluation de la conformité (CAB) autorisé téléchargera chaque certificat ISO/IEC 27001 et la déclaration d'applicabilité associée accordés dans un contexte NIS2 dans la base de données de l'autorité de certification du Centre pour la Cybersécurité Belgique (CCB). L'autorité de certification du Centre pour la Cybersécurité Belgique (CCB) fournira les instructions nécessaires à cet effet.
    - Les entités qui optent pour l'utilisation d'une certification ISO/IEC 27001 pour obtenir une présomption de conformité avec NIS2 sont, comme stipulé dans l'Arrêté royal du 09 juin 2024 (Arrêté royal d'exécution de la loi du 26 avril 2024 établissant un

cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique) Art 22 §1 2° obligées de fournir au CCB le champ d'application et la déclaration d'applicabilité.

- L'accord prévoit l'obligation pour le CAB de coopérer à toute demande du CCB concernant les activités de certification.
  - L'absence de réponse à une demande du CCB entraînera un avertissement.
  - Une réponse insuffisante répétée à une demande du CCB peut entraîner un avertissement.
  - Lorsque le service d'inspection de l'autorité nationale de cybersécurité constate une violation des conditions d'autorisation visées dans le présent document, le service d'inspection peut, par la procédure prévue dans la section 1 du chapitre 2 du titre 4 de la loi NIS2, mettre en demeure l'organisme d'évaluation de la conformité de faire cesser la violation. Dans le cas contraire, l'autorité nationale de cybersécurité peut suspendre ou révoquer l'autorisation.

PARTIE III Conditions d'autorisation pour les CABs accrédités selon d'autres normes relatives aux IT/OT

1. Remarques générales

Le présent chapitre concerne les CAB accrédités selon la norme ISO/IEC 17029 ou ISO/IEC 17021-1 qui vérifient ou certifient des entités par rapport à des normes relatives aux IT/OT autres que la norme ISO/IEC 27001.

L'accréditation du CAB est accordée par un NAB qui :

- Fonctionne conformément au règlement (CE) n° 765/2008 de l'UE fixant les exigences en matière d'accréditation et de surveillance du marché.

Et

- Opère dans le cadre de l'Arrangement IAF de reconnaissance multilatérale (MLA), décrit dans le IAF PL 3.

Et

- Est basé dans un pays où la réglementation NIS2 s'applique.

2. Conditions d'autorisation

Conformément aux articles 14 et 15 de l'AR NIS2, les conditions suivantes doivent être remplies pour obtenir une autorisation :

- Le CAB doit être accrédité selon la norme ISO/IEC 17029 ou ISO/IEC 17021-1 et doit présenter un certificat d'accréditation valide.
  Le CCB peut demander au NAB des détails concernant cette accréditation afin d'étayer sa décision d'autorisation.

- Un accord juridiquement contraignant, comme inclus dans la demande d'autorisation NIS2 sur www.cyfun.eu, doit être mis en place entre le CAB et le CCB :
  - L'accord prévoit l'obligation pour le CAB de fournir un rapport annuel au CCB avec les données suivantes :

    Pour les CABS accrédités selon ISO/IEC 17029

    - Liste des déclarations de vérification dans un contexte de conformité NIS2 + contact
    - Liste des demandes refusées
    - Plaintes (reçues, traitées)
    - Appels (reçus, traités)
    - Déclarations de vérification révisées

    Pour les CABS accrédités selon la norme ISO/IEC 17021-1

    - Liste des certificats actifs dans un contexte de conformité NIS2 + nom des entités + numéro d'enregistrement de la société (si disponible) + contact
    - Liste des certifications refusées ou révoquées

- Liste des certificats actuellement suspendus
- Plaintes (reçues, traitées)
- Appels (reçus, traités)

➢ Téléchargement d'informations dans la base de données de l'autorité de certification du Centre pour la Cybersécurité Belgique (CCB)

- L'organisme d'évaluation de la conformité (CAB) autorisé téléchargera chaque certificat et l'information associée accordés dans un contexte NIS2 dans la base de données de l'autorité de certification du Centre pour la Cybersécurité Belgique (CCB). L'autorité de certification du Centre pour la Cybersécurité Belgique (CCB) fournira les instructions nécessaires à cet effet.

- L'accord prévoit l'obligation pour le CAB de coopérer à toute demande du CCB concernant les activités de certification.
  - ➢ L'absence de réponse à une demande du CCB entraînera un avertissement.
  - ➢ Une réponse insuffisante répétée à une demande du CCB peut entraîner un avertissement.
  - ➢ Lorsque le service d'inspection de l'autorité nationale de cybersécurité constate une violation des conditions d'autorisation visées dans le présent document, le service d'inspection peut, par la procédure prévue dans la section 1 du chapitre 2 du titre 4 de la loi NIS2, mettre en demeure l'organisme d'évaluation de la conformité de faire cesser la violation. Dans le cas contraire, l'autorité nationale de cybersécurité peut suspendre ou révoquer l'autorisation.