CENTRE FOR
CYBERSECURITY
BELGIUM

LA DIRECTIVE NIS2 EN BELGIQUE

Centre for Cybersecurity Belgium
Sous l'autorité du Premier Ministre

Introduction

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 (la « loi NIS2 ») transpose la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 (la « directive NIS2 »)

Afin de faire face à l'expansion du paysage des cybermenaces et à l'émergence de nouveaux défis, l'Union européenne a adopté un nouveau texte législatif concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (la directive 2022/2555 du 14 décembre 2022 - dite "directive NIS2"), qui remplace la "directive NIS1" (directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union).

La directive NIS2 apporte des changements majeurs par rapport à la directive NIS1 : élargissement des secteurs et des entités concernées, nouvelles méthodes de sélection et d'enregistrement, davantage d'exigences en matière de cybersécurité, nouveaux délais de notification des incidents et renforcement des mécanismes de supervision.

Cette directive vise également à renforcer la stratégie et les politiques nationales en matière de cybersécurité. En ce qui concerne les politiques nationales, elles comprennent les cadres et processus nationaux de gestion des crises cybers, les tâches des autorités compétentes et la coopération nationale ou internationale.

En tant qu'autorité nationale de cybersécurité, le Centre pour la Cybersécurité Belgique (CCB) joue un rôle clé dans la coordination et la mise en œuvre de cette directive. Le CCB assure les tâches d'autorité compétente pour tous les secteurs (en collaboration avec les autorités sectorielles potentielles), de CSIRT national, de point de contact national unique et de représentant au sein du Groupe de coopération NIS, du réseau CSIRT et de EU-CyCLONe.

Les entités essentielles et importantes doivent prendre des mesures appropriées et proportionnelles pour gérer les risques cybers. Ces dernières comprennent toutes les mesures organisationnelles, mais également techniques et opérationnelles, avec deux objectifs : prévenir les incidents cyber et minimiser l'impact d'incidents réussis sur la fourniture de leurs services.

Pour soutenir les organisations, le CCB a développé une guidance claire avec la création du CyberFundamentals (CyFun®) Framework. À cette fin, les entités bénéficieront d'une présomption de conformité si elles obtiennent une certification/un label CyFun® ou ISO/IEC 27001.

Les entités NIS2 doivent notifier leurs incidents significatifs au CSIRT national. Cela permet d'atténuer la propagation potentielle d'un incident et permet aux entités de demander de l'aide. Avec la réception de ces informations, le CCB peut gérer les situations de crise de la meilleure façon possible et partager les informations techniques pertinentes avec d'autres entités.

Enfin, le CCB joue également un rôle dans la supervision des entités concernées avec son service d'inspection (en collaboration avec les autorités sectorielles potentielles). La supervision a pour objectif premier de renforcer la cyber-résilience des entités, mais elle permet également d'imposer des sanctions aux entités qui ne prennent pas les mesures nécessaires.

Le présent document a comme objectif de fournir des informations générales quant à l'étendue et au contenu de la transposition de la directive NIS2[1] en Belgique.

[1] Loi NIS2 : https://www.ejustice.just.fgov.be/eli/loi/2024/04/26/2024202344/justel

Arrêté royal : https://www.ejustice.just.fgov.be/eli/arrete/2024/06/09/2024005260/justel

Table des matières

Résumé : NIS2 en sept étapes 4
I. Pourquoi NIS2 ? Et pour qui ? 5
II. Champ d'application 6
A. Taille (« size cap ») 6
B. Service fourni 8
C. Établissement 9
D. Identification et chaîne d'approvisionnement 9
E. Interaction entre NIS2 et DORA 9
III. Obligations 11
A. Enregistrement 11
B. Mesures de gestion des risques en matière de cybersécurité 11
C. Sécurité de la chaîne d'approvisionnement 12
D. Notification d'incidents (voir guide) 13
E. Obligations du management 15
IV. Supervision 17
A. Régime général 17
B. Les CyberFundamentals (CyFun®) 18
V. Sanctions 20
VI. Ligne du temps 21

Résumé : NIS2 en sept étapes

Il semble que votre organisation soit concernée par NIS2, mais vous ne savez pas par où commencer ? Le CCB a formulé les recommandations suivantes pour vous aider à répondre aux exigences de la législation NIS2 belge en seulement 7 étapes.

1. **Suis-je concerné par NIS2 ?**

   a. Dans le champ d'application : les entités NIS2 : utilisez notre outil de test du champ d'application[2] pour déterminer si votre organisation entre ou non dans le champ d'application de la loi NIS2 belge.
   b. Dans la chaîne d'approvisionnement : le CCB recommande aux entités NIS2 d'identifier les organisations essentielles à leur cybersécurité et de les inviter à mettre en œuvre au moins le niveau d'assurance Basic du référentiel CyberFundamentals.

2. **Enregistrez votre entité NIS2**

Toutes les entités NIS2 sont légalement tenues de s'enregistrer sur Safeonweb@Work[3] :

- les entités des secteurs numériques de la loi doivent s'enregistrer au plus tard pour le 18 décembre 2024.
- toutes les autres entités NIS2 doivent s'enregistrer au plus tard pour le 18 mars 2025.

3. **Préparez votre organisation à signaler et à traiter tout incident significatif à partir du 18 octobre 2024**

À partir du 18 octobre 2024, toutes les entités NIS2 sont tenues d'informer le CCB en cas d'incident significatif (voir guide).

Les incidents significatifs peuvent être notifiés au CCB via sa plateforme de notification d'incidents : **https://notif.safeonweb.be** (ou par téléphone au +32 (0)2 501 05 60 - **uniquement en cas d'urgence ou d'indisponibilité de la plateforme**).

La notification d'un incident ne constitue qu'un maillon d'un plus vaste plan de réponse aux incidents. Si votre organisation ne dispose pas encore de plan de réponse aux incidents, il peut être utile de commencer par l'un de nos modèles de politiques.

4. **Déterminez votre niveau de CyberFundamentals (CyFun®)**

Si vous optez pour notre CyFun® Framework, notre outil de sélection CyFun® vous permet de déterminer le niveau d'assurance requis (« Basic », « Important » ou « Essential ») pour votre organisation.

5. **Planifiez des moments de formation à la cybersécurité**

Avant que le conseil d'administration ou la direction ne prennent des décisions concernant les stratégies et mesures à adopter en termes de cybersécurité, il est indispensable de disposer de connaissances de base en matière de gestion des risques et de cybersécurité. Le CCB recommande de planifier la formation des cadres avant avril 2025. La formation des collaborateurs doit aussi toujours faire partie intégrante des mesures de cybersécurité.

6. **Mettez en œuvre les mesures de sécurité**

Les entités NIS2 peuvent utiliser le CyFun® Framework en trois étapes pour se conformer à NIS2 :

1) réaliser une analyse des lacunes à l'aide de l'outil d'auto-évaluation CyFun® ;
2) mettre en œuvre les mesures requises. Votre plan de mise en œuvre doit permettre l'implémentation progressive des mesures de cybersécurité en tenant compte des délais indiqués à l'étape 7 ci-dessous ;
3) mettre à jour votre auto-évaluation et rassembler les preuves nécessaires pour confirmer la mise en œuvre.

[2] https://atwork.safeonweb.be/fr/nis2

[3] https://atwork.safeonweb.be/fr/register-my-organisation

7. Faites réviser votre cybersécurité

Les entités essentielles doivent faire évaluer et réviser régulièrement leur mise en œuvre par une tierce partie. Cela peut se faire par le biais d'une certification CyFun® délivrée par un organisme d'évaluation de la conformité (OEC/CAB) accrédité et agréé. Les entités essentielles doivent obtenir le niveau d'assurance Basic ou Important avant le 18 avril 2026, le niveau final devant être certifié avant le 18 avril 2027.

Les entités importantes peuvent se soumettre à la même évaluation régulière de la conformité avec CyFun®, ce qui leur confère une présomption de conformité.

Sachez qu'en cas d'incident, il peut s'avérer très important que le conseil d'administration et le management disposent du label ou du certificat CyFun® approprié, afin de pouvoir démontrer la conformité de l'entité.

I. Pourquoi NIS2 ? Et pour qui ?

Les réseaux et systèmes d'information sont devenus un élément central de notre vie quotidienne en raison de la transformation numérique et de l'interconnexion de la société. De nombreuses activités sociétales ou économiques critiques dépendent aujourd'hui de leur bon fonctionnement.

Cette évolution a entraîné une expansion du paysage des cybermenaces et cyberincidents qui ne cessent d'augmenter. Celles-ci constituent de véritables menaces en matière de sécurité publique pour la population, les entreprises et les autorités publiques. De nos jours, un cyberincident est, en effet, susceptible de provoquer des perturbations opérationnelles graves dans des secteurs critiques et ainsi affecter des personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

L'ensemble des citoyens, des entreprises et des pouvoirs publics doivent dès lors être conscients de l'importance de se protéger préventivement contre les cybermenaces et les cyberincidents.

L'image suivante donne une brève introduction à la loi NIS2 :

II. Champ d'application

Pour être couverte par la loi NIS2 belge et sauf exceptions, une organisation doit en principe :

1. Fournir dans l'Union européenne un service figurant dans les annexes I ou II de la loi NIS2 ;
2. Dépasser les seuils de taille prévus par la recommandation de la Commission européenne 2003/361/CE, à savoir au moins 50 employés à temps plein ou avoir un chiffre d'affaires annuel/ou un bilan annuel total supérieur à 10 millions d'euros ;
3. Être établie en Belgique.

A. TAILLE (« SIZE CAP »)

La taille d'une entité est calculée sur la base de l'annexe I de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises (la « recommandation »).

La taille d'une organisation est établie sur la base de deux critères : l'effectif (mesuré en équivalents temps plein (ETP)[4]) et les montants financiers (chiffre d'affaires annuel et/ou total du bilan annuel). À quelques exceptions près[5], pour que la loi NIS2 s'applique, une organisation doit être considérée au moins comme une entreprise moyenne au sens de la recommandation. Une « moyenne entreprise » a un effectif d'au moins 50 ETP ou un chiffre d'affaires annuel et/ou un total du bilan annuel supérieur à 10 millions d'euros.

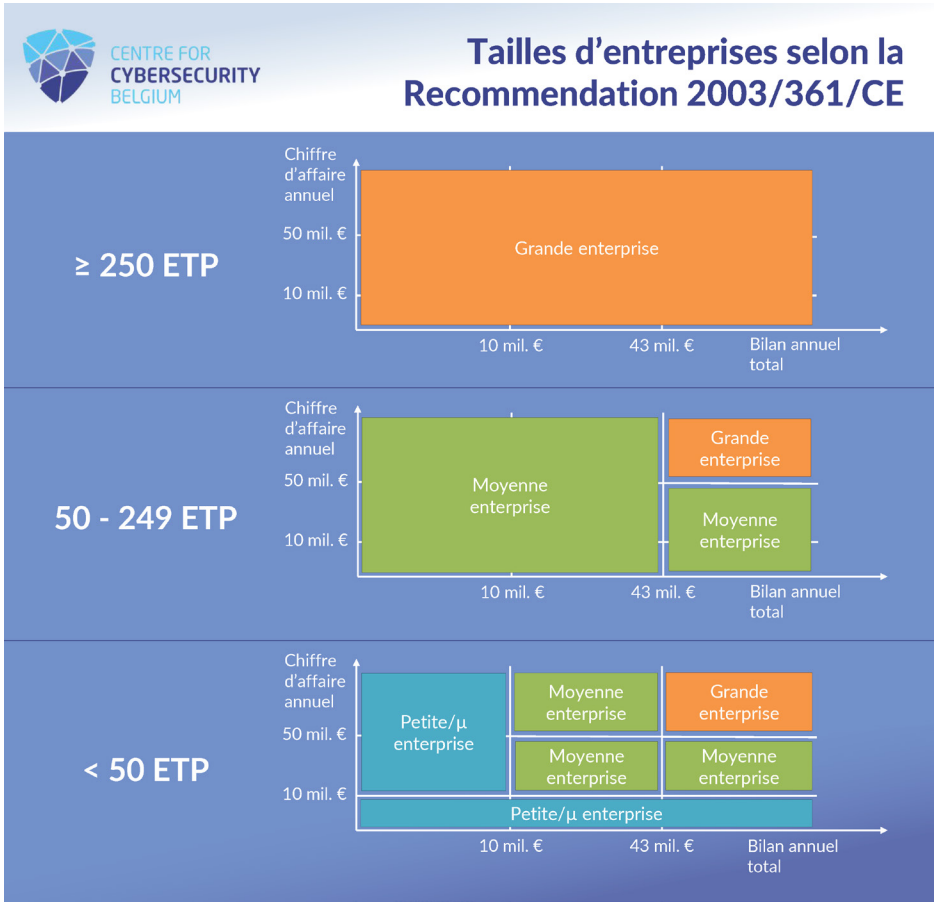
La manière dont ces deux critères sont établis est décrite dans l'annexe de la recommandation ou dans le guide de la Commission intitulé « Guide de l'utilisateur pour la définition des PME »[6]. Toutefois, il est important de préciser que l'entreprise peut choisir de se conformer soit au seuil du chiffre d'affaires, soit au seuil du bilan. Elle peut en effet dépasser l'un des plafonds financiers sans pour autant perdre son statut de PME. Nous ne prenons donc en compte que le plus faible des deux montants.

Le diagramme sur la page suivante représente visuellement les différentes tailles d'entreprises.

[4] Les équivalents temps plein (ETP) (appelés « unités de travail par année » (UTA) dans la recommandation) représentent le nombre de personnes ayant travaillé à temps plein dans l'entreprise en question ou pour son compte pendant toute l'année de référence considérée. Le travail des personnes qui n'ont pas travaillé toute l'année, des personnes qui ont travaillé à temps partiel, quelle qu'en soit la durée, ou le travail saisonnier sont comptés comme des fractions d'UTA. La recommandation et le guide précisent quels membres du personnel doivent être comptabilisés.

[5] Voir p. 7-8.

[6] https://op.europa.eu/fr/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1



La recommandation indique par ailleurs que le calcul de la taille d'une organisation qui fait partie d'un groupe (entreprises « partenaires » ou « liées ») implique une consolidation des données des différentes composantes de ce groupe. Pour plus d'informations, nous vous invitons à consulter le guide de l'utilisateur de la Commission mentionné plus haut ou son outil en ligne « SME Wizard »[7] .

Il existe cependant deux spécificités importantes quant à l'application de la recommandation dans le contexte de la loi NIS2 :

1) la consolidation des données des différentes composantes au sein d'un groupe peut être écartée, dans certaines circonstances, lorsqu'il existe une indépendance des réseaux et systèmes d'information de l'organisation concernée par rapport à ceux des entreprises liées ou partenaires ;

2) l'effectif et les montants financiers d'un organisme public qui contrôle une organisation concernée ne doivent pas être pris en compte pour déterminer la taille de cette dernière.

Si nous combinons les différentes tailles possibles avec le critère de service, nous obtenons le champ d'application suivant (avec quelques exceptions[8]) :

	Moyenne entreprise	**Grande entreprise**
Services de l'annexe I	Entité NIS2 importante	Entité NIS2 essentielle
Services de l'annexe II	Entité NIS2 importante	Entité NIS2 importante

Il existe néanmoins un certain nombre d'exceptions à ce critère de taille. Certains types d'entités font en effet partie du champ d'application de la loi NIS2, peu importe leur taille :

- les prestataires de services de confiance qualifiés (essentiel) ;

[7] https://ec.europa.eu/growth/tools-databases/SME-Wizard/

[8] Voir la liste en dessous du tableau.

- les prestataires de services de confiance non qualifiés (important s'il s'agit d'une micro, petite ou moyenne entreprise et essentiel s'il s'agit d'une grande entreprise) ;
- les fournisseurs de services DNS (essentiel) ;
- les registres de noms de domaine de premier niveau (TLD, « top-level-domain ») (essentiel) ;
- les entités fournissant un service d'enregistrement de noms de domaine (uniquement pour l'obligation d'enregistrement) ;
- les fournisseurs de réseaux de communications électroniques publics (essentiel) ;
- les fournisseurs de services de communications électroniques accessibles au public (essentiel) ;
- les entités recensées en tant qu'exploitants d'un infrastructures critiques en vertu de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (essentiel) ;
- les entités de l'administration publique qui dépendent de l'État fédéral (essentiel).

Indépendamment de ces règles, l'autorité nationale de cybersécurité (le CCB) peut également identifier spécifiquement des entités comme « essentielles » ou « importantes », par exemple lorsqu'elles sont le seul fournisseur d'un service ou lorsque l'interruption du service fourni pourrait avoir un impact significatif sur la sécurité publique, la sûreté publique ou la santé publique.

B. SERVICE FOURNI

La condition relative aux services exige d'une organisation qu'elle procède à une analyse complète de chacun des services qu'elle fournit à des tiers, par secteur et sous-secteur. Il s'agit d'un point important, étant donné que même le service fourni le plus accessoire peut faire en sorte que l'organisation dans son ensemble relève du champ d'application de la loi NIS2, sauf indication contraire dans la définition du service en question. Tous les services relevant de la loi NIS2 sont détaillés dans les annexes I et II (ou dans les définitions[9]) de la loi et regroupés par secteurs :

Secteurs hautement critiques (annexe I)	Autres secteurs critiques (annexe II)
1. Énergie a. Électricité b. Réseaux de chaleur et de froid c. Pétrole d. Gaz e. Hydrogène 2. Transports a. Transports aériens b. Transports ferroviaires c. Transports par eau d. Transports routiers 3. Secteur bancaire 4. Infrastructures des marchés financiers 5. Santé 6. Eau potable 7. Eaux usées 8. Infrastructure numérique 9. Gestion des services ICT (interentreprises) 10. Administration publique 11. Espace	1. Services postaux et d'expédition 2. Gestion des déchets 3. Fabrication, production et distribution de produits chimiques 4. Production, transformation et distribution des denrées alimentaires 5. Fabrication a. Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro b. Fabrication de produits informatiques, électroniques et optiques c. Fabrication d'équipements électriques d. Fabrication de machines et d'équipements n.c.a. e. Construction de véhicules automobiles, remorques et semi-remorques f. Fabrication d'autres matériels de transport 6. Fournisseurs numériques 7. Recherche

Il est très important de **consulter les définitions de ces services** pour vérifier si elles correspondent au service réellement fourni par une organisation.

Pour un meilleur aperçu du champ d'application de la loi, nous vous invitons à consulter notre résumé visuel du champ d'application sur les pages 23 et 24.

[9] Voir article 8 de la loi NIS2.

C. ÉTABLISSEMENT

En principe, la loi NIS2 belge s'applique uniquement aux entités établies en Belgique qui fournissent leurs services ou exercent leurs activités au sein de l'UE. La notion d'« établissement » suppose simplement l'exercice effectif d'une activité au moyen d'une installation stable, indépendamment de la forme juridique retenue, qu'il s'agisse du siège social, d'une simple succursale ou d'une filiale ayant la personnalité juridique.

Il existe toutefois trois exceptions à la règle d'établissement en Belgique :

1) La loi belge s'applique aux fournisseurs de réseaux de communications électroniques publics et fournisseurs de services de communications électroniques accessibles au public quand ils fournissent leur service en Belgique ;

2) La loi belge s'applique aux fournisseurs de services DNS, registres de noms de domaine de premier niveau, entités fournissant des services d'enregistrement de noms de domaine, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données, fournisseurs de réseaux de diffusion de contenu, fournisseurs de services gérés, fournisseurs de services de sécurité gérés, ainsi qu'aux fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux, lorsqu'ils ont leur établissement principal en Belgique ou leur représentant pour l'Union européenne en Belgique ;

3) La loi belge s'applique à toutes les entités de l'administration publique qui ont été créés par la Belgique.

En dehors de ces exceptions, si une entité possède plusieurs établissements dans différents États membres de l'UE, elle sera soumise aux lois de transposition de chaque État membre concerné. Les différentes autorités nationales compétentes collaboreront en ce qui concerne les inspections et la notification des incidents significatifs.

D. IDENTIFICATION ET CHAÎNE D'APPROVISIONNEMENT

Il est possible, après une analyse approfondie du champ d'application de la loi NIS2, que certaines organisations réalisent qu'elles ne relèvent pas de cette loi. Toutes les organisations ne relevant pas de NIS2 doivent savoir que la loi NIS2 peut malgré tout les affecter de deux manières.

Premièrement, l'autorité nationale de cybersécurité (le CCB) peut identifier certaines organisations, quelle que soit leur taille, comme des entités essentielles ou importantes en vertu de la loi NIS2 dans quatre cas de figure, liés au caractère critique de l'organisation. Ce processus se déroule en concertation avec l'entité concernée et d'autres autorités, comme prévu à l'article 11 de la loi NIS2.

Deuxièmement, une organisation peut faire partie de la chaîne d'approvisionnement directe d'une entité NIS2 et être confrontée à l'obligation de mettre en œuvre des mesures de gestion des risques en matière de cybersécurité, par exemple en raison d'une exigence contractuelle de ladite entité NIS2. Dans ce contexte, le CCB conseille à toutes les organisations susceptibles de se trouver dans la chaîne d'approvisionnement d'une entité NIS2 de se conformer au moins aux mesures énoncées dans le niveau Basic du Cyberfundamentals (CyFun®) Framework[10] .

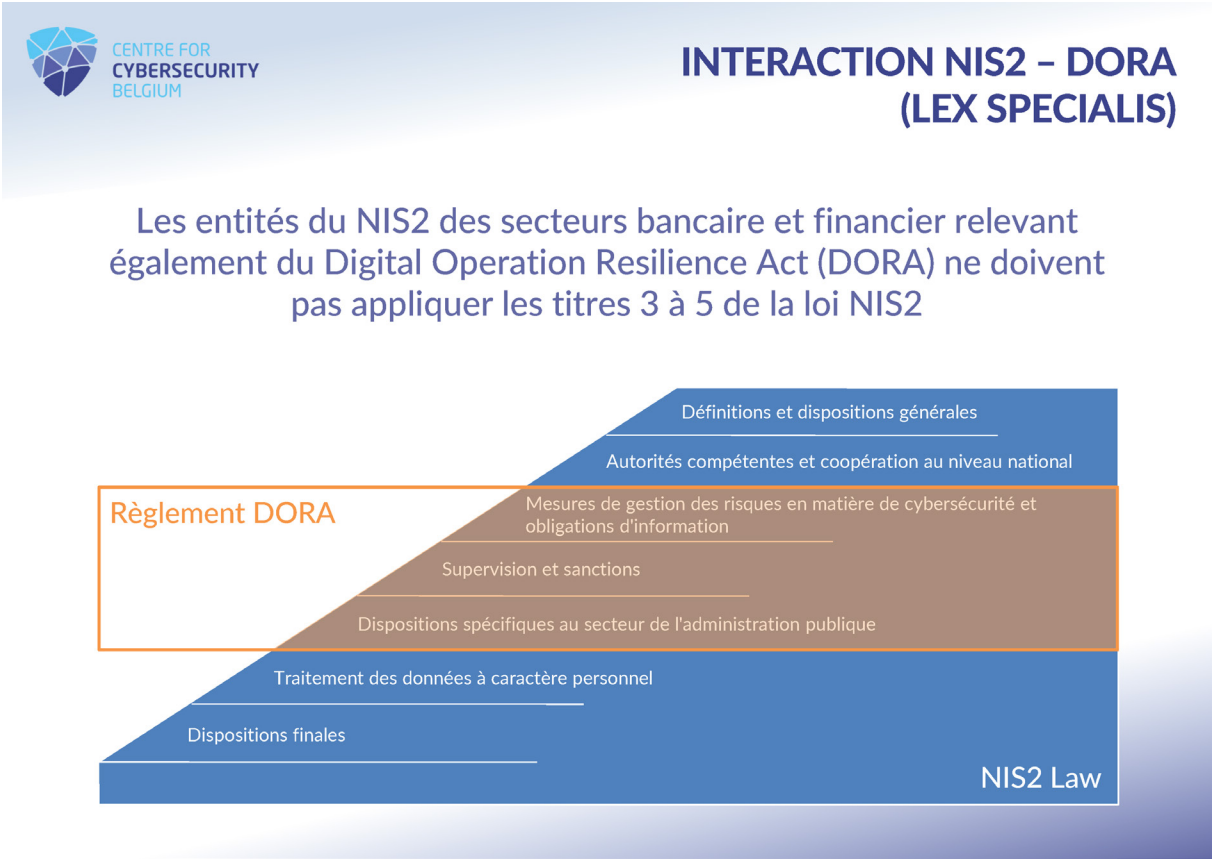
E. INTERACTION ENTRE NIS2 ET DORA

La loi NIS2 prévoit que les titres 3 à 5 de la loi (mesures de gestion des risques en matière de cybersécurité, supervision et sanctions, dispositions spécifiques aux secteurs de l'administration publique) ne s'appliquent pas aux entités du secteur bancaire et du secteur des marchés financiers qui entrent dans le champ d'application de DORA. Ce dernier est l'abréviation du règlement UE 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, qui définit les exigences en matière de sécurité des réseaux et des systèmes d'information des entités financières entrant dans son champ d'application.

Cela découle de la directive NIS2, et plus précisément de l'exclusion des actes juridiques sectoriels de l'Union (appelés *lex specialis*), lorsque ces actes exigent des entités NIS2 qu'elles adoptent des mesures de gestion des risques en matière de cybersécurité ou qu'elles notifient les incidents significatifs et que ces exigences sont au moins équivalentes aux obligations prévues par la directive NIS2.

[10] https://cyfun.be

En pratique, toutes les entités NIS2 couvertes par le règlement DORA peuvent se limiter au respect de ce règlement en ce qui concerne les obligations contenues aux titres 3 à 5 de la loi NIS2. Cela comprend les mesures de gestion des risques en matière de cybersécurité, la notification obligatoire et volontaire des incidents, la supervision, les mesures et amendes administratives. Cependant, toutes les autres dispositions de la loi NIS2, telles que celles relatives à l'enregistrement et à la compétence du CCB, s'appliquent toujours à ces entités.



III. Obligations

A. ENREGISTREMENT

Les entités NIS2 qui relèvent du champ d'application de la loi NIS2 belge doivent s'enregistrer auprès du CCB. Dans la pratique, cet enregistrement se fait au moyen d'un formulaire en ligne, à compléter sur Safeonweb@Work[11].

Le délai d'enregistrement dépend du type d'entité. En principe, les entités essentielles et importantes, ainsi que les fournisseurs de services d'enregistrement de noms de domaine, disposent de **cinq mois à** compter de l'entrée en vigueur de la loi pour s'enregistrer, c'est-à-dire au plus tard le **18 mars 2025[12].**

Il existe un régime légèrement adapté pour les types d'entités suivants des secteurs numériques :

- les fournisseurs de services DNS ;
- les registres des noms de domaines de premier niveau (TLD) ;
- les entités fournissant des services d'enregistrement de noms de domaine ;
- les fournisseurs de services d'informatique cloud ;
- les fournisseurs de services de centres de données ;
- les fournisseurs de réseaux de diffusion de contenu ;
- les fournisseurs de services gérés ;
- les fournisseurs de services de sécurité gérés ;
- les fournisseurs de places de marché en ligne ;
- les fournisseurs de moteurs de recherche en ligne ;
- les fournisseurs de plateformes de services de réseaux sociaux.

Ces entités doivent s'enregistrer avec des informations différentes dans les **deux mois** qui suivent l'entrée en vigueur de la loi, c'est-à-dire au plus tard le **18 décembre 2024[13]**.

Toute modification des informations pertinentes d'une entité doit être immédiatement notifiée au CCB (au plus tard dans les deux semaines).

B. MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSÉCURITÉ

Les mesures de gestion des risques en matière de cybersécurité sont des mesures d'ordre technique, opérationnel ou organisationnel qui permettent à l'entité concernée de gérer les risques liés à la sécurité de son réseau et de ses systèmes d'information, tout en éliminant ou en minimisant l'impact des cyberincidents. Les mesures doivent être adoptées en tenant compte de de l'état des connaissances, du coût des mesures, ainsi que des normes applicables.

Pour chaque entité, les mesures de gestion des risques en matière de cybersécurité doivent être appropriées et proportionnées aux risques encourus, à son degré d'exposition aux risques, à sa taille, à la probabilité que des incidents se produisent et à leur gravité.

La loi NIS2 énumère 11 mesures minimales que chaque entité doit mettre en œuvre[14]. Une vue d'ensemble peut être trouvée dans le diagramme sur la page suivante.

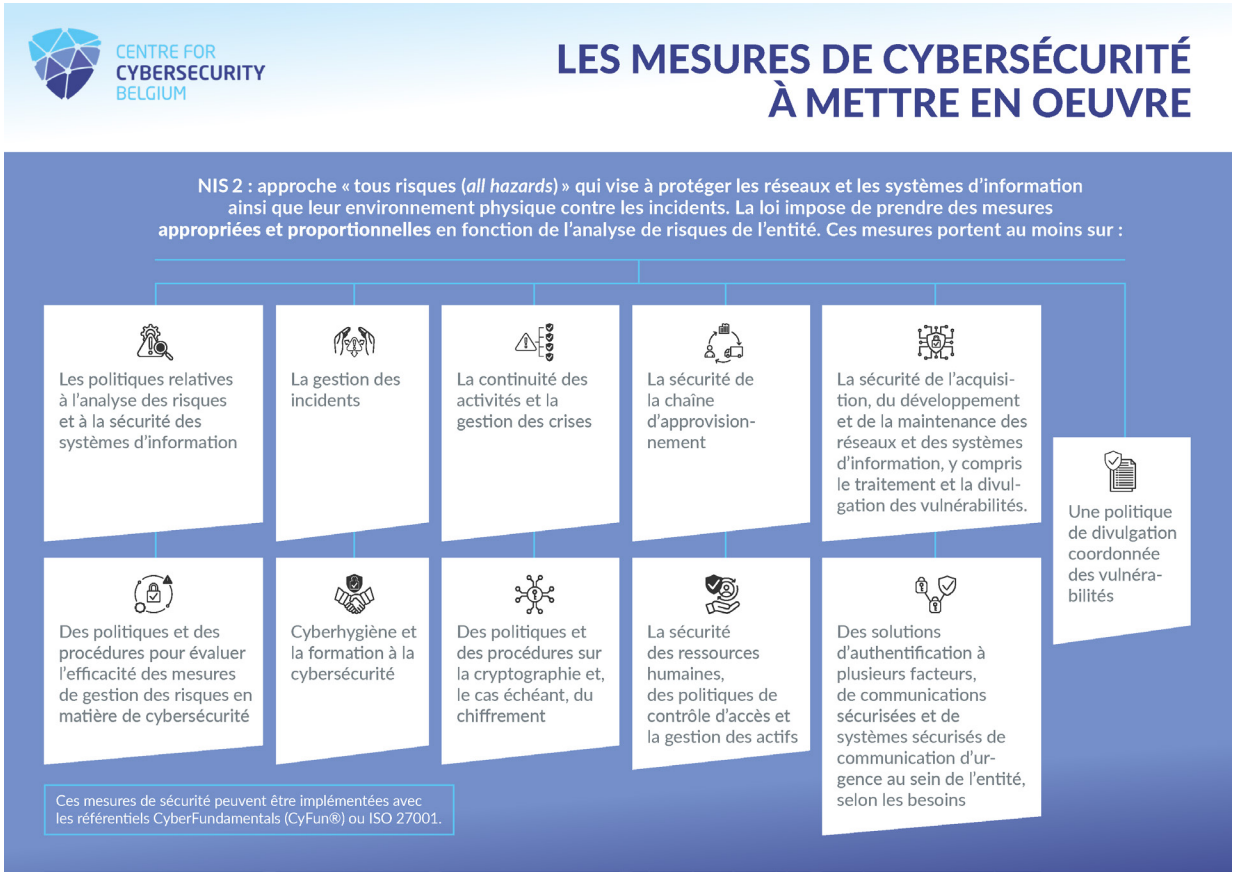
---

[11] https://atwork.safeonweb.be/fr/register-my-organisation

[12] Les informations à fournir dans le cadre du délai d'enregistrement par défaut peuvent être retrouvées à l'article 13, §1 de la loi NIS2.

[13] Les informations à fournir dans le cadre du régime adapté peuvent être retrouvées à l'article 14, §1 de la loi NIS2.

[14] Voir également l'acte d'exécution de la Commission : https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks



Le CCB a créé un référentiel gratuit et publiquement accessible appelé le « CyberFundamentals (CyFun®) Framework », qui couvre chacun de ces points. À l'aide de ce référentiel, les entités NIS2 peuvent se conformer à l'obligation de prendre des mesures appropriées et proportionnées de gestion des risques en matière de cybersécurité[15].

C. SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

La loi NIS2 impose à toutes les entités tombant dans son champ d'application de prendre des mesures appropriées et proportionnées de gestion des risques en matière de cybersécurité. L'une de ces mesures spécifiques est la *« **sécurité de la chaîne d'approvisionnement**, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs directs ou prestataires de services directs ».*

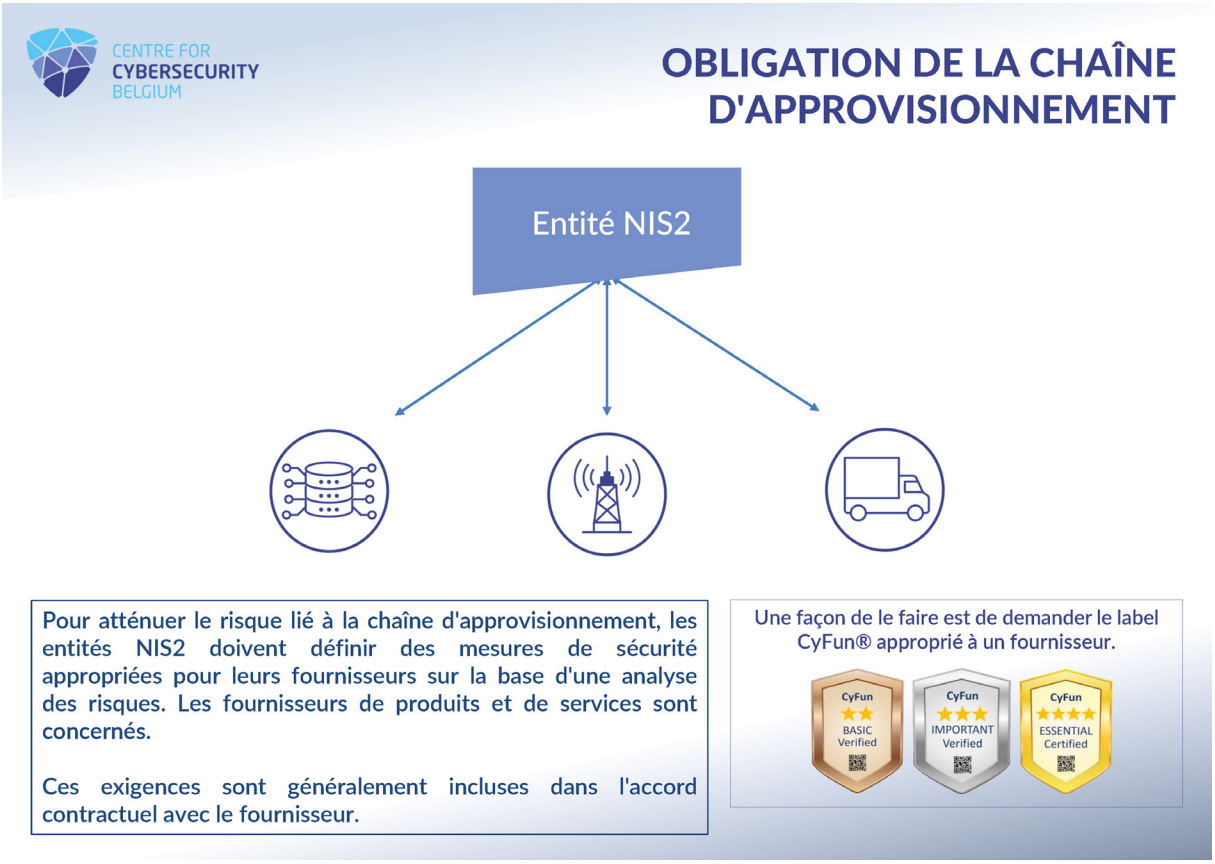
L'impact de cette obligation peut être envisagé sous deux angles : cela implique non seulement que les entités NIS2 doivent imposer des mesures de gestion des risques de cybersécurité aux organisations dans leur(s) chaîne(s) d'approvisionnement (telles que les fournisseurs et prestataires) et pouvoir les contrôler, mais aussi que les entités qui ne relèvent pas du champ d'application de NIS2 seront également tenues de prendre des mesures appropriées et proportionnées de gestion des risques de cybersécurité.

La loi NIS2 ne précise pas comment les entités NIS2 doivent gérer l'obligation de la chaîne d'approvisionnement directe. En particulier, elle laisse aux entités le soin de vérifier si les organisations dans la chaîne d'approvisionnement respectent leurs obligations. Le CCB recommande à toutes les entités NIS2 d'imposer contractuellement un label ou une certification aux organisations dans leur chaîne d'approvisionnement, tels que ceux inclus dans le CyberFundamentals (CyFun®) Framework, afin de faciliter la preuve du respect de l'obligation de la chaîne d'approvisionnement.

Pour toutes les entités qui ne relèvent pas du champ d'application de la loi NIS2, le CCB recommande qu'elles prennent également des mesures appropriées et proportionnées de gestion des risques en matière de cybersécurité et ce, afin de se préparer à l'éventualité qu'elles se voient intégrées dans la chaîne

[15] Pour plus d'informations, voir chapitre IV, section B.

d'approvisionnement d'une entité NIS2. Ici aussi, elles peuvent avoir recours au CyFun® Framework pour identifier et mettre en œuvre les mesures concrètes qu'elles pourraient être amenées à prendre.



D. NOTIFICATION D'INCIDENTS (VOIR GUIDE)

La loi NIS2 impose également à toutes les entités NIS2 de notifier au CCB tout incident pouvant être considéré comme « significatif ». Voici comment la loi définit ce type d'incident :

« Tout incident ayant un impact significatif sur la fourniture de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la loi et qui :

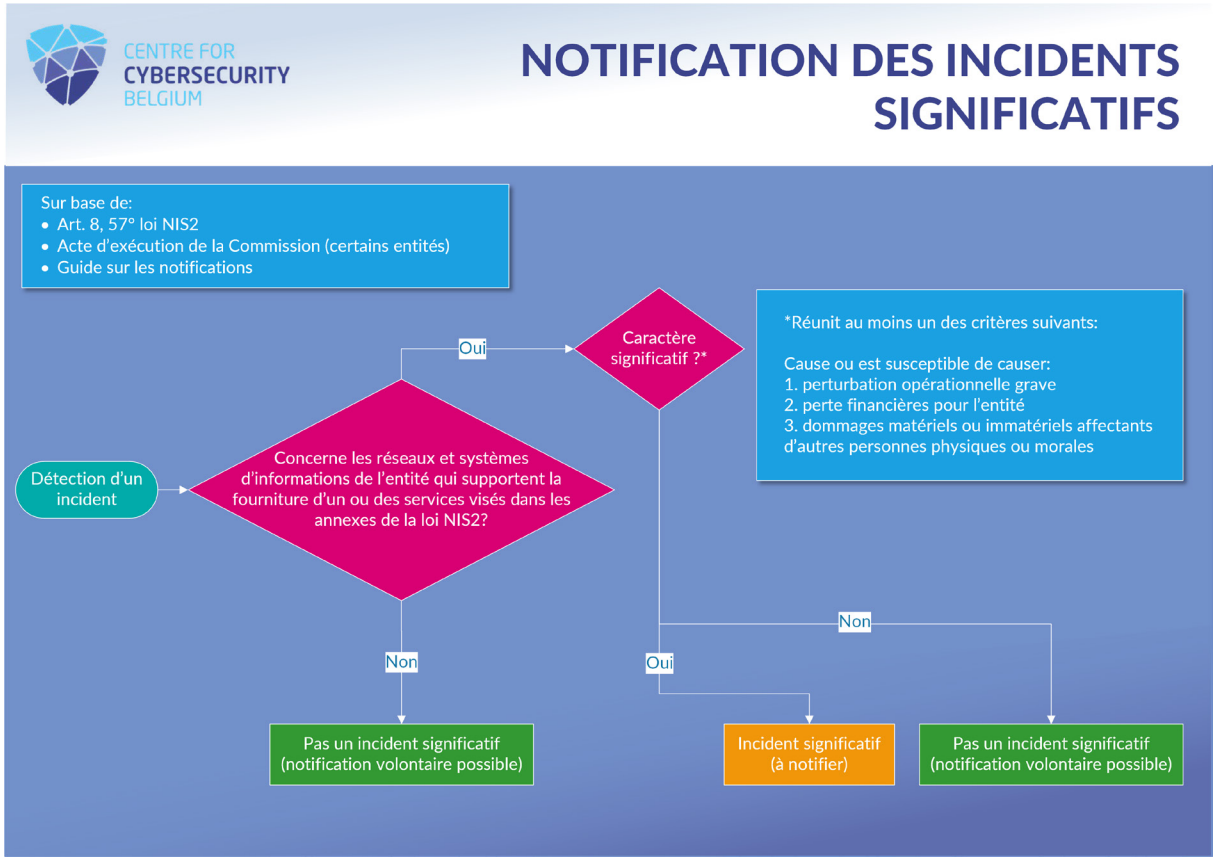
1° a causé ou est susceptible de causer une perturbation opérationnelle grave de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II ou des pertes financières pour l'entité concernée ; ou
2° a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables. ».

L'incident doit avoir un impact sur la fourniture de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la loi, c'est-à-dire qu'il **doit affecter les réseaux et systèmes d'information qui supportent la fourniture de l'un ou de plusieurs de ces services** (par exemple, la distribution d'électricité).

Les notifications obligatoires ne concernent donc que les systèmes d'information et réseaux dont l'entité concernée est tributaire pour fournir le ou les services repris dans les annexes de la loi. Un incident affectant un système d'information isolé et sans lien avec la fourniture des services précités ne doit donc pas obligatoirement être notifié.

Ensuite, cet impact doit être significatif, à savoir causer ou susceptible de causer au moins l'une de ces trois situations :

- une **perturbation opérationnelle grave de l'un des services fournis** (dans les secteurs ou sous-secteurs repris à l'annexe I et II de la loi NIS2) ;
- des **pertes financières pour l'entité concernée** ;
- des **dommages matériels, corporels ou moraux considérables à d'autres personnes physiques ou morales**.



Dès qu'une entité NIS2 fait face à un tel incident, elle doit le notifier au CCB. Cette notification se décline en plusieurs étapes (voir également le visuel ci-dessous) :

1) **sans retard injustifié et, en tout état de cause, dans les 24 heures** après avoir eu connaissance de l'incident significatif, l'entité soumet une alerte précoce ;
2) **sans retard injustifié et, en tout état de cause, dans les 72 heures (24 heures pour les prestataires de services de confiance) après avoir eu connaissance de l'incident significatif**, l'entité soumet une notification d'incident ;
3) à la demande du CSIRT national ou, le cas échéant, de l'autorité sectorielle compétente, l'entité présente un rapport intermédiaire ;
4) **au plus tard un mois après la notification de l'incident visée au point 2**, l'entité présente un rapport final ;
5) en cas d'incident en cours au moment de la présentation du rapport final, l'entité concernée présente un rapport d'avancement puis, dans le mois qui suit le traitement de l'incident, un rapport final.

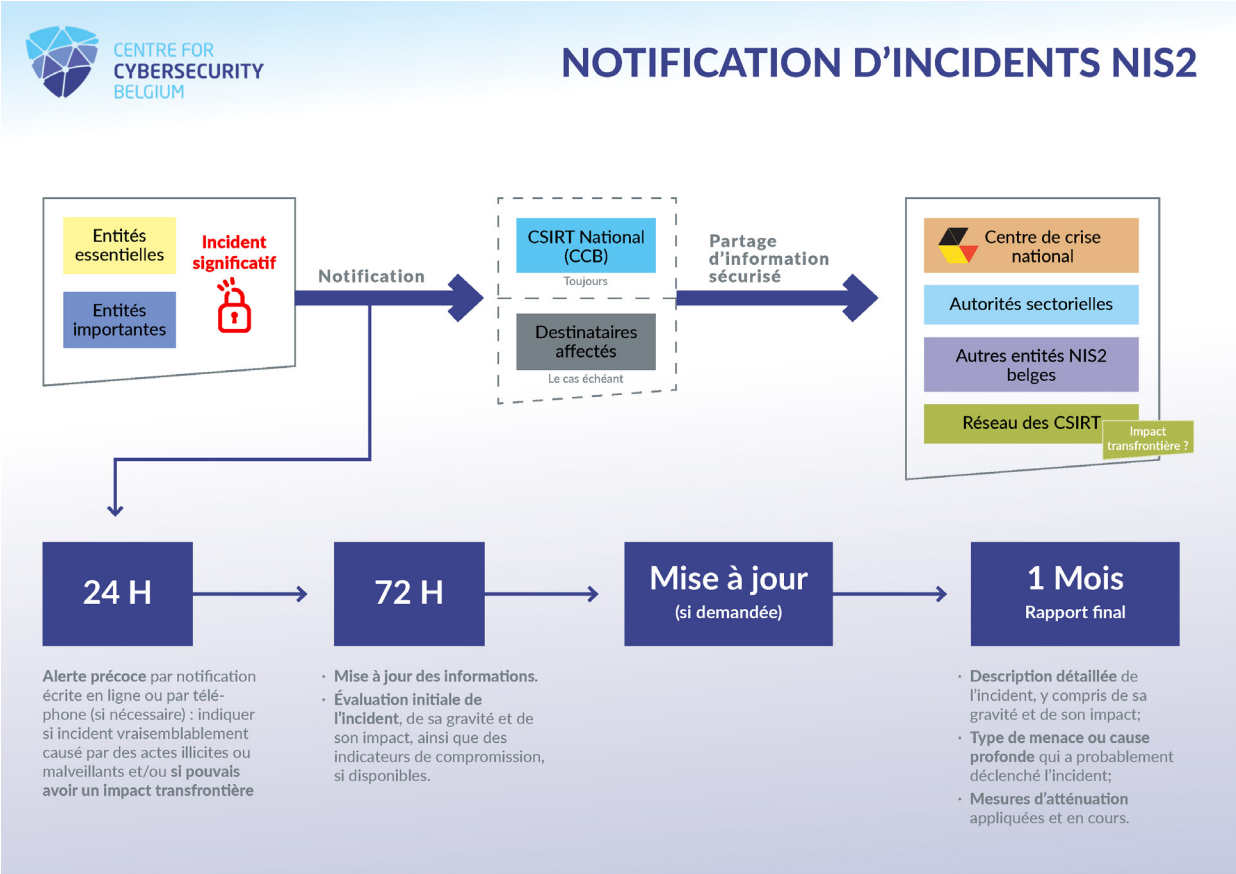
En fonction de l'ampleur de l'incident, l'entité doit également informer les destinataires de son service de l'existence de l'incident et des mesures et corrections que les destinataires peuvent prendre pour y répondre. Le CCB peut partager les informations reçues par l'entité avec d'autres autorités dans la limite de ce qui est nécessaire.

Plus d'informations sur la notification des incidents sont disponibles dans notre **guide de notification des incidents NIS2**[16].

Les incidents NIS2 peuvent être signalés via notre formulaire web de notification d'incident : **https://notif.safeonweb.be/fr**.

[16] https://ccb.belgium.be/fr/cert/signaler-un-incident

Voir également l'acte d'exécution de la Commission : https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks



E. OBLIGATIONS DU MANAGEMENT

La loi NIS2 prévoit plusieurs éléments relatifs au management des entités NIS2 :

1) les organes de direction doivent approuver les mesures de gestion des risques en matière de cybersécurité et superviser leur mise en œuvre ;
2) les membres des organes de direction doivent suivre une formation pour que leurs connaissances et compétences soient suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité ;
3) les organes de direction sont responsables des décisions prises en matière de gestion des risques de cybersécurité, en ce compris la gestion des incidents ;

Ces mesures visent à convaincre la direction de l'importance de la cybersécurité.

L'exposé des motifs de la loi NIS2 définit la notion de « membre d'un organe de direction » comme :

> *Toute personne physique ou morale qui :*
>
> *(i) exerce une fonction au sein d'une entité ou en relation avec celle-ci l'autorisant (a) à administrer et à représenter l'entité en question ou (b) à prendre des décisions au nom et pour le compte de l'entité qui sont juridiquement liantes pour celle-ci ou à participer, au sein d'un organe de l'entité, à la prise de telles décisions, ou*
>
> *(ii) exerce un contrôle de l'entité en question, soit le pouvoir de droit ou de fait d'exercer une influence décisive sur la désignation de la majorité des administrateurs ou gérants de celle-ci ou sur l'orientation de sa gestion.*
>
> *Lorsque l'entité en question est une société de droit belge, un tel contrôle est déterminé conformément aux articles 1:14 à 1:18 du Code des sociétés et des associations.*

Lorsque la personne dont le rôle est examiné est une personne morale, la notion de « membre d'un organe de direction » est examinée de façon récursive et recouvre tant la personne morale en question que tout membre d'un organe de direction de ladite personne morale.

Ces règles de responsabilité sont sans préjudice des règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

Il convient de noter que les personnes physiques exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans une entité NIS2 peuvent se voir interdire temporairement l'exercice de responsabilités dirigeantes dans cette entité, en cas de manquements aux exigences de la loi NIS2.

IV. Supervision

A. RÉGIME GÉNÉRAL

En matière de contrôle, la loi fait une différence entre les entités importantes et les entités essentielles :

- les entités importantes font l'objet d'une supervision « *ex-post* », c'est-à-dire après un incident ou lorsque l'autorité de supervision dispose de suffisamment d'éléments indiquant qu'une entité importante ne respecte pas les obligations de la loi ;
- les entités essentielles font l'objet d'une supervision « *ex-post* » mais aussi « *ex-ante* », c'est-à-dire qu'elles doivent, à tout moment être en mesure de prouver qu'elles respectent la loi. À cet effet, la loi soumet les entités essentielles à une évaluation périodique de conformité obligatoire.

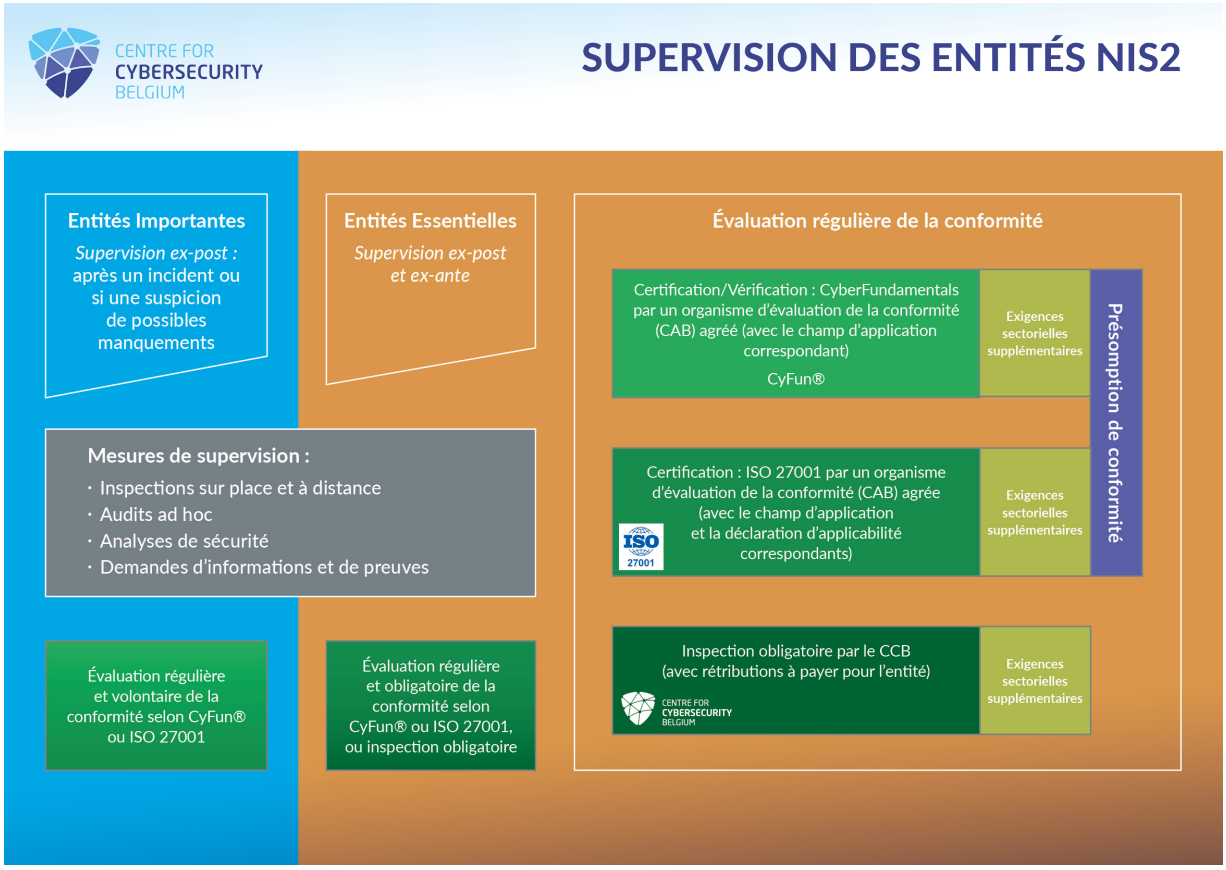
Cette évaluation périodique et obligatoire de la conformité peut être accomplie de trois manières différentes :

1) une certification (niveau Essential) ou une vérification (niveau Important ou Basic) de l'entité en vertu du **CyberFundamentals (CyFun®) Framework** par un organisme d'évaluation de la conformité (OEC/CAB) accrédité par BELAC et agréé par le CCB, avec le champ d'application correspondant ;
2) une certification de l'entité selon la **norme ISO/IEC 27001** délivrée par un CAB accrédité avec le champ d'application et le *statement of applicability* pertinents. Pour la norme ISO/IEC 27001, le CAB doit être accrédité par un organisme d'accréditation qui a signé le *Multi-Lateral Agreement* (MLA) dont relève la norme ISO/IEC 27001 dans le cadre de la Coopération européenne pour l'accréditation (EA) ou du Forum international de l'accréditation (IAF), et également être agréé par le CCB ;
3) une **inspection** par le service d'inspection du CCB (une rétribution est demandée pour ce service).

À ces trois possibilités, une autorité sectorielle peut ajouter des exigences supplémentaires que les entités relevant de son secteur doivent respecter. De plus, les entités qui choisissent d'effectuer leur évaluation périodique de conformité par le biais de CyFun® ou d'ISO/IEC 27001 peuvent bénéficier d'une présomption de conformité.

Au cours de sa supervision, le service d'inspection peut avoir recours à des inspections sur place et des contrôles à distance, à des audits ad hoc, mais aussi à des scans de sécurité et à des demandes générales d'informations et de preuves. Toutes les entités NIS2 doivent à tout moment se conformer aux demandes formulées par le service d'inspection. Dans le cas contraire, elles s'exposent à des mesures et amendes administratives.

Les entités importantes peuvent également se soumettre volontairement à une évaluation périodique de la conformité. Dans ce cas, elles ont uniquement le choix entre CyFun® et ISO/IEC 27001.



B. LES CYBERFUNDAMENTALS (CYFUN®)

Le CyberFundamentals (CyFun®) Framework[17] compile une série de mesures concrètes visant à :

- protéger les données ;
- réduire considérablement le risque des cyberattaques les plus courantes ;
- accroître la cyber-résilience d'une organisation.

Pour répondre à la gravité de la menace à laquelle une organisation est exposée, outre le niveau de départ « Small », trois niveaux d'assurance sont prévus : Basic, Important et Essential. Le référentiel a été validé à l'aide des profils d'attaque du CERT (obtenus à la suite d'attaques réussies). La conclusion est la suivante :

- les mesures du niveau d'assurance Basic permettent de couvrir 82 % des attaques ;
- les mesures du niveau d'assurance Important permettent de couvrir 94 % des attaques ;
- les mesures du niveau d'assurance Essential permettent de couvrir 100 % des attaques.

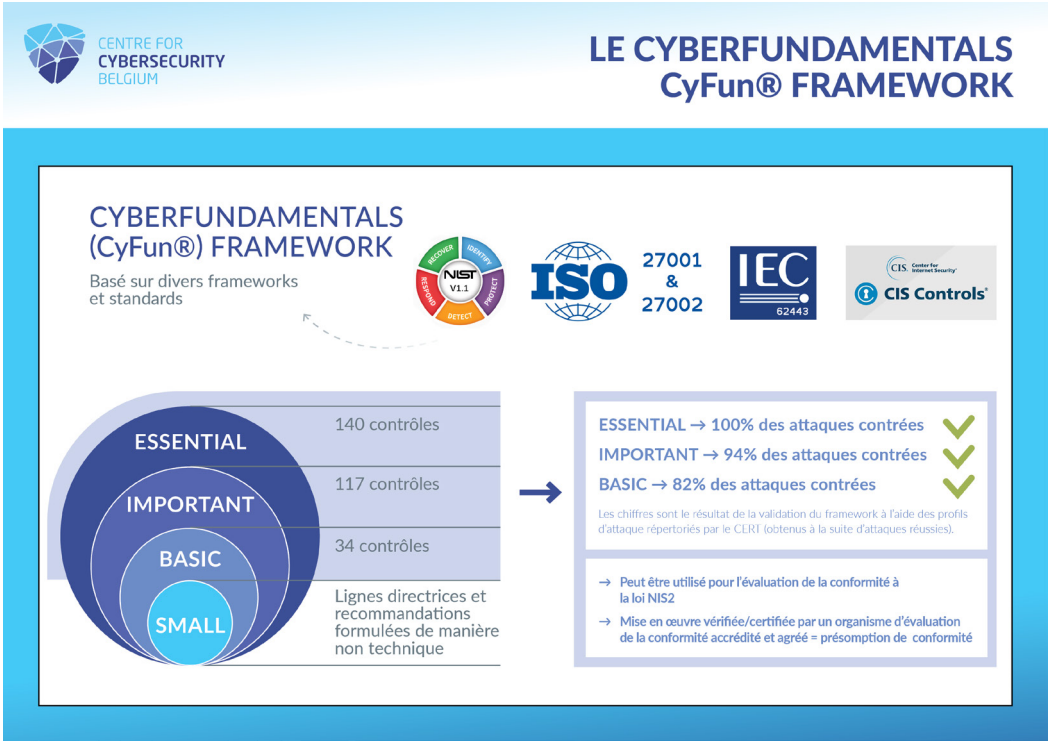
En outre, le CyFun® Framework :

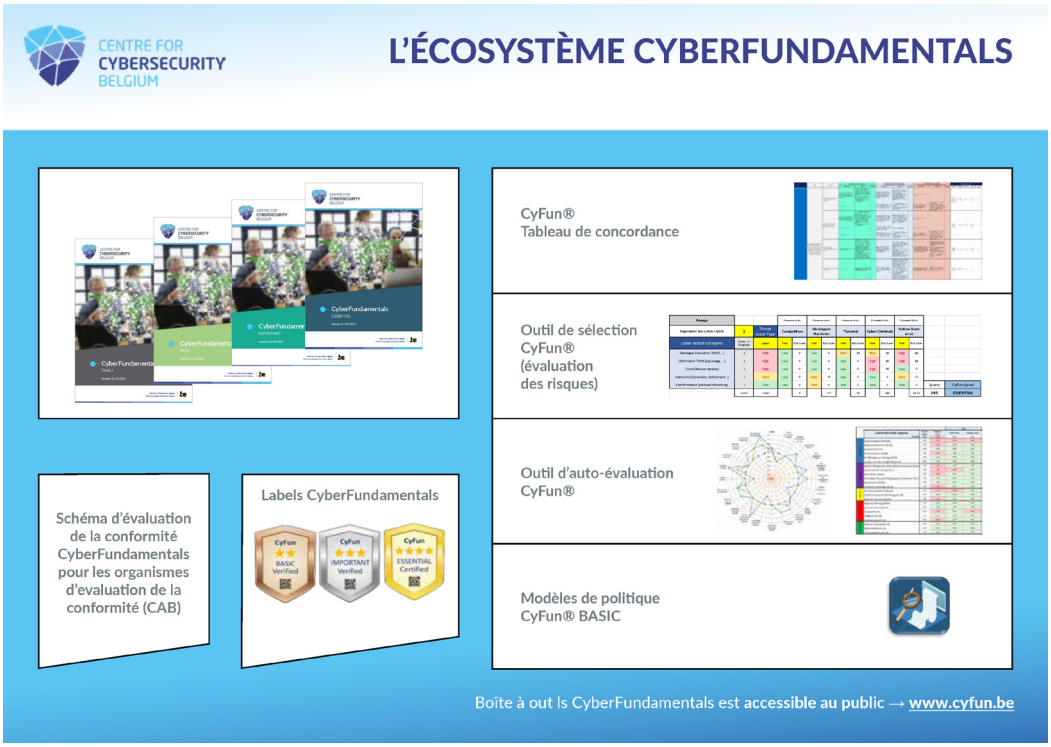
- **repose sur des normes reconnues** : CyFun® sélectionne des contrôles pertinents basés sur des normes communes telles que NIST CSF, ISO/IEC 27001, CIS Controls et IEC 62443 ;
- **correspond aux mesures nécessaires** pour prévenir les principales attaques identifiées par le CCB ;
- peut être **utilisé sans aide** : chaque contrôle est accompagné de conseils pour faciliter sa mise en œuvre. L'outil d'auto-évaluation de CyFun® permet de superviser la mise en œuvre ;
- permet de **valider votre implémentation** : vous pouvez valider votre mise en œuvre en demandant une évaluation par un organisme d'évaluation de la conformité agréé. Cette attestation fournit la preuve de votre mise en œuvre à vos clients et à vos autorités (par exemple, pour se conformer à NIS2).

Dans le contexte de NIS2, le CyFun® Framework est un outil particulièrement pratique, non seulement pour les entités essentielles soumises à une évaluation périodique de la conformité, mais aussi pour les entités importantes.

[17] https://cyfun.be

Disponible gratuitement, il offre des solutions claires pour l'évaluation des risques, l'auto-évaluation et la mise en place concrète des mesures minimales de gestion des risques en matière de cybersécurité exigées par la loi NIS2. En outre, une mise en œuvre validée ou certifiée du CyFun® Framework confère aux entités concernées une présomption de conformité dans le cadre de la supervision prévue par la loi NIS2. Le CCB recommande vivement à toutes les entités NIS2 d'utiliser le CyFun® Framework.





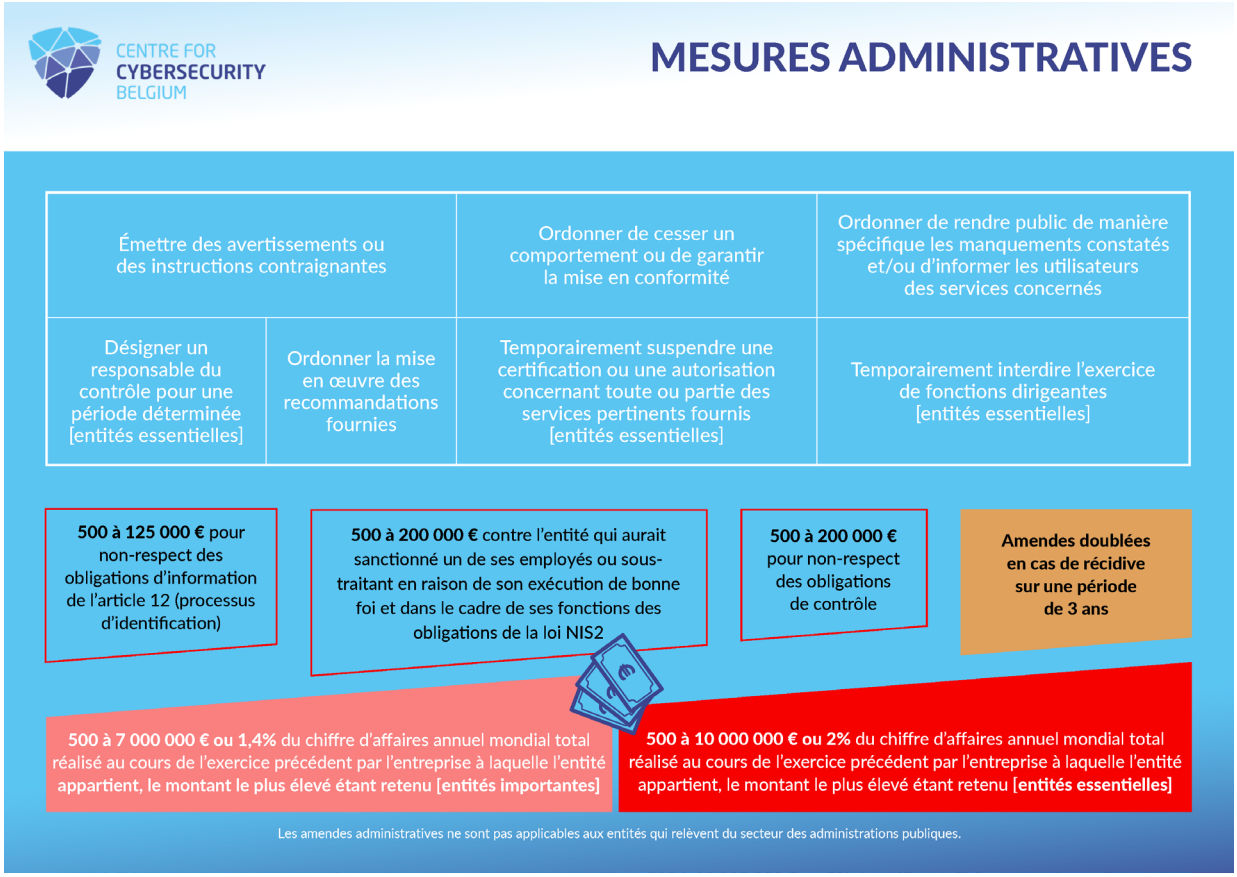
V. Sanctions

Les entités NIS2 qui ne respectent pas leurs obligations peuvent être soumises à une série de mesures et amendes administratives.

L'objectif du CCB est d'atteindre un niveau élevé de cybersécurité à travers le pays, en étroite collaboration avec toutes les entités concernées. Il existe néanmoins des situations dans lesquelles des sanctions peuvent s'avérer nécessaires. À cette fin, la loi (titre 4, chapitre 2) prévoit une procédure spécifique qui définit l'interaction entre le CCB et l'entité concernée. Cette procédure prévoit notamment l'obligation pour le CCB (ou une autorité sectorielle) d'informer l'entité de son intention d'imposer une sanction. Il va de soi que cette potentielle décision de sanction doit être suffisamment motivée. L'entité a alors la possibilité de se défendre.

Si une sanction est jugée nécessaire, le CCB doit prendre en compte un certain nombre d'éléments pour déterminer une sanction appropriée et proportionnée, par exemple la catégorie de l'entité, la gravité de l'infraction, sa durée, les infractions antérieures, les dommages, la négligence, etc.

La liste des mesures et amendes administratives possibles figure dans l'infographie ci-dessous :



VI. Ligne du temps

La plupart des dispositions du cadre légal NIS2 s'appliquent à partir du 18 octobre 2024. Toutefois, pour certaines d'entre elles, la loi ou l'arrêté royal accordent aux entités un délai supplémentaire avant leur mise en application.

À partir du 18 octobre 2024, les obligations suivantes s'appliquent notamment :

- prendre les mesures minimales de gestion des risques en matière de cybersécurité ;
- notifier tous les incidents significatifs ;
- se soumettre à la supervision des autorités compétentes et coopérer avec elles ;
- pour les organes de direction : approuver les mesures de gestion des risques en matière de cybersécurité, superviser la mise en œuvre des mesures, être responsable des manquements commis par l'entité et suivre une formation à la cybersécurité.

En ce qui concerne l'enregistrement des entités auprès du CCB sur la plateforme Safeonweb@Work, la loi prévoit des délais suivants :

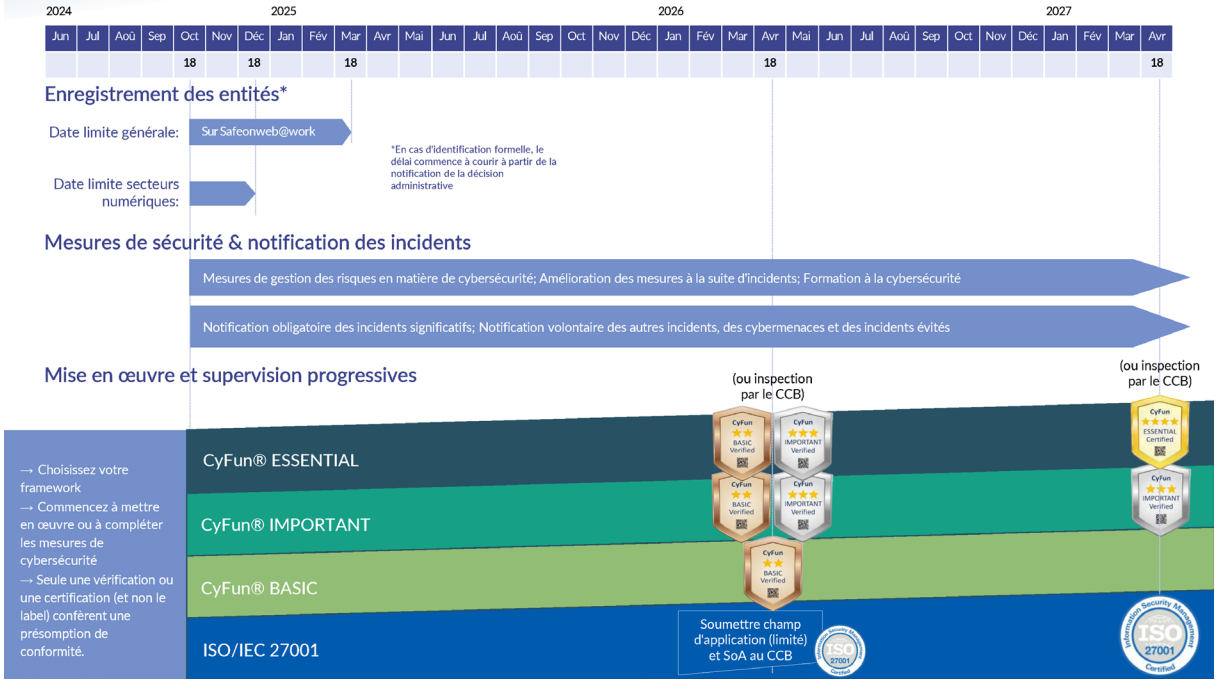
- les entités fournissant des services relevant des secteurs numériques visés dans les annexes (liste à l'art. 14, §1er, de la loi) ont deux mois à partir du 18 octobre 2024 pour s'enregistrer (**au plus tard pour le 18 décembre 2024**) ;
- toutes les autres entités disposent de cinq mois à partir du 18 octobre pour s'enregistrer (**au plus tard pour le 18 mars 2025**).

La supervision/l'évaluation périodique de la conformité des entités essentielles se fait également de manière progressive :

- pour le CyberFundamentals (CyFun®) Framework :
  - les entités qui, sur la base de leur évaluation des risques, déterminent qu'elles doivent se conformer au **niveau d'assurance Basic**, disposent d'un délai de 18 mois (**au plus tard pour le 18 avril 2026**) pendant lequel elles doivent recourir à une vérification par un organisme d'évaluation de la conformité – ci-après OEC (CAB) – accrédité et agréé ;
  - les entités qui, sur la base de leur évaluation des risques, déterminent qu'elles doivent se conformer au **niveau d'assurance Important**, disposent d'un délai de 18 mois (**au plus tard pour le 18 avril 2026**) pendant lequel elles doivent recourir à une vérification par un OEC (CAB) accrédité et agréé ;
    Au besoin, elles peuvent procéder à une première vérification au niveau Basic et à une vérification au niveau Important à l'issue d'un délai supplémentaire de 12 mois (**au plus tard pour le 18 avril 2027**) ;
  - les entités qui, sur la base de leur évaluation des risques, déterminent qu'elles doivent se conformer au **niveau d'assurance Essential**, disposent d'un délai de 18 mois (**au plus tard pour le 18 avril 2026**) pendant lequel elles doivent obtenir une vérification Basic ou Important par un OEC (CAB) accrédité et agréé.
    Elles disposent d'un délai supplémentaire de 12 mois (**au plus tard pour le 18 avril 2027**) pour obtenir une certification au niveau d'assurance Essential par OEC (CAB) accrédité et agréé.
- les entités qui choisissent d'être certifiées ISO/IEC 27001 doivent transmettre leur champ d'application et leur *statement of applicability* **au plus tard pour le 18 avril 2026** au CCB et obtenir une certification par un OEC (CAB) accrédité et agréé **au plus tard pour le 18 avril 2027**.
- les entités qui ont choisi d'être inspectées directement par le CCB :
  - **au plus tard pour le 18 avril 2026** : transmettre au CCB leur auto-évaluation de CyFun® Basic ou Important, ou transmettre au CCB leur politique de sécurité de l'information, leur champ d'application et leur *statement of applicability* ISO/IEC 27001;
  - **au plus tard pour le 18 avril 2027** : rapport sur les progrès accomplis en matière de conformité.

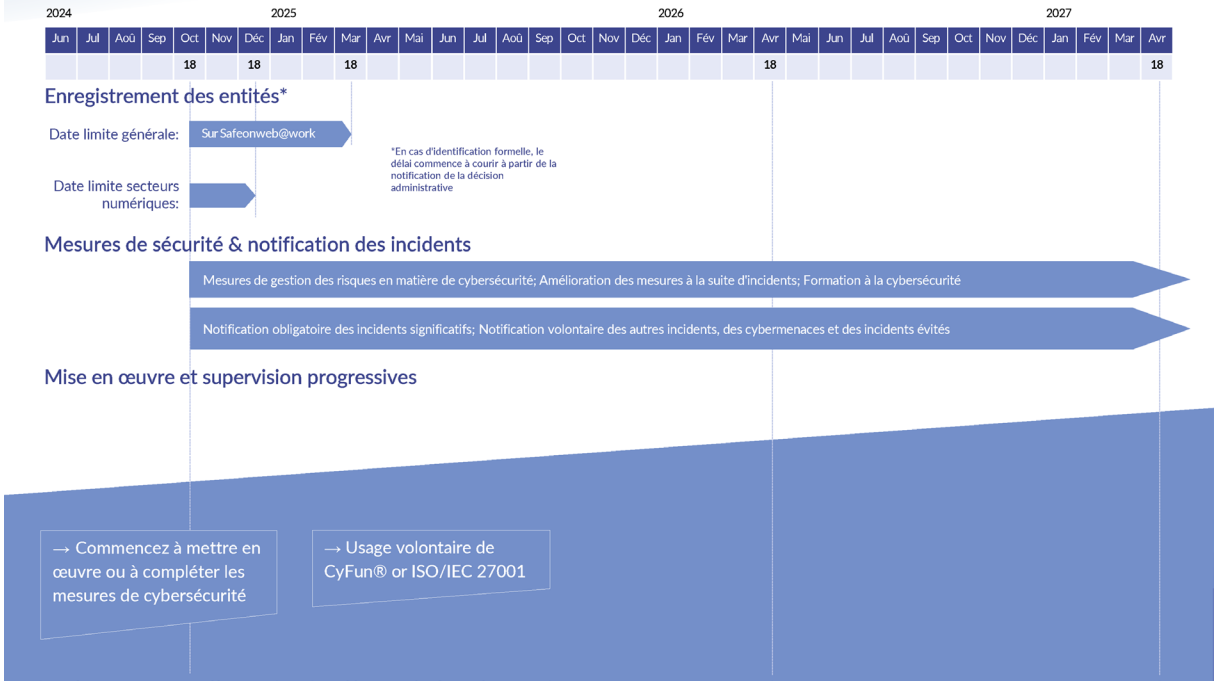
CENTRE FOR CYBERSECURITY BELGIUM

LIGNE DE TEMPS MISE EN ŒUVRE ENTITÉS ESSENTIELLES



CENTRE FOR CYBERSECURITY BELGIUM

LIGNE DE TEMPS MISE EN ŒUVRE ENTITÉS IMPORTANTES



CENTRE FOR CYBERSECURITY BELGIUM

ANNEXE I : SECTEURS HAUTEMENT CRITIQUES

SECTEUR	SOUS-SECTEUR et/ou TYPE D'ENTITÉ		GRANDES ENTREPRISES *effectif d'au moins 250 ETP, ou chiffre d'affaires annuel > € 50 M et bilan annuel total > € 43 M*	MOYENNES ENTREPRISES *effectif d'au moins 50 ETP, ou > € 10 M de chiffre d'affaires annuel / bilan annuel total*	PETITES & MICRO ENTREPRISES
1. Énergie	Électricité	Entreprises d'électricité ; Gestionnaires de réseau de distribution ; Gestionnaires de réseau de transport ; Producteurs ; Opérateurs désignés du marché de l'électricité ; Acteurs du marché ; Exploitants d'un point de recharge	Essentiel	Important*	Seulement si identifié*
	Réseaux de chaleur et de froid	Opérateurs de réseaux de chaleur ou de réseaux de froid			
	Pétrole	Exploitants d'oléoducs ; Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole ; Entités centrales de stockage			
	Gaz	Entreprises de fourniture ; Gestionnaires de réseau de distribution ; Gestionnaires de réseau de transport ; Gestionnaires d'installation de stockage ; Gestionnaires d'installation de GNL ; Entreprises de gaz naturel ; Exploitants d'installations de raffinage et de traitement de gaz naturel			
	Hydrogène	Exploitants de systèmes de production, de stockage et de transport d'hydrogène			
2. Transports	Transports aériens	Transporteurs aériens utilisés à des fins commerciales ; Entités gestionnaires d'aéroports, aéroports, et entités exploitant les installations annexes se trouvant dans les aéroports ; Services du contrôle de la circulation aérienne			
	Transports ferroviaires	Gestionnaires de l'infrastructure ; Entreprises ferroviaires			
	Transports par eau	Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret ; Entités gestionnaires des ports et les entités exploitant des infrastructures et des équipements à l'intérieur des ports ; Exploitants de services de trafic maritime (STM)			
	Transports routiers	Autorités routières chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale ; Exploitants de systèmes de transport intelligents			
3. Secteur bancaire	Établissements de crédit *[DORA Lex specialis]*				
4. Infrastructures des marchés financiers	Exploitants de plates-formes de négociation ; Contreparties centrales *[DORA Lex specialis]*				
5. Santé	Prestataires de soins de santé ; Laboratoires de référence de l'Union européenne ; Recherche et développement dans le domaine des médicaments ; Fabrication de produits pharmaceutiques de base et de préparations pharmaceutiques ; Fabrication de dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique				
6. Eau potable	Fournisseurs et distributeurs d'eaux destinées à la consommation humaine, **seulement si** cette activité est une partie essentielle de leur activité générale				
7. Eaux usées	Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées, **seulement si** cette activité est une partie essentielle de leur activité générale				
8. Infrastructure numérique	Prestataires de services de confiance qualifiés		Essentiel		
	Fournisseurs de services DNS [à l'exclusion des opérateurs de serveurs racines de noms de domaine]				
	Registres de noms de domaine de premier niveau				
	Fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public		Essentiel		Important*
	Prestataires de services de confiance non-qualifiés		Essentiel	Important*	Seulement si identifié*
	Fournisseurs de points d'échange internet				
	Fournisseurs de services d'informatique en nuage				
	Fournisseurs de services de centres de données				
	Fournisseurs de réseaux de diffusion de contenu				
9. Gestion des services TIC	Fournisseurs de services (de sécurité) gérés				
10. Administration publique (à l'exclusion du pouvoir judiciaire, des parlements, des banques centrales, de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi)	Administrations publiques qui dépendent de l'État fédéral		Essentiel		
	Administrations publiques qui dépendent des entités fédérées (après identification suite à une évaluation basée sur les risques de la criticité des services fournis)		Important*		
	Zones de secours (y compris le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale)				
11. Espace	Exploitants d'infrastructures terrestres qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics		Essentiel	Important*	Seulement si identifié*

Les définitions ces types d'entités peuvent être retrouvées aux annexes I et II ou à l'article 8 de la loi NIS2.

(*) Le CCB peut, le cas échéant, en fonction de la criticité des services fournis et des risques encourus, identifier certaines entités importantes comme entités essentielles ou identifier au sein d'un secteur d'autres catégories d'entité-types comme importantes ou essentielles.

CENTRE FOR CYBERSECURITY BELGIUM

ANNEXE II : AUTRES SECTEURS CRITIQUES

SECTEUR	SOUS-SECTEUR et/ou TYPE D'ENTITÉ	GRANDES ENTREPRISES *effectif d'au moins 250 ETP, ou chiffre d'affaires annuel > € 50 M et bilan annuel total > € 43 M*	MOYENNES ENTREPRISES *effectif d'au moins 50 ETP, ou > € 10 M de chiffre d'affaires annuel / bilan annuel total*	PETITES & MICRO ENTREPRISES
1. Services postaux et d'expédition	Prestataires de services postaux, y compris les prestataires de services d'expédition	Important*		Seulement si identifié*
2. Gestion des déchets	Seulement s'il s'agit de la principale activité économique			
3. Produits chimiques	Fabrication de substances et distribution de substances ou de mélanges ; Production d'articles à partir de substances ou de mélanges			
4. Denrées alimentaires	Activités de distribution en gros, production industrielle ou transformation industrielle de denrées alimentaires			
5. Fabrication	Dispositifs médicaux (in vitro); produits informatiques, électroniques et optiques ; équipements électriques ; machines et équipements n.c.a. ; véhicules automobiles, remorques et semi-remorques ; d'autres matériels de transport (NACE C 26-30)			
6. Fournisseurs numériques	Fournisseurs de places de marché en ligne			
	Moteurs de recherche en ligne			
	Plateformes de services de réseaux sociaux			
7. Recherche	Organismes de recherche, à l'exclusion des établissements d'enseignement			

(*) Le CCB peut, le cas échéant, en fonction de la criticité des services fournis et des risques encourus, identifier certaines entités importantes comme entités essentielles ou identifier au sein d'un secteur d'autres catégories d'entité-types comme importantes ou essentielles.

Remarque : les entités fournissant des services d'enregistrement de noms de domaine relèvent également de NIS2, mais elles doivent uniquement s'enregistrer sur Safeonweb@Work ainsi que mettre en place et maintenir une base des données d'enregistrement des noms de domaine complète et exacte.

LA DIRECTIVE NIS2 EN BELGIQUE

Ce document a été élaboré par le Centre pour la Cybersécurité Belgique (CCB). Cette administration fédérale a été créé par l'arrêté royal du 10 octobre 2014 et est sous l'autorité du Premier Ministre.

Les informations fournies :

- sont exclusivement à caractère général et n'entendent pas prendre en considération toutes les situations particulières ;
- ne sont pas nécessairement exhaustives, précises ou actualisées sur tous les points.

Éditeur responsable :
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur général
Rue de la loi, 18
1000 Bruxelles

Dépot légal:
D/2024/14828/007