Module 1 : NIS2 en bref

Six leçons courtes sur ce que tout dirigeant et tout collaborateur d'une organisation NIS2 devrait savoir, suivies d'un quiz de 10 questions. Il faut 80 % pour réussir.

NIS2 Aware · nis2aware.eu · novembre 2026

LEÇON 1 SUR 6

Pourquoi NIS2 ?

Hôpitaux, ports, fournisseurs d'énergie, producteurs alimentaires, services cloud : notre économie repose sur les réseaux et les systèmes d'information. Une seule attaque par rançongiciel peut arrêter une production, bloquer des livraisons ou mettre des patients en danger, et les dégâts s'étendent souvent aux clients et aux fournisseurs.

L'Union européenne a d'abord répondu avec la **directive NIS** en 2016. Elle visait un nombre limité d'opérateurs, et chaque pays l'appliquait à sa manière. Sa remplaçante, la **directive NIS2** (directive (UE) 2022/2555), a été adoptée en décembre 2022 pour relever le niveau de cybersécurité dans toute l'Union.

Ce que NIS2 change

- **Un champ plus large :** beaucoup plus de secteurs et, en règle générale, toutes les moyennes et grandes organisations de ces secteurs.
- **Des obligations plus strictes :** un socle commun de mesures de gestion des risques et des délais de notification harmonisés.
- **La responsabilité de la direction :** l'organe de direction doit approuver et superviser la cybersécurité, et il doit être formé.
- **Un vrai contrôle :** une supervision par les autorités nationales et des amendes importantes.

La directive ne s'applique pas directement aux entreprises : chaque État membre devait la transposer dans son droit national pour le 17 octobre 2024. En Belgique, c'est la loi NIS2.

À RETENIR

- NIS2 est la directive (UE) 2022/2555, qui succède à la directive NIS de 2016.
- Elle couvre plus de secteurs et plus d'organisations, avec des règles plus strictes.
- Elle s'applique aux entreprises via le droit national.

LEÇON 2 SUR 6

La loi NIS2 belge

La Belgique a transposé NIS2 par 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, complétée par un **arrêté royal du 9 juin 2024**. La loi est entrée en vigueur le **18 octobre 2024**.

Les acteurs clés

Qui	Rôle
CCB, Centre pour la Cybersécurité Belgique	Autorité nationale de cybersécurité : supervision, inspections, sanctions et accompagnement. Son équipe CERT.be est le CSIRT national qui traite les notifications d'incidents.
Autorités sectorielles	Travaillent aux côtés du CCB dans certains secteurs (par exemple finance, télécoms, énergie, transport, santé).
Safeonweb@Work (atwork.safeonweb.be)	Le portail du CCB où les entités s'enregistrent et trouvent informations et outils.

CyberFundamentals : la boîte à outils belge

Le CCB a développé le cadre **CyberFundamentals (CyFun®)** : un ensemble de mesures de sécurité concrètes, avec des niveaux d'assurance (Basic, Important et Essential). Une version actualisée, CyFun 2025, a été publiée en octobre 2025. Les organisations peuvent utiliser CyFun, ou la norme internationale **ISO/IEC 27001**, pour structurer leurs mesures et démontrer leur conformité.

> **Bon à savoir :** NIS2 Aware est un organisme de formation indépendant. Pour l'information officielle, référez-vous toujours au CCB.

À RETENIR

- Loi NIS2 belge : 26 avril 2024, en vigueur depuis le 18 octobre 2024.
- Le CCB est l'autorité nationale ; l'enregistrement se fait sur Safeonweb@Work.
- CyberFundamentals (CyFun) ou ISO/IEC 27001 aident à structurer et à prouver vos mesures.

LEÇON 3 SUR 6

Qui est concerné ?

La loi s'applique aux organisations établies en Belgique qui remplissent deux conditions : elles sont actives dans un **secteur** visé par NIS2, et elles sont au moins de **taille moyenne**.

Condition 1 : le secteur

Secteurs hautement critiques (annexe I)	Autres secteurs critiques (annexe II)
Énergie · Transport · Banque · Infrastructures des marchés financiers · Santé · Eau potable · Eaux usées · Infrastructure numérique (cloud, centres de données, DNS, télécoms…) · Gestion des services TIC, B2B (prestataires de services informatiques et de sécurité gérés) · Administration publique · Espace	Services postaux et d'expédition · Gestion des déchets · Produits chimiques · Production, transformation et distribution de denrées alimentaires · Fabrication (dispositifs médicaux, produits informatiques et électroniques, équipements électriques, machines, véhicules à moteur, autres matériels de transport) · Fournisseurs numériques (places de marché en ligne, moteurs de recherche, réseaux sociaux) · Recherche

Condition 2 : la taille

- **Moyenne :** à partir de 50 travailleurs, ou un chiffre d'affaires annuel et un total du bilan supérieurs à 10 millions d'euros.
- **Grande :** à partir de 250 travailleurs, ou un chiffre d'affaires supérieur à 50 millions d'euros et un total du bilan supérieur à 43 millions d'euros.

Les entreprises partenaires et liées (par exemple au sein d'un groupe) peuvent être prises en compte dans ces chiffres.

Exceptions

Certaines organisations sont visées **quelle que soit leur taille**, par exemple les fournisseurs de services DNS, les registres de noms de domaine de premier niveau, les prestataires de services de confiance qualifiés et certains fournisseurs de communications électroniques publiques. Le CCB peut aussi désigner des entités spécifiques.

> **Votre responsabilité :** personne ne vous enverra de courrier. Chaque organisation doit évaluer elle-même si elle est concernée.

Pas concerné ? Vous pouvez l'être indirectement : les entités NIS2 doivent gérer la sécurité de leurs fournisseurs et vous transmettront donc des exigences.

À RETENIR

- Deux conditions : un secteur NIS2 et au moins une taille moyenne (50 travailleurs ou plus, ou plus de 10 M€ de chiffre d'affaires et de bilan).
- Certains fournisseurs numériques sont visés quelle que soit leur taille.
- Chaque organisation doit vérifier elle-même sa situation ; les fournisseurs sont touchés indirectement.

LEÇON 4 SUR 6

Entité essentielle ou importante ?

Les organisations concernées relèvent de l'une de deux catégories. Les obligations de base sont **les mêmes** ; ce qui change, c'est l'intensité de la supervision et le niveau des amendes.

	Entité essentielle	Entité importante
Profil type	Grandes organisations des secteurs hautement critiques (annexe I), plus certains cas spécifiques	Organisations moyennes de l'annexe I, et moyennes ou grandes de l'annexe II
Supervision	Proactive (*ex ante*) : le CCB peut inspecter à tout moment	Réactive (*ex post*) : surtout après un incident ou des indices de non-conformité
Évaluation de la conformité	Obligatoire et périodique (CyberFundamentals ou ISO/IEC 27001)	Volontaire, mais elle donne une présomption de conformité
Amende maximale	10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial	7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial

Au-delà des amendes, les autorités peuvent donner des instructions contraignantes et, pour les entités essentielles qui persistent dans le manquement, interdire temporairement à une personne d'exercer des fonctions de direction.

> **En pratique :** pour les entités essentielles, le CCB déploie l'évaluation de la conformité par étapes. Un premier jalon est tombé le 18 avril 2026, et d'autres suivent. Vérifiez auprès du CCB les dates qui s'appliquent à vous.

À RETENIR

- Mêmes obligations ; supervision et amendes différentes.
- Essentielle : supervision proactive et évaluation de la conformité obligatoire ; amendes jusqu'à 10 M€ ou 2 %.
- Importante : supervision réactive ; amendes jusqu'à 7 M€ ou 1,4 %.

LEÇON 5 SUR 6

Les quatre obligations clés

1. S'enregistrer

Les entités s'enregistrent auprès du CCB sur **Safeonweb@Work**. Les délais étaient fixés au 18 décembre 2024 pour certains fournisseurs numériques et au 18 mars 2025 pour toutes les autres. Une organisation qui devient concernée plus tard doit s'enregistrer sans tarder.

2. Prendre des mesures de gestion des risques

Les mesures doivent être appropriées et proportionnées aux risques, selon une approche « tous risques ». La loi vise au moins les domaines suivants :

- analyse des risques et politiques de sécurité des systèmes d'information
- gestion des incidents
- continuité des activités : sauvegardes, reprise après sinistre, gestion de crise
- sécurité de la chaîne d'approvisionnement
- sécurité de l'acquisition, du développement et de la maintenance des systèmes, y compris la gestion des vulnérabilités
- évaluation de l'efficacité des mesures
- cyberhygiène de base et formation à la cybersécurité
- cryptographie et chiffrement
- sécurité des ressources humaines, contrôle d'accès et gestion des actifs
- authentification multifacteur et communications sécurisées

3. Notifier les incidents significatifs

Délai	Quoi
24 heures	Alerte précoce au CCB après avoir pris connaissance d'un incident significatif
72 heures	Notification de l'incident avec une première évaluation
1 mois	Rapport final

Le cas échéant, les destinataires de vos services doivent également être informés.

4. Impliquer et former la direction

L'organe de direction doit **approuver** les mesures, **superviser** leur mise en œuvre, et il peut être tenu **responsable**. Ses membres doivent **suivre une formation** ; une formation régulière du personnel est également encouragée.

À RETENIR

- S'enregistrer sur Safeonweb@Work.
- Mettre en place des mesures dans au moins dix domaines, de l'analyse des risques au MFA.
- Notifier les incidents significatifs : 24 heures, 72 heures, un mois.
- La direction approuve, supervise, est responsable et doit être formée.

LEÇON 6 SUR 6

Dates clés et prochaines étapes

Décembre 2022
Adoption de la directive NIS2 au niveau européen

26 avril 2024
Adoption de la loi NIS2 belge

18 octobre 2024
Entrée en vigueur en Belgique

18 décembre 2024
Date limite d'enregistrement pour certains fournisseurs numériques

18 mars 2025
Date limite d'enregistrement pour toutes les autres entités

Octobre 2025
Publication de CyberFundamentals 2025

18 avril 2026
Premier jalon d'évaluation de la conformité pour les entités essentielles

2027 et au-delà
Autres jalons d'évaluation de la conformité pour les entités essentielles (à vérifier auprès du CCB)

Cinq étapes à suivre dès maintenant

1. **Vérifiez si vous êtes concerné** et dans quelle catégorie (essentielle ou importante).
2. **Enregistrez-vous** sur Safeonweb@Work si ce n'est pas encore fait.
3. **Évaluez vos écarts** par rapport à CyberFundamentals ou à ISO/IEC 27001 et planifiez les améliorations.
4. **Organisez la notification des incidents** : qui décide, qui notifie, dans les 24 heures.
5. **Formez votre direction et votre personnel**, et conservez-en la preuve.

> Vous avez terminé les leçons du module 1. Faites le quiz pour tester vos connaissances.

À RETENIR

- En vigueur depuis le 18 octobre 2024 ; les délais d'enregistrement sont passés.
- Les entités essentielles sont en phase d'évaluation de la conformité.
- Prochaines étapes : champ d'application, enregistrement, analyse des écarts, procédure d'incident, formation.

Ce module donne une information générale sur le cadre NIS2 belge en date de novembre 2026. Il ne constitue pas un avis juridique. Consultez toujours les dernières informations du CCB (ccb.belgium.be et atwork.safeonweb.be).