Version 2.1.2
02/2026

CENTRE FOR CYBERSECURITY BELGIUM

Questions fréquemment posées (Frequently Asked Questions - FAQ) NIS2 en Belgique

Ce document a comme objectif de répondre aux questions fréquemment posées au sujet du cadre légal NIS2 en Belgique. Il complète les informations qui sont déjà disponibles sur le site web du CCB et sur Safeonweb@Work.

Pour toute question et réponse supplémentaire concernant spécifiquement l'utilisation opérationnelle de NIS2 et du CyberFundamentals Framework (inspection, informations à fournir, labels, etc.), veuillez consulter le FAQ opérationnel NIS2/CyFun®.

Table des matières

Historique des versions

Changements de la version 1.0 à 2.0

Questions supplémentaires	Questions approfondies
1.2, 1.6, 1.8, 1.13, 1.15, 1.15.1, 1.15.2, 1.15.3, 1.15.4, 1.15.5, 1.16, 1.16.1, 1.16.2, 1.16.3, 1.16.4, 1.16.5, 1.16.6, 1.16.7, 1.20, 1.21.2, 1.21.3, 1.22, 1.22.1, 1.22.2, 1.22.3, 1.22.4, 1.22.5, 1.22.6, 1.22.7, 1.22.8, 1.22.9, 1.22.10, 1.22.11, 1.22.12 2.2, 2.3, 2.6, 2.7, 2.8, 2.9 3.3.2, 3.4, 3.7, 3.8, 3.9, 3.10, 3.11, 3.13.2, 3.13.3, 3.13.4, 3.13.5, 3.13.6, 3.13.7, 3.13.8, 3.13.9, 3.13.10 4.3, 4.5, 4.7, 4.10, 4.12, 4.16 5.2, 5.3	1.3, 1.5, 1.12, 1.14, 1.17, 1.19, 1.21.1 2.4, 2.5 3.2, 3.3, 3.3.1, 3.6, 3.14 4.2.1, 4.4, 4.6, 4.9, 4.11, 4.14 5.1

Changements de la version 2.0 à 2.1

Questions supplémentaires	Questions approfondies
1.5.1, 1.5.2, 1.22.1.2, 1.22.2.2, 1.22.3, 1.22.3.1, 1.22.4.1, 1.22.4.2, 1.22.4.3, 1.22.4.4, 1.22.4.5, 1.22.4.6, 1.22.4.7, 1.22.5.8, 1.22.5.9, 1.22.7.3, 1.22.10, 1.22.11.5, 1.22.12.1, 1.22.13.1 2.10, 2.11 3.13.4 4.14.1, 4.14.2, 4.19	1.2, 1.5, 1.6, 1.18, 1.22.1.1, 1.22.4, 1.22.5.1, 1.22.5.3, 1.22.5.5, 1.22.5.6, 1.22.6, 1.22.7.1, 1.22.8, 1.22.11.4, 1.22.14.1 2.4, 2.7 3.13.10 4.2.2, 4.7, 4.11, 4.14

Un tableau de concordance est disponible à la fin du document.

Changements dans la version 2.1.*

La version 2.1.1 corrige quelques erreurs typographiques dans les quatre traductions.

La version 2.1.2 met à jour les explications et les références dans plusieurs questions relatives à l'adoption de la loi du 19 décembre 2025 sur la résilience des entités critiques, qui remplacera la loi du 1er juillet 2011 sur la sécurité et la protection des infrastructures critiques. Elle corrige également une erreur dans la section 1.21.3 relative à la qualification des fournisseurs de réseaux de communications électroniques publics et de services de communications électroniques accessibles au public.

Abréviations & Références

Les abréviations et références suivantes sont utilisés dans ce document :

- Arrêté Royal NIS2 : Arrêté royal du 9 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 (disponible sur Justel)
- BELAC : Organisme belge d'Accréditation
- CAB : *Conformity Assessment Body* (organisme d'évaluation de la conformité)
- CCB : Centre pour la Cybersécurité Belgique (autorité nationale de cybersécurité & CSIRT national)
- Convention SOLAS : Convention internationale de 1974 pour la sauvegarde de la vie humaine en mer
- CSIRT : Centre de réponse aux incidents de cybersécurité (*Computer Security Incident Response Team)* (en Belgique le CSIRT national est le CCB)
- CyFun® : CyberFundamentals Framework (disponible sur SafeonWeb@Work)
- 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 (disponible sur Eur-Lex)
- Directive NIS2 : Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (disponible sur Eur-Lex)
- DORA : Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011 (disponible sur Eur-Lex)
- Loi NIS1 : Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (disponible sur Justel)
- 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 (disponible sur Justel)
- NCCN : Centre de Crise National
- Recommandation (2003/361/CE) : Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (disponible sur Eur-Lex)
- RGPD : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (disponible sur Eur-Lex)

1. Général - Champ d'application

1.1. Quels sont les objectifs de la loi NIS2 ?

La directive 2022/2555 (dite « NIS2 ») et la loi NIS2 belge qui la transpose visent à renforcer la cyber-résilience en se concentrant sur les objectifs clés suivants :

1) Protection en matière de cybersécurité des services essentiels fournis dans l'Union européenne. En comparaison avec la directive NIS1, la directive NIS2 élargit le nombre de services essentiels visés dans différents secteurs hautement critiques (Annexe I) ou autres secteurs critiques (Annexe II). Le champ d'application est désormais principalement déterminé par l'utilisation de définitions européennes (comme « entité-type ») et d'un critère de taille (« size-cap ») ;
2) Renforcement des mesures de gestion des risques en matière de cybersécurité que les entités doivent prendre, ainsi que la notification des incidents significatifs (avec deux catégories d'entités essentielles ou importantes) ;
3) Encourager le partage d'informations sur les incidents et risques de cybersécurité entre les entités concernées et les CSIRTs nationaux ;
4) Renforcer la supervision et les sanctions ;
5) Assurer une coopération européenne et nationale.

1.2. Qu'est-ce qui a changé entre la loi NIS1 et la loi NIS2 ?

Le champ d'application de NIS2 a été largement étendu par rapport à NIS1, avec un changement important de paradigme. Au lieu de s'appuyer sur une procédure d'identification formelle, la loi NIS2 repose désormais principalement sur deux critères : le service fourni (type d'entité) par une organisation dans des secteurs ou sous-secteurs spécifiques, et sa taille (équivalente à celle d'une grande ou moyenne entreprise). À quelques exceptions près, seules les organisations établies en Belgique relèvent de la loi NIS2, que ce soit en tant qu'entités essentielles ou importantes. De plus amples informations sur le champ d'application de NIS2 sont disponibles à la section 1.3.

La plupart des entités NIS1 (opérateurs de services essentiels ou fournisseurs de services numériques) sont soumises à la loi NIS2 et doivent s'enregistrer en tant qu'entité NIS2 sur la plateforme du CCB (https://atwork.safeonweb.be). Les entités qui se sont déjà enregistrées pour le *Early Warning System* (EWS) du CCB doivent également s'enregistrer sur la plateforme Safeonweb@work. De plus amples informations sur l'enregistrement sont disponibles dans la section 3.13.1.

Les mesures de cybersécurité que les entités NIS2 doivent mettre en œuvre sont similaires à celles de NIS1, mais la loi NIS2 contient désormais une liste minimale de mesures spécifiques. Les exigences vont de la gestion de la chaîne d'approvisionnement à la gestion des vulnérabilités et à l'authentification multifactorielle (MFA), et sont plus explicites et détaillées qu'auparavant. De plus amples informations sur les mesures de cybersécurité sont disponibles à la section 3.2.

La procédure de notification des incidents est désormais plus détaillée et plus complète. La notification est obligatoire pour les entités essentielles et importantes lorsqu'un incident

significatif se produit, dans certains délais (sans retard injustifié et au plus tard dans les 24 heures pour l'alerte précoce, 72 heures pour la notification complète et 1 mois pour le rapport final). D'autres incidents, cybermenaces et incidents évités peuvent également être notifiés volontairement. La plateforme de notification des incidents NIS1 a été remplacée par un nouveau formulaire en ligne, accessible à tous sans nécessiter de connexion (https://notif.safeonweb.be). De plus amples informations sur la notification des incidents sont disponibles à la section 3.3.

Pour les entités relevant des secteurs bancaire et financier des annexes de la loi NIS2, le règlement DORA (Digital Operational Resilience Act) est une *lex specialis*, ce qui signifie qu'il remplace certaines obligations NIS2, telles que celles liées aux mesures de cybersécurité et à la notification des incidents. De plus amples informations sur DORA sont disponibles à la section 1.17.

NIS2 met l'accent sur la responsabilité des organes de direction des entités NIS2 en matière de cybersécurité. De plus amples informations sur cette responsabilité sont disponibles à la section 3.9.

L'extension du champ d'application des secteurs a nécessité une approche différente de la supervision :

- Les entités essentielles sont soumises à une évaluation périodique de la conformité obligatoire effectuée par un organisme d'évaluation de la conformité (CAB), ou à une inspection par le CCB ;
- Les entités importantes peuvent se soumettre volontairement à la même évaluation périodique de la conformité et sont en tout état de cause soumises à des contrôles ex post ;

De plus amples informations sur la supervision sont disponibles au chapitre 4.

La même nouvelle approche de supervision contient également un régime plus étendu de sanctions administratives, avec diverses amendes et mesures à la disposition de l'autorité de supervision. Les sanctions pénales prévues par NIS1 ont été supprimées. De plus amples informations sur les sanctions sont disponibles à la section 4.18.

En ce qui concerne les autorités impliquées dans la supervision, les autorités sectorielles NIS1 sont toutes devenues des autorités sectorielles NIS2, même si leur rôle a été adapté. En effet, le CCB dirige désormais la supervision pour tous les secteurs. De plus amples informations sur les autorités compétentes sont disponibles à la section 4.1.

1.3. Quel est le champ d'application de la loi NIS2 ?

Art. 3 à 7 loi NIS2

La loi NIS2 vise les entités publiques ou privées qui sont, en principe, établies en Belgique (il y a quelques exceptions à cette règle) et qui fournissent un service repris à l'annexe I ou II de la loi au sein de l'Union européenne.

Pour être considéré comme une entité soumise à la loi, il suffit d'exercer, indépendamment de sa forme juridique, au moins une des activités reprises dans les annexes I ou II de la loi au sein de l'Union européenne et de dépasser les seuils d'une entreprise moyenne au sens de la Recommandation 2003/361/CE de la Commission européenne du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises.

Les entités essentielles sont les organisations qui fournissent un service repris dans l'annexe I et qui dépassent les seuils d'une grande entreprise au sens de la Recommandation 2003/361/CE.

Les entités importantes sont les organisations qui fournissent un service :

- soit repris dans l'annexe I et qui dépassent les seuils d'une moyenne entreprise au sens de la Recommandation 2003/361/CE ;
- soit repris dans l'annexe II et qui dépassent les seuils d'une moyenne ou d'une grande entreprise, au sens de la Recommandation 2003/361/CE ;

L'article 1 de l'annexe de la Recommandation 2003/361/CE considère comme "entreprise" toute entité exerçant une activité économique, quelle que soit sa forme juridique. Cette notion peut inclure l'administration publique ou les entités publiques lorsqu'elles fournissent des services critiques (comme d'autres entités privées) mentionnées dans les annexes de la loi NIS2.

La règle du size-cap ne s'applique pas à certains types d'entités comme les administrations publiques, les entités critiques identifiées, les prestataires de services de confiance, les registres de noms de domaine de premier niveau et les fournisseurs de services DNS.

Il est important de souligner que **le champ d'application de la loi NIS2 porte sur l'ensemble de l'entité** concernée et non uniquement sur ses activités reprises dans les annexes de la loi.

Sauf si la définition du type d'entité (service) repris dans les annexes prend en considération le caractère accessoire ou non-essentiel de l'activité concernée, une entité tombe dans le champ d'application de la loi **même si le service concerné qu'elle fournit n'est qu'une partie accessoire ou non-essentielle de toutes ses activités.**

Pour plus d'informations, voir les sections suivantes.

1.4. Qu'est-ce qu'une "entité" dans le cadre de NIS2 ?

Art. 8, 37° loi NIS2 ; Art. 6 (35) directive NIS2

La loi NIS2 s'applique aux organisations qui peuvent être qualifiées d'"entité" au sens de la loi.

Une "entité" est définie comme suit dans la loi NIS2 : "*une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations*".

La loi NIS2 s'applique à toutes les entités de manière individuelle, même si elles sont regroupées et détenues par la même société holding. Le champ d'application et les obligations de la loi NIS2 doivent donc être analysés par chaque entité individuellement, en fonction des services qu'elle fournit.

Pour le secteur de l'administration publique, la directive NIS2 prévoit une notion spécifique d'"entité de l'administration publique" qui permet aux États membres de prendre en compte chaque entité reconnue comme telle conformément à leur droit public national.

Par exemple, il est possible de distinguer dans le secteur de l'administration publique plusieurs entités NIS2 distinctes au sein d'une même personne morale de droit public - à condition qu'une distinction juridiquement reconnue soit faite entre les différentes administrations publiques concernées.

1.5. Comment calculer la taille d'une entité ?

Vue d'ensemble

Art. 3, §§ 1 et 2 loi NIS2 & Recommandation 2003/361/CE

Pour les besoins du champ d'application de la loi NIS2, la taille de l'entité est calculée sur base des règles de l'annexe de la Recommandation 2003/361/CE. La Commission européenne a publié un guide explicatif détaillé et a mis à disposition un outil de calcul.

Une organisation est qualifiée de moyenne entreprise :

- soit lorsqu'elle occupe entre 50 et 249 travailleurs (salariés, personnel temporaire ou intérimaire, exploitants, associés, etc.) - effectif calculé en unités de travail par année (UTA) ; ou
- soit lorsqu'elle réalise un chiffre d'affaires annuel supérieur à 10 millions d'euros jusqu'à 50 millions d'euros et dispose d'un bilan annuel total supérieur à 10 millions d'euros jusque 43 millions d'euros.

Une organisation est qualifiée de grande entreprise :

- soit lorsqu'elle occupe 250 travailleurs ou plus (salariés, personnel temporaire ou intérimaire, exploitants, associés, etc.) - effectif calculé par unité de travail par année (UTA) ; ou
- soit lorsqu'elle réalise un chiffre d'affaires annuel supérieur à 50 millions d'euros et dispose d'un bilan annuel total supérieur à 43 millions d'euros.

Pour l'application de ces seuils de données financières, l'organisation concernée a **le choix de retenir soit son chiffre d'affaires annuel, soit son bilan annuel total**. **Une de ces deux données peut excéder le seuil d'une moyenne ou grande entreprise**, sans que cela ait d'impact sur la qualification d'une organisation.

Exemple 1 : une entreprise de 35 UTA (petite) a un chiffre d'affaires annuel de 1.000.000 € (petite) et un total du bilan annuel de 50.000.000 € (grande). Pour les montants financiers, elle choisit de ne prendre en compte que le plus faible : son chiffre d'affaires. Il s'agit donc d'une petite ou micro-entreprise.

Exemple 2 : une entreprise de 80 UTA (moyenne) a un chiffre d'affaires annuel de 1.000.000 € (petite) et un total du bilan annuel de 70.000.000 € (grande). Pour les montants financiers, elle choisit de ne prendre en compte que le plus faible : son chiffre d'affaires. Comme le chiffre d'affaires est petit mais que l'effectif est moyen, il s'agit d'une entreprise de taille moyenne.

Une explication visuelle est disponible ici.

Consolidation des données

Il faut tenir compte que dans les situations d'entreprises « partenaires » ou « liées », une consolidation proportionnelle des données (effectifs et financières) de l'entité concernée et de ces autres entités doit être réalisée pour calculer la taille.

Sauf exception, une entreprise est considérée comme « partenaire » lorsqu'elle détient entre 25% et 50% du capital ou des droits de vote (le plus élevé étant retenu) dans l'entité concernée (ou vice-versa). Ce type de relation décrit la situation des entreprises qui établissent certains

partenariats financiers avec d'autres entreprises, sans que les unes exercent un contrôle réel direct ou indirect sur les autres.

Sauf exception, une entreprise est considérée comme « liée » lorsqu'elle détient au-delà de 50% du capital ou des droits de vote (le plus élevé étant retenu) dans l'entité concernée (ou vice-versa).

En ce qui concerne les entreprises partenaires, l'entreprise considérée doit ajouter à ses propres données une proportion des effectifs et des données financières de l'autre entreprise pour déterminer sa taille. Cette proportion reflétera le pourcentage des parts ou des droits de vote détenus (le plus élevé des deux facteurs). Dans le cas d'entreprises liées, l'entreprise en question doit ajouter 100 % des données de l'entreprise liée aux siennes.

Par exemple, si une entreprise détient une participation de 30 % dans une autre entreprise, elle ajoute à ses propres chiffres 30 % des effectifs de l'entreprise partenaire, de son chiffre d'affaires et du total de son bilan. S'il y a plusieurs entreprises partenaires, le même type de calcul doit être effectué pour chaque entreprise partenaire située immédiatement en amont ou en aval de l'entreprise en question.

Dans le cadre de la loi NIS2, un mécanisme est néanmoins prévu permettant, en cas de situation disproportionnée, à l'autorité nationale de cybersécurité (CCB) de tenir compte du degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées, en particulier en ce qui concerne les réseaux et les systèmes d'information qu'elle utilise pour fournir ses services et en ce qui concerne les services qu'elle fournit. Ces éléments devront être démontrés au CCB, au cas par cas, par l'organisation qui souhaiterait en bénéficier. L'application de ce mécanisme peut conduire à requalifier une organisation comme entité d'importante plutôt qu'essentielle ou de l'exclure complètement du champ d'application de la loi. Voir également la section 1.5.1 ci-dessous.

Selon l'article 4 de l'annexe de la recommandation, les effectifs et les données financières à prendre en compte sont ceux du dernier exercice comptable approuvé, calculé sur une base annuelle, à compter de la date de clôture des comptes, hors TVA. Pour passer d'une qualification de taille à une autre, l'entreprise doit dépasser ou passer en dessous d'un seuil pendant au moins deux années consécutives. Une entreprise qui oscille entre deux seuils peut être amenée à remonter plus de deux ans en arrière pour déterminer sa qualification.

Voir également la section 1.21.3. et le guide détaillé sur le calcul de la taille pour plus de détails.

1.5.1. Quand et comment une organisation peut-elle faire usage du mécanisme d'indépendance visé à l'article 3, § 2, de la loi NIS2 ?

Lors du calcul de la taille d'une entité, les données des entreprises partenaires et liées doivent, en principe, toujours être consolidées avec les données de cette entité, conformément à la Recommandation (2003/361/CE). Dans certains cas exceptionnels, une organisation peut faire usage d'une option visée à l'article 3, § 2, de la loi NIS2.

Dans ce cas, les réseaux et systèmes d'information (environnements IT/OT) de l'entité doivent être **complètement indépendants (physiquement et/ou techniquement séparés)** des réseaux et systèmes d'informations d'entreprises partenaires. Ela doit être exécuté d'une manière telle que les environnements séparés n'influencent les risques pour les environnements dans le champ d'application de NIS2.

Cela signifie concrètement que si un environnement IT/OT d'une entreprise partenaire ou liée est affecté par un incident (telle qu'une cyberattaque), cela n'impacte pas la sécurité des opérations des systèmes IT/OT qui rentrent dans le champ d'application de NIS2.

D'un point de vue pratique, cela implique, entre autres choses :

- Pas d'infrastructures partagées (telles que des serveurs, segments de réseaux, Active Directory, location de service en nuage).
- Pas de dépendance qui pourrait compromettre un environnement lors d'un incident sur un autre environnement (par exemple via des tunnels VPN, des contrôles OT partagés, ou des plateformes de gestion centralisées).
- Une isolation du risque : une attaque sur un environnement ne peut pas mener à des interruptions, réductions de disponibilités, ou augmentations de la vulnérabilité des systèmes couverts par NIS2.

Cela est examiné au cas par cas par l'autorité compétente pour l'inspection, lors de ses contrôles.

La revendication d'une indépendance suffisante doit être **justifiée en détails** et relève **entièrement de la responsabilité de l'organisation concernée**. L'indépendance peut résulter en une consolidation réduite des données lors du calcul de la taille d'une organisation, ce qui peut influencer la qualification d'une organisation comme essentielle, importante, ou hors du champ d'application.

1.5.2. Quand une organisation passe-t-elle d'une taille d'entreprise à une autre ?

L'article 4.2 de l'annexe de la recommandation 2003/361/CE stipule, comme expliqué dans le guide de la Commission européenne, que si une entreprise dépasse les plafonds en termes d'effectifs ou de chiffre d'affaires au cours de l'année de référence, cela n'affectera pas sa situation et elle conservera la taille qu'elle avait au début de l'exercice comptable.

Toutefois, elle changera de taille si elle dépasse les plafonds pendant deux exercices comptables consécutifs. La nouvelle taille s'appliquera alors à partir de la fin de l'exercice comptable en question.

Les mêmes considérations s'appliquent en cas de réduction de taille si une entreprise passe en dessous des plafonds pendant deux exercices comptables consécutifs.

1.6. Pourquoi le site web et la FAQ du CCB concernant le size-cap semblent-ils différents de ce qui est écrit dans la recommandation 2003/361 de l'UE ?

Le texte de la Recommandation 2003/361 fait référence à "et" lorsqu'il décrit les seuils d'une PME. Cela s'explique par le fait que la recommandation décrit les seuils de la plus grande à la plus petite taille d'entreprise. Sur le site web du CCB cependant, et aux fins de NIS2, ces seuils sont décrits de la plus petite à la plus grande entreprise, ce qui aboutit à une description différente. Comme expliqué ci-après, les seuils restent inchangés :

- « 1. La catégorie des micro, petites et moyennes entreprises (PME) est constituée des entreprises qui occupent moins de 250 personnes et dont le chiffre d'affaires annuel **n'excède pas** 50 millions d'euros ou dont le total du bilan annuel **n'excède pas** 43 millions d'euros. »

  ➔ Le texte indique qu'une PME a < 250 ETP **et** < 50 mil. d'euros CAA ou ≤ 43 mil. BAT
  ➔ Donc une grande entreprise a ≥ 250 ETP **ou** > 50 mil. d'euros CAA et > 43 mil. BAT

- « 2. Dans la catégorie des PME, une petite entreprise est définie comme une entreprise qui occupe moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel **n'excède pas** 10 millions d'euros. »

  ➔ Le texte indique qu'une petite entreprise a < 50 ETP **et** ≤ 10 mil. d'euros CAA ou BAT
  ➔ Donc une entreprise moyenne a ≥ 50 ETP **ou** > 10 mil. d'euros CAA et > 10 mil. BAT, mais pas ≥ 250 ETP **ou** > 50 mil. CAA et > 43 mil. BAT

Il s'agit d'une application logique des seuils pour les besoins de NIS2.

L'outil officiel "SME Wizard" de la Commission européenne, conçu pour aider les entreprises à vérifier si elles sont ou non des PME, confirme les résultats de l'interprétation ci-dessus.

Notre page NIS2 sur Safeonweb@Work indique donc correctement (formulé légèrement différemment dans la section 1.5 ci-dessus) :

> *« Dépasser les seuils de taille d'une entreprise moyenne définis dans la recommandation 2003/361/CE, c'est-à-dire avoir un effectif d'au moins 50 travailleurs à temps plein ou un chiffre d'affaires annuel et un total de bilan annuel supérieur à 10 millions d'euros »*

Ceci est également correctement reflété dans notre outil de « scoping » (de détermination du champ d'application). Pour plus d'information, veuillez vous référer à la section 1.5 ci-dessus.

Un peu plus loin sur la page de NIS2, il est également indiqué ce qui suit :

> *« Ensuite, l'effectif doit être combiné avec les montants financiers pour obtenir la catégorisation définitive : une entreprise peut choisir de respecter soit le plafond du chiffre d'affaires, soit le plafond du total du bilan. Elle* ***peut dépasser l'un des plafonds financiers sans que cela n'ait d'incidence sur son statut de PME****. Nous ne* ***prenons donc en considération que le plus bas des deux*** *montants. »*

Ce texte est basé sur le guide officiel de la Commission européenne sur l'application de la Recommandation 2003/361/CE (p. 11).

Une entité est donc classée comme moyenne entreprise dans plusieurs situations possibles, soit sur la base du nombre de salariés à temps plein, soit sur la base des données financières, soit les deux ensembles. Cela correspond à la logique du mot "ou".

En ce qui concerne la qualification d'une organisation en tant qu'entité essentielle et importante en vertu de la loi NIS2, il importe peu de savoir si l'on détermine d'abord si l'organisation fournit un service énuméré dans les annexes de la loi, ou si l'on détermine d'abord la taille (ou si le size-cap ne s'applique pas). Le résultat final sera identique.

1.7. Quels sont les secteurs et services visés par la loi ?

Annexes I et II loi NIS2, article 8 loi NIS2

L'entité concernée doit fournir au moins l'un des services repris dans les annexes I ou II de la loi (même si ce service ne constitue qu'une partie accessoire de ses activités – sauf lorsque la définition elle-même utilise comme critère le caractère principal ou accessoire du service fourni) parmi les secteurs suivants :

Les secteurs hautement critiques (annexe I)	**Les autres secteurs critiques (annexe II)**
○ Energie (électricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène) ○ Transports (aériens, ferroviaires, par eau, routiers) ○ Secteur bancaire ○ Infrastructures des marchés financiers ○ Santé ○ Eau potable ○ Eaux usées ○ Infrastructure numérique ○ Gestion des services TIC ○ Administration publique ○ Espace	○ Services postaux et d'expédition ○ Gestion des déchets ○ Fabrication, production et distribution de produits chimiques ○ Production, transformation et distribution des denrées alimentaires ○ Fabrication (de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro; de produits informatiques, électroniques et optiques; d'équipements électriques; de machines et équipements n.c.a., véhicules automobiles, remorques et semi-remorques; d'autres matériels de transport) ○ Fournisseurs numériques ○ Recherche

Chaque service visé par la loi NIS2 **est défini** dans les annexes I ou II, avec un renvoi vers les définitions des normes juridiques européennes pertinentes ou à l'article 8 de la loi NIS2. Ces définitions doivent impérativement être consultées pour comprendre le service (type d'entité) concerné. À cette fin, les annexes sont accessibles sur le site du Moniteur belge (après le texte/dispositif de la loi).

Voir également la section 1.21.4 pour plus de détails sur la manière de déterminer quel(s) service(s) votre organisation fournit dans l'Union européenne et le test du champ d'application NIS2.

Voir la section 1.22 pour des informations plus spécifiques sur les secteurs.

1.8. Le service mentionné dans les annexes doit-il être l'activité principale de l'entité ?

Art. 3 loi NIS2

L'exposé des motifs de la loi NIS2 indique ce qui suit à propos de l'article 3 de la loi :

> *« Pour être considéré comme une entité publique ou privée d'un type visé à l'annexe I ou II de la loi, il suffit d'exercer, indépendamment de sa forme juridique, au moins une des activités reprises dans les annexes I ou II de la loi,* ***même si ce service ne constitue qu'une partie accessoire de ses activités*** *et de dépasser les plafonds visés au*

paragraphe 1er ou de rencontrer un des critères visés aux paragraphes 3 et suivants (voir infra) » (nous avons souligné)

L'article 3 de la loi NIS2, qui définit son champ d'application, se réfère aux concepts d'entités publiques ou privées d'un type visé à l'annexe I ou II, et qui constituent une moyenne ou grande entreprise au sens de la recommandation européenne 2003/361/CE.

De la même manière que la directive elle-même, cela signifie en pratique que le champ d'application de la loi NIS2 dépend directement des définitions figurant dans ses annexes I et II.

En général, **le caractère accessoire ou non essentiel de l'activité de l'entité concernée n'est pas pris en considération dans les définitions** (et n'influence donc pas le champ d'application de la loi NIS2). Toutefois, il existe quelques exceptions limitées où le critère d'"activité économique principale" ou de "partie non essentielle de l'activité générale" est utilisé dans les définitions et est effectivement pertinent (comme dans les secteurs de la gestion des déchets, de l'eau potable ou des eaux usées).

Ce n'est que dans les exceptions limitées prévues explicitement dans les définitions des annexes que la **nature accessoire ou non essentielle de l'activité doit être prise en compte**. Une entité concernée peut donc entrer dans le champ d'application de la loi**, même si le service concerné qu'elle fournit n'est qu'une partie accessoire ou non essentielle de l'ensemble de ses activités**, sauf disposition contraire dans les annexes**.**

Il n'y a ainsi pas de contradiction entre l'exposé des motifs et les dispositions de la loi NIS2 (et ses annexes), et le service ne doit être l'activité principale d'une entité que si cela est explicitement mentionné dans les annexes.

1.9. Est-il possible d'étendre les secteurs visés par la loi NIS2 dans le futur ?

Art. 3, § 6 loi NIS2

Le Roi pourrait ajouter des secteurs ou sous-secteurs aux annexes I et II par arrêté délibéré en Conseil des ministres après avoir consulté les éventuelles autorités sectorielles concernées et l'autorité nationale de cybersécurité (CCB).

De cette manière, lorsqu'il apparaît, dans le futur, qu'un secteur ne se trouvant pas encore dans le champ d'application devrait y être intégré en raison de son importance pour des activités sociétales et/ou économiques critiques, les annexes pourront être étendues.

1.10. Est-il possible qu'une entité relève de plusieurs secteurs ?

Art. 8, 34°; 25 ; 39, al. 2 et 44, § 1, al. 2 loi NIS2

Oui, il est possible qu'une même entité relève de plusieurs secteurs (en fonction de l'ensemble de ses activités). Dans ce cas, plusieurs considérations sont à prendre en compte :

- Les obligations plus strictes l'emportent sur les obligations moins strictes. En conséquence et si le critère de taille est réuni (grande entreprise), une entité qui fournit des services qui relèvent à la fois de l'annexe I et II sera dans son ensemble soumise aux obligations qui incombent à une entité essentielle ;

- L'entité pourra alors potentiellement relever de la supervision de l'autorité national de cybersécurité (CCB) et de plusieurs autorités sectorielles. Ces dernières collaboreront entre elles dans le cadre de la supervision ;
- Une entité publique qui exerce à titre principal un service repris dans un autre secteur des annexes de la loi relève uniquement de ce secteur (et non simultanément de ce secteur et du secteur de l'administration publique).

1.11. Quelle est la différence entre les entités « essentielles » et les entités « importantes » ?

Art. 39-42 ; 48, §§ 1 et 2 ; 58 et 59 loi NIS2

Les entités essentielles et importantes se distinguent principalement dans le cadre de la supervision et des sanctions. En effet, les entités essentielles sont contrôlées de façon proactive « *ex ante* » et réactive « *ex post* ». Plus particulièrement, les entités essentielles sont soumises à une évaluation régulière de la conformité.

Les entités importantes font l'objet d'une supervision « *ex post* », c'est-à-dire sur base d'éléments de preuve, d'indications ou d'informations selon lesquels une entité importante ne respecte pas les obligations de la loi.

Pour plus d'informations quant à la supervision, voir la section 4.4.

Pour le reste, les deux types d'entités sont soumises aux mêmes obligations, par exemple en matière de notification des incidents (section 3.3.) ou de prise de mesures de gestion de risques en matière de cybersécurité (section 3.2.).

1.12. Comment fonctionne l'éventuelle procédure complémentaire d'identification ?

Art. 11 loi NIS2

D'initiative ou sur proposition de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité (CCB) peut identifier, au sein d'un secteur existant des annexes de la loi NIS2, une entité comme essentielle ou importante, quelle que soit sa taille, dans les cas suivants :

1. l'entité est le seul prestataire, en Belgique, d'au moins un service essentiel au maintien d'activités sociétales ou économiques critiques, dans l'un des secteurs ou sous-secteurs repris aux annexes I et II de la loi;
2. une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique;
3. une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en particulier pour les secteurs où une telle interruption pourrait avoir un impact transfrontière;
4. l'entité est critique en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants, en Belgique.

Une proposition de décision d'identification est communiquée à l'entité concernée et aux autorités sectorielles compétentes, qui peuvent émettre avis dans un délai de soixante jours.

Le CCB évalue et, le cas échéant, met à jour l'identification des entités essentielles et importantes au moins tous les deux ans, selon les mêmes modalités.

1.13. Que se passe-t-il lorsqu'une entité NIS2 est acquise par une autre organisation ?

Si une société ou association acquiert une entité NIS2, l'entité NIS2 concernée devra toujours se conformer à la loi, tant que le(s) service(s) qu'elle fournit et les critères de size-cap demeurent remplis. La qualification NIS2 de l'entité concernée n'est pas transférée à l'organisation acquéreuse ou à l'organisation mère (si elles restent deux entités juridiques différentes). Bien entendu, l'organisation acquéreuse pourrait elle-même tomber sous le coup de la loi si elle fournit un service NIS2 au sein même de l'UE.

La qualification en tant qu'entité importante sous NIS2 pourrait changer après l'acquisition, car l'entité deviendra peut-être plus grande selon les calculs du size-cap. Ceux-ci peuvent en effet être revus après une période de deux ans (section 1.5). En fonction du service fourni par l'entité NIS2 (annexes), une augmentation de la taille pourrait conduire à une nouvelle qualification comme entité essentielle au lieu d'importante.

En tout état de cause, l'organisation acquéreuse pourrait devoir mettre en œuvre des mesures de gestion des risques en matière de cybersécurité en raison de l'obligation de l'entité NIS2 de sécuriser sa chaîne d'approvisionnement ou dans le cas où elles partagent les mêmes réseaux et systèmes d'information (section 3.14).

1.14. Que signifie "établissement (principal)" ? La loi s'applique-t-elle uniquement aux organisations belges ou également à d'autres entités ?

La loi NIS2 belge s'applique en principe aux entités qui sont **établies en Belgique** et qui fournissent leurs services ou exercent leurs activités au sein de l'UE (règle de l'établissement).

Art. 4 loi NIS2

La notion d'« entité » est définie à l'article 8, 37° de la loi NIS2, comme : *« une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations »*. Voir également la section 1.4.

La notion d'établissement consiste en 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, d'une filiale, d'une unité d'établissement, d'une usine, d'un bureau commercial, etc.

La loi NIS2 prévoit trois exceptions à la règle de l'établissement en Belgique :

1) Lorsque des fournisseurs de réseaux de communications électroniques publics et fournisseurs de services de communications électroniques accessibles au public fournissent leur service en Belgique (règle de localisation de service);

2) Lorsque des 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 ont leur établissement principal en Belgique (règle de l'établissement principal);
3) Lorsque des entités de l'administration publique ont été créés par la Belgique.

Pour déterminer l'"établissement principal" d'une entité, les établissements suivants doivent être déterminés en cascade (si le premier critère ne peut être déterminé ou est situé en dehors de l'UE, le deuxième ou le troisième est utilisé) :

1° où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité ;
2° où l'entité mène ses opérations de cybersécurité ;
3° où l'entité compte le plus grand nombre de salariés dans l'Union.

Si une entité n'est pas établie dans l'UE mais fournit un service soumis à la règle de juridiction de l'établissement principal, elle doit désigner un représentant légal établi dans l'un des États membres où elle fournit ses services. Si ce représentant est situé en Belgique, l'entité sera considérée comme ayant son établissement principal en Belgique.

Dans le cadre du régime de la juridiction de l'établissement principal, si une entité possède plusieurs établissements dans différents États membres de l'UE, elle ne sera soumise aux obligations NIS2 que dans l'État membre où se trouve son établissement principal.

Voir les sections suivantes pour des scénarios plus complexes.

1.15. Questions spécifiques relatives à la juridiction et à l'établissement (à qui la loi s'applique-t-elle ?)

1.15.1. Que se passe-t-il si mon organisation fournit des services qui relèvent des règles de juridiction en matière d'établissement et d'établissement principal ? Comment combiner différentes règles de juridiction ?

En fonction du type de services fournis, les entités NIS2 peuvent être amenées à combiner différentes règles juridictionnelles (par exemple, un opérateur de télécommunications peut fournir des réseaux de communications électroniques publics relevant de la règle de juridiction basée sur la localisation, produire de l'électricité relevant de la règle d'établissement et un service de sécurité géré relevant de la règle d'établissement principal) et éventuellement être soumises à plusieurs législations de transposition et plusieurs autorités de supervision compétentes (en fonction du service concerné et de la localisation de ses établissements).

Les différentes autorités nationales compétentes collaboreront en ce qui concerne les inspections et la notification des incidents significatifs. Toutefois, cela implique que l'entité devra, dans cette situation, combiner les règles d'au moins deux États membres différents en

appliquant les règles les plus strictes de l'un d'entre eux à tous ses services. Cela permet de s'assurer que les règles de plusieurs États membres sont correctement respectées.

1.15.2. Que se passe-t-il si une entité dispose une société fille/mère ou une filiale dans un autre État membre de l'UE qui doit également se conformer à NIS2 ?

Cela dépend du service fourni par l'organisation concernée dans l'autre État membre. La société fille/mère/filiale doit être qualifiée d'"entité" en vertu de la loi NIS2 (voir section 1.4).

La loi NIS2 **s'applique à toutes les organisations de manière individuelle**, même si elles sont regroupées et/ou détenues par la même société holding. Le champ d'application et les obligations de la loi NIS2 doivent donc être analysés par chaque organisation individuellement, sur la base des services qu'elle fournit. Il est donc possible qu'une société fille doive se conformer à la loi NIS2, alors qu'une société mère ne le doive pas.

Les points suivants fournissent une analyse plus approfondie des différentes possibilités.

A. Le service fourni ne relève pas de l'une des exceptions de juridiction (section 1.14)

L'organisation dans l'autre État membre devra respecter la loi NIS2 de l'État membre où elle est établie.

Exemple : La société mère est établie en Belgique et la société fille est établie en France. Elles fournissent toutes les deux des services relevant du secteur des denrées alimentaire (annexe II de la loi NIS2). Leur effectif consolidé (size-cap) est suffisant pour être qualifié de moyennes entreprises. La société mère en Belgique devra respecter NIS2 en Belgique, et la société fille devra respecter NIS2 en France.

B. Le service fourni relève de l'exception basée sur la localisation du service (communication électronique).

L'organisation dans l'autre État membre devra respecter la loi NIS2 de l'État membre ou des États membres où elle fournit ses services.

Exemple : La société mère est établie en Belgique et la société fille est établie au Luxembourg. Cette dernière fournit des services de communication électronique publique en Belgique, au Luxembourg et en Allemagne. Si l'on y ajoute les données de la société mère, il s'agit d'une grande entreprise. La société fille doit donc respecter les législation NIS2 de la Belgique, du Luxembourg et de l'Allemagne (en tant qu'entité essentielle). Dans la pratique, il faudra combiner les différentes exigences et respecter les règles les plus strictes pour garantir la conformité avec les trois régimes juridiques.

C. Le service fourni relève de l'exception de l'établissement principal

L'organisation dans l'autre État membre devra respecter la loi NIS2 de l'État membre où elle a son établissement principal (voir section 1.14).

Exemple : La société mère est établie en Belgique. Elle prend principalement les décisions relatives aux mesures de gestion des risques en matière de cybersécurité pour elle-même mais également pour sa filiale aux Pays-Bas. La société mère ne fournit pas de service NIS2 et n'est donc pas elle-même concernée par NIS2. La filiale est établie aux Pays-Bas, est une entreprise

de taille moyenne et y fournit des services gérés. Néanmoins, comme son établissement principal se trouve en Belgique, la filiale relève de NIS2 en Belgique (et doit par exemple s'enregistrer uniquement en Belgique).

1.15.3. Que se passe-t-il si, au sein d'un même groupe, il y a des entités NIS2 établies dans plusieurs États membres de l'UE ?

Comme expliqué dans la section 1.15.2, selon les services fournis par les différentes organisations, celles-ci peuvent être soumises à plusieurs juridictions au sein de l'UE.

Il est tout à fait possible qu'une entreprise d'un groupe doive se conformer à NIS2 en Belgique, tandis qu'une autre entreprise doit se conformer à NIS2 en Pologne, par exemple. Si le groupe possède une société holding, cette dernière devra également analyser si elle tombe sous NIS2 en raison d'un service qu'elle fournit (NIS2 s'applique à toutes les organisations de manière individuelle, mais la taille est calculée au niveau du groupe avec les entreprises partenaires ou liées).

1.15.4. Une entreprise active dans l'un des secteurs NIS2 doit suivre NIS2 dans le pays A, mais sa société mère établie dans le pays B ne doit pas le faire. Comment cela fonctionne-t-il ?

L'entreprise n° 1 doit respecter les obligations contenues dans la loi NIS2 du pays A. Cela comprend l'enregistrement, la notification des incidents, les mesures de cybersécurité, etc. La société mère n° 2 du pays B ne doit pas respecter toutes ces obligations puisqu'elle ne tombe pas sous NIS2.

Cependant, il existe d'autres façons dont la société mère peut être affectée :

1. Si les deux entreprises partagent les mêmes réseaux et systèmes d'information, l'application de NIS2 à l'entreprise n° 1 exigera que les mesures de gestion des risques de cybersécurité soient prises sur l'ensemble du (des) système(s) et du (des) réseau(x) afin de tout protéger (approche tous risques des mesures de gestion des risques de cybersécurité sous NIS2, voir section 3.2).
2. L'obligation pour l'entreprise n° 1 sous NIS2 d'assurer la sécurité de sa chaîne d'approvisionnement pourrait l'amener à imposer la mise en œuvre de mesures de cybersécurité à sa société mère n° 2 (voir la section 3.14).

Si l'entité établie dans le pays A n'est qu'une succursale (même entité juridique) de la société établie dans le pays B, c'est l'ensemble de l'entité juridique qui est soumise aux obligations de NIS2 conformément à NIS2 dans le pays A (indépendamment de l'endroit où son réseau et ses systèmes d'information sont physiquement situés).

1.15.5. Que se passe-t-il si une organisation (fille/mère) est établie en dehors de l'UE mais fournit des services dans l'UE ?

En principe, les organisations établies en dehors de l'UE ne tombent pas sous NIS2, sauf si elles fournissent dans l'UE un service qui relève de l'une des trois règles de compétence exceptionnelles expliquées à la section 1.14.

Pour le service relevant de la règle de juridiction basé sur la localisation des services (communication électronique), la législation NIS2 du ou des États membres dans lesquels l'organisation établie en dehors de l'UE fournit ses services s'applique.

Si l'organisation située en dehors de l'UE fournit un service au sein de l'UE qui relève de l'exception relative à l'établissement principal, elle doit désigner un représentant légal établi dans un État membre où elle fournit ses services. Si ce représentant est situé en Belgique, l'entité sera considérée comme ayant son établissement principal en Belgique.

La loi définit un représentant légal comme : *« une personne physique ou morale établie dans l'Union européenne qui est expressément désignée pour agir pour le compte d'un fournisseur de services DNS, d'un registre de noms de domaine de premier niveau, d'une entité fournissant des services d'enregistrement de noms de domaine, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu, d'un fournisseur de services gérés, d'un fournisseur de services de sécurité gérés ou d'un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l'Union européenne, qui peut être contactée par l'autorité nationale de cybersécurité à la place de l'entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi »*.

Afin de déterminer si une telle entité propose des services dans l'Union, il convient d'examiner si elle envisage d'offrir des services à des personnes dans un ou plusieurs États membres. La seule accessibilité, dans l'Union, du site internet de l'entité ou d'un intermédiaire ou d'une adresse électronique ou d'autres coordonnées ou encore l'utilisation d'une langue généralement utilisée dans le pays tiers où l'entité est établie devraient être considérées comme ne suffisant pas pour établir une telle intention. Cependant, des facteurs tels que l'utilisation d'une langue ou d'une monnaie généralement utilisée dans un ou plusieurs États membres avec la possibilité de commander des services dans cette langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union pourraient indiquer que l'entité envisage d'offrir des services dans l'Union.

Le représentant devrait agir pour le compte de l'entité et devrait pouvoir être contacté par les autorités compétentes ou les CSIRT. Le représentant devrait être expressément désigné par un mandat écrit de l'entité le chargeant d'agir en son nom pour remplir les obligations, y compris la notification des incidents.

Pour savoir comment enregistrer une organisation établie en dehors de la Belgique, voir la section 3.13.8.

1.16. Questions spécifiques relatives aux groupes d'organisations ou d'entreprises

1.16.1. Comment évaluer le champ d'application de NIS2 par rapport à un groupe d'organisations ou d'entreprises ?

Au sein d'un groupe d'organisations ou d'entreprises, comme expliqué dans les sections précédentes, chaque entité juridique/organisation doit analyser et déterminer individuellement si elle entre dans le champ d'application de NIS2 sur la base de ses activités et des services qu'elle fournit. Le partage de données, de réseaux ou de systèmes d'information au sein du

groupe n'a aucune incidence sur le champ d'application. Il est conseillé à chaque organisation de procéder individuellement à travers les explications contenues dans la section 1.21.

Il convient de noter qu'au sein d'un groupe d'organisations ou d'entreprises, le nombre d'équivalents temps plein et les données financières devront être consolidés sur la base des différentes règles de la Recommandation 2003/361/CE. Pour plus d'information, voir la section 1.5.

1.16.2. Quel est l'impact d'une entité NIS2 sur les autres organisations ou entreprises du même groupe ?

Voir les explications de la section 1.15.4.

1.16.3. Que se passe-t-il si une autre organisation ou entreprise du même groupe utilise les mêmes réseaux et/ou systèmes d'information qu'une entité NIS2 ?

Si les deux organisations partagent les mêmes réseaux et systèmes d'information, l'inclusion d'une entité dans le champ d'application de NIS2 exigera que les mesures de gestion des risques en matière de cybersécurité soient prises sur l'ensemble des systèmes et réseaux partagés afin de tout protéger (conformément à l'approche « tous risques » des mesures de gestion des risques en matière de cybersécurité sous NIS2, voir la section 3.2).

1.16.4. Que se passe-t-il s'il existe à la fois des entités essentielles et des entités importantes au sein d'un même groupe d'organisations ou d'entreprises ?

La loi NIS2 s'applique individuellement à chaque entité juridique. Les entités qui ne sont pas dans le champ d'application de NIS2 mais qui font partie du même groupe ne seront pas directement affectées par NIS2, au-delà de ce qui est décrit dans la section 1.15.4. Le fait que des entités faisant partie du même groupe soient qualifiées d'entités essentielles ou d'importantes ne changera pas la situation.

1.16.5. Que se passe-t-il si une organisation ou une entreprise conclut un contrat avec un fournisseur de services NIS2 et permet à d'autres organisations d'utiliser ce contrat/service ?

Par exemple, une entreprise X conclut un contrat avec un fournisseur de services numériques - l'entreprise Y (comme un fournisseur de centre de données) - et permet ensuite que ce contrat/service soit utilisé par l'entreprise partenaire Z. Dans une telle situation, les services NIS2 restent fournis par l'entreprise Y et non par l'entreprise X (tant que l'entreprise X ne joue pas un rôle dans la fourniture du service NIS2 à l'entreprise Z).

1.16.6. Qu'en est-il des holdings qui n'ont (presque) pas de personnel, qui n'ont pas de chiffre d'affaires et dont le bilan est simplement positif ?

Si une société holding ne fournit pas de service NIS2, elle ne sera pas concernée par NIS2. Toutefois, l'effectif et ses données financières sont prises en compte pour l'évaluation du size-cap de toute entreprise liée ou partenaire fournissant un service NIS2.

Outre ces éléments, les considérations de la section 1.15.4 s'appliquent également.

1.16.7. Que se passe-t-il si une organisation fournit des services informatiques à d'autres organisations au sein du même groupe d'organisations ou d'entreprises ?

Au sein d'un groupe d'organisations ou de sociétés, chaque entité juridique distincte doit analyser pour elle-même et individuellement si elle relève du champ d'application de NIS2, sur base de ses propres activités et services fournis (les effectifs et les données financières seront toutefois en principe consolidés avec les entreprises liées ou partenaires (voir section 1.5)).

Lorsqu'une entité juridique fournit un service NIS2 (par exemple, en tant que prestataire de services gérés ou en tant que prestataire de services informatiques en nuage) à une autre entité juridique distincte, celle-ci peut tomber sous NIS2 (en fonction de sa taille), **même si l'activité n'est proposée qu'à un nombre limité d'organisations ou d'entreprises au sein d'un même groupe**.

Toutefois, la situation peut être envisagée différemment si deux ou plusieurs organisations partagent effectivement des données, des réseaux ou des systèmes entre elles au sein d'un groupe (et partagent ensemble les coûts pertinents) et qu'il n'y a pas une organisation spécifique qui fournit des services gérés aux autres.

Voir également la section 1.22.7.2 sur les fournisseurs de services gérés.

1.17. Quel sont les interactions entre le Règlement DORA et la directive NIS2 ?

Art. 6 loi NIS2
Art. 2 & 47 DORA

La directive NIS2 et sa loi de transposition visent des mesures transversales en matière de cybersécurité dans l'UE. L'objectif est d'améliorer la cybersécurité globale dans l'UE et, en particulier, d'assurer un niveau élevé de cybersécurité de certaines entités critiques pour les activités sociétales et économiques.

Le Règlement DORA (Digital Operational Resilience Act) cible spécifiquement les opérateurs du secteur financier. Il vise à renforcer la résilience opérationnelle des systèmes d'information dans le secteur financier et à coordonner les réglementations existantes en la matière.

DORA s'applique aux institutions financières qui sont énumérées à l'article 2 du règlement. Il s'agit des :

- établissements de crédit;
- établissements de paiement;

- prestataires de services d'information sur les comptes;
- établissements de monnaie électronique;
- entreprises d'investissement;
- prestataires de services sur crypto-actifs;
- dépositaires centraux de titres;
- contreparties centrales;
- plates-formes de négociation;
- référentiels centraux;
- gestionnaires de fonds d'investissement alternatifs;
- sociétés de gestion;
- prestataires de services de communication de données;
- entreprises d'assurance et de réassurance;
- intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire;
- institutions de retraite professionnelle;
- agences de notation de crédit;
- administrateurs d'indices de référence d'importance critique;
- prestataires de services de financement participatif;
- référentiels des titrisations;
- prestataires tiers de services TIC.

Les exigences de NIS2 et DORA se chevauchent pour les entités actives dans le secteur bancaire et financier. La directive NIS2 prévoit dès lors une règle de *lex specialis* : lorsque des exigences sectorielles équivalentes en matière de cybersécurité et de notification des incidents significatifs existent au niveau européen, elles prévalent sur les exigences générales/trans-sectorielles issues de la directive NIS2.

Toutefois, les prestataires de services TIC tiers couverts par DORA ne sont pas concernés par la règle de *la lex specialis* et peuvent être soumis aux obligations de DORA et NIS2.

Il est important de noter que les entités NIS2 des secteurs bancaire et financier établies en Belgique doivent toujours s'enregistrer comme les autres entités NIS2. Les incidents significatifs notifiés par les entités DORA via leur propre mécanisme de notification seront transmis par les autorités compétentes (Banque Nationale de Belgique et FSMA) au CCB.

1.18. Est-ce que les infrastructures critiques / entités critiques tombent dans le champ d'application de la loi NIS2 ?

Art. 9, 5° et 25, § 2 loi NIS2

Oui, **l'exploitant d'infrastructures critiques** identifié dans le cadre de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et les organisations identifiées comme entités critiques au sens de la loi du 19 décembre 2025 relative à la résilience des entités critiques sont considérées comme une entité essentielle au sens de la loi NIS2.

Les **exploitants d'infrastructures critiques** sont des organisations **formellement identifiées** par l'autorité sectorielle compétente conformément à la loi du 01 juillet 2011 relative à la sécurité et la protection des infrastructures critiques. **Les organisations qui ont été identifiées ont reçues une lettre formelle** relative à leur identification et sont sujettes à des obligations

spécifiques en matière de sécurité. En cas de doute, veuillez consulter un expert juridique au sein de votre organisation pour vérifier si vous devez vous conformer à cette loi.

Les **entités critiques (entités CER)** sont des organisations qui ont été formellement identifiées dans le cadre de la loi du 19 décembre 2025 sur la résilience des entités critiques. **Les entités critiques (« entités CER ») ont remplacé les « exploitants d'infrastructures critiques ». Ces derniers seront automatiquement considérés comme des entités critiques après le 17 juillet 2026, conformément à l'article 79 de la loi du 19 décembre 2025.** Les entités critiques sont également notifiées officiellement de leur identification par l'autorité compétente.

Les autorités NIS2 et les autorités compétentes en vertu de la loi du 1er juillet 2011 la loi du 19 décembre 2025 collaborent entre elles dans le cadre de la supervision de ces entités.

Plus d'informations sur les infrastructures critiques peuvent être trouvés sur le site internet du Centre de Crise National.

1.19. Est-ce que les codes NACE peuvent être utilisés pour déterminer si une entité tombe sous la loi NIS2 ?

Annexes I et II loi NIS2

Certains services repris aux annexes I et II renvoient effectivement vers des codes NACE. Les entités établies en Belgique et qui fournissent des services relevant de ces codes NACE doivent donc examiner attentivement si la loi NIS2 ne s'appliquerait pas à elles (voir notamment la section 1.22.13).

Pour toutes les entités qui ne sont pas dans le cas précité, visés dans les annexes de la loi NIS2, les codes NACE ne constituent pas une base suffisante pour déterminer si une entité tombe dans le champ d'application de la loi NIS2. Certains codes NACE peuvent être utilisés de manière préliminaire par les entités, mais une vérification plus approfondie de leur service fourni exacte est nécessaire afin de déterminer si elles relèvent ou non du champ d'application souvent plus restrictif de la loi NIS2. L'indication d'un certain code NACE sur le site de la Banque-Carrefour des Entreprises (BCE) n'a aucun effet sur le champ d'application pour ces types d'entités.

1.20. Est-ce que les organismes d'évaluation de la conformité entrent dans le champ d'application de la loi ?

Les services normalement fournis par les organismes d'évaluation de la conformité (CAB) ne figurent pas en tant que tels dans la liste des entités des annexes I et II de la loi NIS2. Cela signifie que les CAB qui limitent leurs activités à l'évaluation de la conformité n'entrent pas dans le champ d'application de la loi NIS2.

Toutefois, les CAB qui fournissent également des services décrits à l'annexe I ou II de la loi NIS2 peuvent entrer dans le champ d'application de la loi s'ils remplissent également le critère de taille, même si ces services ne sont qu'accessoires à leurs activités principales.

1.21. Quelle est la méthode à suivre pour déterminer si une organisation tombe sous le champ d'application de la loi NIS2 ?

La méthode décrite ci-dessous expose de manière détaillée les différentes étapes du raisonnement lié au champ d'application de la loi NIS2. Celle-ci ne prétend toutefois pas être exhaustive ou la seule méthode utilisable.

Cette section couvre les éléments suivants :

1. Avant d'examiner la loi NIS2 proprement dite :
    a. Est-ce que mon organisation a été identifiée en tant qu'exploitant d'une infrastructure critique ou entité critique ?
    b. Mon organisation est-elle soumise à DORA ?
2. Quelle est la taille de mon organisation ?
3. Quel(s) service(s) mon organisation fournit-elle dans l'Union européenne ?
4. Quel est le lieu d'établissement de mon organisation en Europe ?
5. Est-ce que mon organisation pourrait être identifiée par la suite ou est-elle dans la chaine d'approvisionnement d'une entité NIS2 ?

Voir aussi notre outil de test du champ d'application NIS2.

1.21.1. Avant d'examiner la loi NIS2 proprement dite

Avant d'entrer dans l'analyse proprement dite, il est d'abord nécessaire de se pencher sur deux possibilités qui ont un impact important sur comment fonctionne le champ d'application de la loi NIS2 pour les organisations concernées.

1.21.1.1. Est-ce que mon organisation a été identifiée en tant qu'exploitant d'une infrastructure critique ou entité critique ?

L'article 3, § 4 de la loi NIS2 précisait que la loi s'appliquait automatiquement aux entités identifiées comme exploitants d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques. À compter du 19/01/2026, il est désormais prévu que la loi s'applique automatiquement aux organisations identifiées comme entités critiques au sens de la loi du 19 décembre 2025 relative à la résilience des entités critiques, quelle que soit leur taille.

Les entités critiques (avant les « exploitants d'une infrastructure critique ») ne doivent donc pas analyser si leur organisation entre ou non dans le champ d'application : elles tombent sous la loi NIS2 et sont automatiquement qualifiées en tant qu'entités essentielles.

Voir la section 1.18.

1.21.1.2. Mon organisation est-elle soumise à DORA ?

Les entités établies en Belgique et soumises au règlement DORA sont exclues des principales exigences de la loi NIS2.

Voir la section 1.17.

1.21.2. Mon organisation est-elle une "entité" (groupe d'entreprises) ?

Pour que la loi soit applicable, une organisation doit être qualifiée d'"entité" selon l'article 8, 37° de la loi NIS2 : "*une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations*".

Cet élément est particulièrement important pour les grandes organisations ou les groupes de sociétés, où les établissements situés dans d'autres États membres, tels que les succursales, peuvent ne pas être en mesure d'agir sous leur propre nom ou d'exercer des droits et d'être soumis à des obligations. Dans une telle situation, la loi NIS2 s'appliquerait à la société qui a la personnalité juridique de la succursale.

1.21.3. Quelle est la taille de mon organisation ?

Pour tomber dans le champ d'application de la loi NIS2, une entité doit avoir une certaine taille. Pour calculer cette taille, la loi NIS2 fait référence à la Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises. Cette Recommandation définie les seuils à partir de quand une entreprise (toute entité engagée dans une activité économique) peut être considérée comme étant une petite, moyenne, ou grande entreprise. Sauf exceptions, seules les entreprises de taille moyenne ou grande entrent dans le champ d'application de la loi NIS2.

Deux conditions sont à vérifier pour établir la taille : l'effectif (mesuré en unités de travail par année (UTA)[1]) et les montants financier (chiffre d'affaires et/ou bilan annuel total).

L'effectif doit être combiné avec les montants financiers pour obtenir la taille d'entreprise : une entreprise peut choisir de respecter soit le plafond du chiffre d'affaires, soit le plafond du total du bilan. Elle **peut dépasser l'un des plafonds financiers sans que cela n'ait d'incidence sur son statut de PME**. En principe, nous ne **prenons donc en considération que le plus bas des deux** montants.

Exemple 1 : une entreprise de 35 UTA (petite) a un chiffre d'affaires annuel de 1.000.000 € (petite) et un total du bilan annuel de 50.000.000 € (grande). Pour les montants financiers, elle choisit de ne prendre en compte que le plus faible : son chiffre d'affaires. Il s'agit donc d'une petite ou microentreprise.

Exemple 2 : une entreprise de 80 UTA (moyenne) a un chiffre d'affaires annuel de 1.000.000 € (petite) et un total du bilan annuel de 70.000.000 € (grande). Pour les montants financiers, elle choisit de ne prendre en compte que le plus faible : son chiffre d'affaires. Comme le chiffre d'affaires est petit mais que l'effectif est moyen, il s'agit d'une entreprise de taille moyenne.

Vous trouverez un résumé visuel des tailles d'entreprise possibles sur notre site web.

Si nous combinons les différentes tailles possibles avec le critère du service fourni, nous obtenons le champ d'application suivant :

[1] Les unités de travail par année (UTA) correspondent au nombre de personnes ayant travaillé dans l'entreprise considérée ou pour le compte de cette entreprise à temps plein pendant toute l'année considérée. Le travail des personnes n'ayant pas travaillé toute l'année, ou ayant travaillé à temps partiel, quelle que soit sa durée, ou le travail saisonnier, est compté comme fractions d'UTA.

- Une moyenne entreprise a un effectif entre 50 et 249 UTA ou a un chiffre d'affaires annuel et bilan annuel total qui dépasse les 10 millions d'euros :
  - ➔ Entre dans le champ d'application en tant que « entité importante » si elle fournit un service repris dans l'annexe II de la loi.
  - ➔ Entrent **en principe** dans le champ d'application en tant que « entité importante » si elle fournit un service repris dans l'annexe I de la loi.
- Une grande entreprise a un effectif d'au moins 250 UTA ou a un chiffre d'affaires annuel qui excède 50 millions d'euros et un total du bilan annuel qui excède 43 millions d'euros :
  - ➔ Entre dans le champ d'application en tant que « entité importante » si elle fournit un service essentiel repris dans l'annexe II de la loi.
  - ➔ Entre **en principe** dans le champ d'application en tant que « entité essentielle » si elle fournit un service repris dans l'annexe I de la loi.

La Recommandation prévoit notamment que dans le cadre d'entités groupées en tant que « entreprises liées » ou « entreprises partenaires », selon les critères définis, les données (nombre de travailleurs à temps plein & montants financiers) des autres entités faisant partie du groupe d'entités sont prises en compte pour effectuer le calcul de la taille.

Voir aussi section 1.5.

Pour plus d'informations sur l'application de la Recommandation, nous invitons vivement de consulter le Guide de l'utilisateur pour la définition des PME de la Commission. Il reprend tous les critères et des exemples visuels pour au mieux vous aider à appliquer la Recommandation. La Commission a également mis en place un outil pour tester la taille de votre organisation.

Il existe toutefois quelques **exceptions**. Les types entités suivantes tombent dans le champ d'application de la loi NIS2, quelle que soit leur taille :

- prestataires de services de confiance qualifiées (essentiel) ;
- prestataires de services de confiance non-qualifiées (important si micro, petite, moyenne entreprise et essentiel si grande entreprise) ;
- fournisseurs d'un service DNS (essentiel) ;
- registres de noms de domaines de premier niveau (essentiel) ;
- services d'enregistrement de noms de domaine (pour l'enregistrement uniquement) ;
- fournisseurs de réseaux de communications électroniques publics (Important si micro ou petite entreprise et essentiel si moyenne ou grande entreprise) ;
- fournisseurs de services de communications électroniques accessibles au public (Important si micro ou petite entreprise et essentiel si moyenne ou grande entreprise) ;
- entités identifiées comme exploitants d'une infrastructure critique en vertu de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou comme entité critique en vertu de la loi du 19 décembre 2025 relative à la résilience des entités critiques (essentiel) ;
- entités de l'administration publique qui dépendent de l'État fédéral (essentiel).

Le point suivant explique comment retrouver les définitions des services fournis par ces types d'entités.

1.21.4. Quel(s) service(s) mon organisation fournit-elle dans l'Union européenne ?

Une fois la taille d'une entité connue, il faut ensuite effectuer une analyse détaillée de l'ensemble des services fournis à des tiers par celle-ci, par secteur ou sous-secteur. Il est important de faire une topographie de chaque service, même si celui-ci ne constitue qu'une activité accessoire de l'entité (sauf si la définition du service prend en considération le caractère principal ou accessoire du service concerné).

Les annexes I et II (ou les définitions) de la loi NIS2 détaillent les services concernés (« entité type »), souvent avec une référence aux législations européennes correspondantes ou aux définitions prévues à l'article 8 de la loi.

Les différents secteurs et sous-secteurs sont les suivants :

Les secteurs hautement critiques (annexe I)	Les 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 TIC (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 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 s'agit alors de faire le lien entre les services fournis l'organisation et les définitions précitées. La condition liée au service fourni est ainsi remplie en cas de correspondance entre les deux. Il est tout à fait possible qu'une organisation fournissent plusieurs services listés dans différents secteurs (voir à cet égard la section 1.10).

En conclusion, les entités « importantes » et les entités « essentielles » sont les suivantes (à l'exception des entités types listés à la fin de la section 1.21.3 précédente) :

	Moyenne entreprise	Grande entreprise
Services de l'annexe I	Importante	Essentielle
Services de l'annexe II	Importante	Importante

1.21.5. L'établissement

En principe, la loi NIS2 belge s'applique aux entités qui sont **établies en Belgique et 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.

Selon le type d'entité concernée, il existe néanmoins certaines exceptions à la règle de l'établissement en Belgique. Les règles quant au champ d'application territorial/juridiction de la loi NIS2 belge sont expliqués à la section 1.14.

1.21.6. Identification additionnelle et chaine d'approvisionnement

Nonobstant les règles précitées, le CCB a la possibilité, au besoin, de procéder à l'identification de certaines entités établies en Belgique et actives dans les secteur repris aux annexes de la loi NIS2. Cette identification additionnelle se déroule en concertation avec l'organisation concernée – voir la section 1.12.

Indépendamment du champ d'application de la loi NIS2, il faut tenir compte qu'un grand nombre d'organisation seront impactées indirectement par ces nouvelles exigences légales dès lors que celles-ci se retrouvent dans la chaine d'approvisionnement d'une ou plusieurs entité(s) NIS2. Ces dernières ont l'obligation de garantir la sécurité de leur propre chaine d'approvisionnement et peuvent ainsi imposer contractuellement des obligations à leurs fournisseurs directs ou prestataires de service. Pour plus d'explications, voir la section 3.14.

1.22. Questions sectorielles relatives à certains types d'entités et de secteurs

1.22.1. Annexe I - 1. Énergie - (a) Électricité

1.22.1.1. Est-ce que les organisations produisant de l'électricité principalement pour leur propre consommation (y compris les panneaux solaires, etc.) tombent dans le champ d'application de la loi ?

Annexe I Loi NIS2 et directive (UE) 2019/944

En vertu de l'article 3, lu conjointement avec l'annexe I, point (1)(a) tiret 4, de la loi NIS2, les "[p]roducteurs tels que définis à l'article 2, point (38), de la directive (UE) 2019/944" entrent dans le champ d'application lorsqu'ils sont qualifiés de moyennes entreprises au titre de l'article 2 de l'annexe de la recommandation 2003/361/CE, ou qu'ils dépassent les plafonds fixés pour les moyennes entreprises.

L'article 2, point (38), de la directive (UE) 2019/944 définit le **"producteur"** comme "une personne physique ou morale qui produit de l'électricité", tandis que la **"production"** est définie comme "la production d'électricité" conformément à l'article 2, point (37), de la directive (UE) 2019/944.

Conformément à ces définitions, les entités qui exploitent des panneaux solaires ou des éoliennes connectés au réseau électrique, même si elles consomment principalement elles-

mêmes l'électricité autoproduite, sont considérées comme des producteurs en vertu de l'article 2, point (38), de la directive (UE) 2019/944, et entrent par conséquent dans le champ d'application de NIS2 si elles sont au moins une entreprise de taille moyenne.

Toutefois, il a été convenu au niveau de l'UE que ces "producteurs" ne sont pas les entités hautement critiques visées dans le sous-secteur de l'électricité de la directive NIS2. Par conséquent, ils restent dans le champ d'application de NIS mais une approche de supervision moins stricte peut leur être appliquée. En Belgique, ces entités **peuvent justifier plus facilement l'usage d'un niveau inférieur du CyFun®**.

En Belgique, les entités qui relèvent de la définition d'un service dans le sous-secteur de l'électricité, **uniquement** parce qu'elles produisent principalement de l'électricité pour leur **propre consommation**, conservent leur qualification NIS2 (essentielle ou importante), mais sont soumises à une supervision moins stricte. En pratique, elles doivent toujours s'enregistrer, signaler les incidents significatifs et appliquer des mesures de cybersécurité, mais l'utilisation d'un **niveau d'assurance inférieur du CyberFundamentals (CyFun®) Framework** (par exemple, Basic) pour se conformer à leurs obligations, sera considéré comme proportionné. Cette solution tient compte de l'impact sociétal et économique plutôt limité de leur production d'électricité.

Cette approche s'explique de par la formulation des définitions de l'Annexe I de la loi NIS2. Il n'est pas juridiquement possible de dévier des définitions de l'Annexe I, ce qui signifie que tout « producteur » d'électricité rentre dans le champ d'application de NIS2 s'il constitue au moins une moyenne entreprise. Dans ce contexte, le CCB ne peut pas interpréter le texte d'une manière qui serait contraire à ce que la loi prévoit expressément.

1.22.1.2. Mon organisation est-elle un producteur d'électricité si... ?

L'article 2, point (38), de la directive (UE) 2019/944 définit **« producteur »** comme « une personne physique ou morale qui produit de l'électricité », tandis que « production » est défini comme « la production d'électricité », selon le même article, point (37), de la directive (UE) 2019/944.

Là où les sous-sections qui suivent mentionnent des « panneaux solaires », tout autre moyen d'autoproduction d'électricité, tel que les éoliennes, peut être utiliser de manière interchangeable.

Veuillez vous référer à la section 1.22.1.1 ci-dessus pour plus d'informations.

A) Mon organisation possède des panneaux solaires, mais consomment toute l'électricité qu'elle produit elle-même

Dans cette situation, l'organisation rentre tout de même dans le champ d'application de NIS2 si ses panneaux solaires sont connectés au réseau.

B) Mon organisation possède des panneaux solaires, mais aucune quantité de l'électricité produite est injectée dans le réseau

Si l'électricité n'est pas injectée dans le réseau, l'organisation ne rentre pas dans le champ d'application de NIS2. En effet, les risques sociétaux et économiques qui découlent de la production d'électricité au moyen de panneaux solaires sont dus à l'éventuel impact qu'une perturbation pourrait avoir sur le réseau d'électricité.

C) Mon organisation loue un bâtiment muni de panneaux solaires que l'organisation ne possède pas, mais dont elle consomme l'électricité (en tout ou en partie)

Si l'organisation ne possède pas et/ou n'exploite pas les panneaux solaires en question, elle ne peut pas être considérée comme un « producteur » qui produit de l'électricité. Elle ne rentre donc pas dans le champ d'application de NIS2.

D) Mon organisation permet à une autre organisation d'utiliser l'espace sur toit de mon organisation pour placer des panneaux solaires que l'autre organisation exploite

Mêmes considérations qu'au point C.

E) Mon organisation achète de l'électricité à une autre organisation qui exploite des panneaux solaires placés sur le toit de mon organisation

Mêmes considérations qu'au point C.

1.22.1.3. Qu'est-ce qui relève des "exploitants de points de recharge" ?

L'annexe I, sous-secteur électricité de la loi NIS2 mentionne les "[e]xploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité". En l'absence de définitions supplémentaires, les termes doivent être compris dans leur sens usuel.

Cette définition implique les conditions suivantes :

1) L'exploitant d'un point de recharge
2) Responsable de la gestion et de l'exploitation dudit point de recharge
3) La recharge est fournie aux utilisateurs finaux (y compris au nom et pour le compte d'un fournisseur de services de mobilité).

Par exemple, si un supermarché place des points de recharge sur son parking, il peut tomber sous NIS2 s'il est responsable de la gestion et de l'exploitation du point de recharge. Cette gestion et cette exploitation sont souvent déléguées contractuellement à une organisation tierce, même si les points de recharge sont étiquetés au nom du supermarché. Une organisation doit donc vérifier concrètement si elle gère et exploite elle-même une borne de recharge ou si ce service est confié à une organisation tierce.

1.22.2. Annexe I - 1. Énergie - (c) Pétrole

1.22.2.1. Qu'est-ce qui est couvert par les "exploitants d'oléoducs" ?

La loi NIS2 et son annexe ne donnent pas de définition des "exploitants d'oléoducs". Ces termes doivent donc être compris dans leur sens habituel.

1.22.2.2. Que couvre la notion « [d']exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole » ?

Ce type d'entité couvre les services suivants :

- Exploitants d'installations de production de pétrole
- Exploitants d'installations de raffinage de pétrole
- Exploitants d'installations de traitement de pétrole
- Exploitants d'installations de stockage de pétrole

- Exploitants d'installations de transport de pétrole

Pour la notion « d'exploitants d'installation de stockage de pétrole » spécifiquement, il n'y a pas de capacité de stockage minimum requise. Cette notion faire référence à une organisation qui fournit un service à un tiers qui consiste en l'exploitation d'une installation de stockage de pétrole. Cela implique que les organisations qui stockent du pétrole pour elles-mêmes, sans que cela consiste en son activité économique, ne sont pas concernées. Il faut noter que, par exemple, les stations de pompes à essence franchisées correspondent au type d'entité ici expliqué mais ne dépassent probablement pas les seuils de taille.

La notion d'exploitants d'installations de transport de pétrole se limite aux exploitants de pipeline pour pétrole. Cette notion n'inclue pas le transport de pétrole par route.

Voici ci-dessous une liste exemplative de produits pétroliers couverts par la notion de « pétrole » :

- essences et naphtas ;
- kérosènes (en ce compris (kérosène d'aviation) ;
- gas-oils (en ce compris le carburant diesel, mazout pour chauffage domestique et flux de mélange de gas-oil) ;
- huiles combustibles lourdes.

1.22.3. Annexe I – 1. Énergie – (e) Hydrogène

1.22.3.1. Que couvre la notion « [d']exploitants de systèmes de production, de stockage et de transport d'hydrogène » ?

La Directive NIS2 ne fournit pas de définition ou de clarification pour la notion « [d']exploitants de systèmes de production, de stockage et de transport d'hydrogène ». Cela étant, de manière systématique, la Directive NIS2 fait référence à des définitions existantes de la législation régulant des aspects du marché intérieur, dans d'autres sous-secteurs. En particulier, le sous-secteur de l'électricité, à l'Annexe I (1) (a) de la Directive NIS2 contient des références aux définitions établies par la Directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et par le Règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité. Pour le sous-secteur du gaz, à l'Annexe I (1) (d) de la Directive NIS2 contient des références à la Directive 2009/73/CE du Parlement Européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel, qui a été abrogée et remplacée par la Directive (UE) 2024/1788 du Parlement européen et du Conseil du 13 juin 2024 concernant des règles communes pour les marchés intérieurs du gaz renouvelable, du gaz naturel et de l'hydrogène.

Le cadre politique européen sur l'hydrogène n'a été proposé par la Commission qu'en juillet 2021 et n'était donc pas encore en vigueur lorsque la Directive NIS2 a été adoptée. Cela étant, toute disposition du droit de l'Union doit être placé dans son contexte et interprété à la lumière de l'ensemble des dispositions de ce droit, de ses finalités, et de l'état de son évolution à la date à laquelle l'application de la disposition en cause doit être faite[2]. Etant donné que la Directive NIS2 fait référence à des définitions établies dans la législation du marché intérieur relative aux sous-secteurs de l'électricité et du gaz, il apparaît plausible de faire référence aux définitions établies

[2] C.J., 6 octobre 1982, *Srl CILFIT et Lanificio di Gavardo SpA* contre *Ministère de la santé*, C-283/81, point 20.

par la Directive(UE) 2024/1788 du Parlement européen et du Conseil du 13 juin 2024 concernant des règles communes pour les marchés intérieurs du gaz renouvelable, du gaz naturel et de l'hydrogène, afin de clarifier la notion « [d']exploitants de systèmes de production, de stockage et de transport d'hydrogène ».

Compte tenu de ce qui précède, les notions « [d']exploitants de systèmes de stockage d'hydrogène » et « [d']exploitants de systèmes de transport d'hydrogène » devraient être compris comme « gestionnaire de stockage d'hydrogène » tel que défini à l'article 2 (6) de la Directive (UE) 2024/1788 et « gestionnaire de réseau de transport d'hydrogène » tel que défini à l'article 2 (26) de la Directive (UE) 2024/1788. En outre, « exploitants de systèmes de production » devrait être compris dans le sens de l'article 2 (14), de la Directive (EU) 2024/1788 qui dispose qu'une « entreprise d'hydrogène » désigne « *une personne physique ou morale qui remplit au moins une des fonctions suivantes: la production [...] d'hydrogène [...]* ».

1.22.4. Annexe I - 2. Transport

Le secteur des transports comprend plusieurs sous-secteurs et types d'entités :

a) Air :
   a. Transporteurs aériens
   b. Entités gestionnaires d'aéroports, aéroports, et entités exploitants les installations annexes se trouvant dans les aéroports
   c. Services du contrôle de la circulation aérienne
b) Rail :
   a. Gestionnaires de l'infrastructure
   b. Entreprises ferroviaires
c) L'eau :
   a. Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret
   b. Entités gestionnaires des ports
   c. Exploitants de services de trafic maritime
d) Route :
   a. Autorités routières
   b. Exploitants de systèmes de transport intelligents

1.22.4.1. Que couvre la notion « [d']entités gestionnaires d'aéroports » ?

Une entité gestionnaire d'aéroport consiste en « une entité qui, conjointement ou non avec d'autres activités, tient de la législation nationale, de la réglementation ou de contrats la mission d'administration et de gestion des infrastructures de l'aéroport ou du réseau aéroportuaire, ainsi que de coordination et de contrôle des activités des différents opérateurs présents dans les aéroports ou le réseau aéroportuaire concernés », ainsi défini par l'article 2 (2), de la Directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires.

1.22.4.2. Que couvre le mot « aéroport » ?

Un aéroport est défini comme « tout terrain spécifiquement aménagé pour l'atterrissage, le décollage et les manœuvres d'aéronefs, y compris les installations annexes que ces opérations peuvent impliquer pour les besoins du trafic et le service des aéronefs, y compris les installations

nécessaires pour assister les services commerciaux de transport aérien » par l'article 2 (1), de la Directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires.

1.22.4.3. Que couvre la notion « [d']entités exploitants les installations annexes se trouvant dans les aéroports » ?

La notion « [d']entités exploitants les installations annexes se trouvant dans les aéroports » n'est définie ni dans la loi NIS2 ni la directive NIS2. Dans cette situation, et en coopération avec l'autorité sectorielle compétente, le CCB fait usage de la définition suivante pour délimiter le champ d'application :

La notion « [d']**entités exploitants les installations annexes se trouvant dans les aéroports** » désignent *les organisations qui gèrent les installations situées dans, ou connectées à, un aéroport et qui se reposent sur le système numérique de l'aéroport pour soutenir leurs opérations, et qui peuvent être intégrées de manière étroite dans l'écosystème de l'aéroport, en ce compris dans les systèmes d'information de l'aéroport afin d'accéder et d'échanger des données critiques telles que les horaires de vol, le statut en temps réel, le contrôle de sécurité et d'accès, le suivi de bagages et de cargos, la planification de ressources, et intégrées de manière étroite dans les plateformes de communication permettant la coordination avec le contrôle du trafic aérien, avec la gestion au sol, et avec d'autres parties prenantes*.

1.22.4.4. Que couvre le mot « route » ?

Le terme de « route » peut être compris dans le sens de « voie publique », tel que définie à l'article 2, I, de l'arrêté royal du 3 juin 2024 relatif au Code de la voie publique (le code fédéral de la voie publique). Cette définition étant très longue, elle n'est pas reproduite dans ce document.

Il faut noter cependant que le code fédéral de la voie publique n'entre en vigueur qu'à partir du 1er juin 2027. Jusqu'à cette date, les définitions de l'arrêté royal du 1er décembre 1975 portant règlement général sur la police de la circulation routière et de l'usage de la voie publique resteront en vigueur. La notion de voie publique y est similaire.

1.22.4.5. Que couvre la notion de « sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret » ?

L'annexe I, secteur transport, sous-secteur du transport par eau comprend les « sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, telles qu'elles sont définies pour le domaine du transport maritime à l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil, à l'exclusion des navires exploités à titre individuel par ces sociétés ». Le règlement auquel il est fait référence a pour objectif de fournir une base pour l'interprétation et la mise en œuvre harmonisées, ainsi que le contrôle communautaire des mesures spéciales pour renforcer la sûreté maritime, tel que prescrit dans la convention internationale de 1974 relative à la sauvegarde de la vie en mer (convention SOLAS). L'annexe I de cette régulation contient et amende des extraits de la convention SOLAS.

Cependant, ni ces extraits, ni la convention SOLAS ne contiennent de définition de « sociétés de transport par voie d'eau ». Il faut à la place porter son attention sur la définition de « compagnie », définie dans la régulation IX/1.2 (Chapitre IX, régulation 1, point 2) de la convention SOLAS. Cette définition est la suivante :

« *« Compagnie » désigne le propriétaire du navire ou tout autre organisme ou personne, tel que l'armateur gérant ou l'affréteur coque nue, auquel le propriétaire du navire a confié la responsabilité de l'exploitation du navire et qui, en assumant cette responsabilité, s'acquitte des tâches et des obligations imposées par le code international de gestion de la sécurité*. »

Ce type d'entité repris à l'annexe I de la loi NIS2 porte donc sur les compagnies, tel que défini ci-dessus, qui fournit le transport par voie d'eau intérieure, maritime et côtier de passagers et de fret. Les compagnies qui transportent du fuel (« fret ») par voie d'eau, par exemple, tombent a priori dans le champ d'application de cette définition.

1.22.4.6. Que couvre la notion « [d']entités gestionnaires des ports » ?

L'annexe I de la loi NIS2 mentionne les « entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE du Parlement européen et du Conseil, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004, ainsi que les entités exploitant des infrastructures et des équipements à l'intérieur des ports ».

La directive 2006/65/CE et le règlement 725/2004 fournissent les définitions suivantes :

- Un port signifie « *toute étendue déterminée de terre et d'eau, dont le périmètre est défini par les États membres dans lequel le port est situé, comprenant des infrastructures et équipements destinés à faciliter les opérations de transport maritime commercial* ».
- Une installation portuaire signifie « *un emplacement où a lieu l'interface navire/port; elle comprend les zones telles que les zones de mouillage, les postes d'attente et leurs abords à partir de la mer, selon le cas* »

1.22.4.7. Que couvre la notion « [d']exploitants de systèmes de transport intelligents » ?

Les exploitants de systèmes de transport intelligents (STI) sont définis comme les exploitants de « *systèmes dans lesquels des technologies de l'information et de la communication sont appliquées, dans le domaine du transport routier, y compris les infrastructures, les véhicules et les usagers, et dans la gestion de la circulation et la gestion de la mobilité, ainsi que pour les interfaces avec d'autres modes de transport* » (art. 4, 1., directive 2010/40/EU).

Bien que la directive 2010/40/EU contient les définitions des termes « prestataire de services STI » et « utilisateur de STI », les termes « exploitants de STI » ne sont pas définis par la directive 2010/40/EU. La définition de « prestataire de services STI » à l'article 4, 5., de la directive 2010/40/EU se réfère à tout prestataire d'un service STI, qu'il soit public ou privé. L'article 4, 4., de la directive 2010/40/EU définit un « service STI » comme « *la mise en place d'une application STI dans un cadre organisationnel et opérationnel clairement défini en vue d'améliorer la sécurité de l'utilisateur, l'efficacité, la mobilité durable ou le confort, ou de faciliter ou de soutenir les opérations de transport et de voyage* ». Un « *utilisateur de STI » signifie « tout utilisateur d'applications ou de services STI, notamment les voyageurs, les usagers vulnérables de la route, les usagers et les exploitants des infrastructures de transport routier, les gestionnaires de flottes et les opérateurs de services d'urgence* », conformément à l'article 4, 6., de la directive 2010/40/EU.

Vu que la directive NIS2 a pour objectif d'obtenir un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, reflétant l'importance des secteurs ou services pour les activités sociales et économiques dans le marché intérieur, « exploitants de STI » devrait être compris comme

« prestataire de services STI » dans le sens de l'article 4. 5., de la directive 2010/40/EU. Inversement, ceux qui fournissent un service ITS aux exploitants, tels que les développeurs du programme sous-jacent, ne semblent pas tomber dans le champ d'application de la définition, mais pourraient tomber dans le champ d'application d'un autre secteur NIS2 ou dans la chaîne d'approvisionnement.

1.22.5. Annexe I - 5. Santé

Le secteur de la santé comprend plusieurs types d'entités :

- Prestataires de soins de santé
- Laboratoires de référence de l'Union européenne
- Entités exerçant des activités de recherche et de développement dans le domaine des médicaments
- Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques
- Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique

1.22.5.1. Quelles sont les organisations qui répondent à la définition d'un prestataire de soins de santé (hôpitaux, maisons de repos, soins résidentiels, etc.) ?

Les prestataires de soins de santé mentionnés à l'annexe I, 5. Santé, font référence aux prestataires de soins de santé tels que définis à l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil et sont définis comme suit : « toute personne physique ou morale ou toute autre entité qui dispense légalement des soins de santé sur le territoire d'un État membre ».

Pour déterminer si une organisation relève de la définition de prestataire de soins de santé, il convient de vérifier si des "soins de santé" sont dispensés par ces entités :

1) Les soins de santé sont définis dans cette directive comme « des services de santé fournis par des professionnels de la santé aux patients pour évaluer, maintenir ou rétablir leur état de santé, y compris la prescription, la délivrance et la fourniture de médicaments et de dispositifs médicaux ».
2) La directive définit également les "professionnels de la santé" comme « un médecin, un infirmier responsable des soins généraux, un praticien de l'art dentaire, une sage-femme ou un pharmacien au sens de la directive 2005/36/CE, ou un autre professionnel exerçant des activités dans le secteur des soins de santé qui sont limitées à une profession réglementée telle que définie à l'article 3, paragraphe 1, point a), de la directive 2005/36/CE, ou une personne considérée comme un professionnel de la santé conformément à la législation de l'État membre de traitement »

Chaque entité concernée doit donc vérifier elle-même si les activités qu'elle exerce constituent des services de santé/des soins de santé fournis par un professionnel de la santé ou si ces entités se contentent de fournir des soins.

Les soins de santé/services de santé comprennent par exemple : les soins aux personnes âgées, les soins psychiatriques et psychologiques, les hôpitaux, les centres de revalidation, les maisons

de retraite, les soins résidentiels, les activités de soins infirmiers à domicile, les centres de réadaptation ambulatoire, les médecins, les infirmiers, ... Les entités qui fournissent des soins aux personnes handicapées et l'enseignement ordinaire/spécialisé peuvent également relever de cette catégorie, si des activités liées aux soins de santé sont également fournies au sein de ces entités.

Les entités qui ne fournissent généralement pas de services de santé sont par exemple : les soins à domicile (seul le travail domestique est fourni), la garde d'enfants, les crèches, ...

Il est important que chaque organisation analyse ses propres activités dans la pratique pour vérifier si elle fournit des services de santé. Comme indiqué précédemment, toutes les activités d'une entité doivent être prises en compte pour déterminer s'il s'agit d'une entité NIS2. Même les activités accessoires, et pas seulement l'activité principale, peuvent faire en sorte qu'une entité tombe sous NIS2. Il est également important de noter qu'une entité exerçant une activité NIS2 et remplissant le critère de taille sera soumise à la loi NIS2 dans son ensemble (pour tous ses réseaux et systèmes d'information).

1.22.5.2. Quelle est la différence entre "soins" et "soins de santé" ?

Les soins de santé sont des services de santé fournis par des professionnels de la santé aux patients pour évaluer, maintenir ou rétablir leur état de santé, y compris la prescription, la délivrance et la fourniture de médicaments et de dispositifs médicaux.

La notion de soins est plus large et peut, par exemple, englober la garde d'enfants, les activités de soins à domicile, etc.

1.22.5.3. Tous les prestataires de soins de santé dans le champ d'application NIS2 doivent-ils respecter les mêmes obligations (maisons de repos, soins psychiatrique, réadaptation) ?

Les maisons de repos, les instituts de soins psychiatriques qui constituent des petites ou moyennes entreprises, et les centres de réadaptation entrent dans la définition d'un prestataire de soins de santé (voir section 1.22.5.1). Elles sont donc, si elles répondent aux critères de taille et sont établies en Belgique, soit une entité essentielle, soit une entité importante au sens de la loi NIS2.

Toutefois, il a été convenu au niveau de l'UE que ces "prestataires de soins de santé" au sein de la catégorie des institutions de soins de longue durée ne sont pas les entités hautement critiques visées dans le secteur des soins de santé de la directive NIS2. Par conséquent, une approche de supervision moins stricte peut leur être appliquée.

En Belgique, les entités essentielles et importantes qui répondent à la définition de prestataire de soins de santé **uniquement** parce qu'elles disposent d'une, ou sont une **maison de retraite, un institut de soins psychiatriques qui constituent une petite ou moyenne entreprise, ou un centre de réadaptation**, conservent leur qualification NIS2 (essentielle ou importante), mais sont soumises à une supervision moins stricte. En pratique, elles doivent toujours s'enregistrer, notifier les incidents significatifs et appliquer des mesures de cybersécurité, mais l'utilisation d'un **niveau d'assurance inférieur du CyberFundamentals** (**CyFun®**) **Framework** (par exemple, Basic) pour se conformer à leurs obligations sera considéré comme proportionné. Cette solution tient compte de l'impact sociétal et économique plutôt limité de leurs services de santé.

1.22.5.4. Que se passe-t-il si mon organisation n'emploie pas ses propres professionnels de la santé ?

Dans le cadre de NIS2, une organisation doit fournir elle-même un service NIS2 pour entrer dans son champ d'application. Cela signifie que les organisations qui n'emploient pas leurs propres professionnels de la santé, mais font appel à des tiers pour fournir le service de santé, n'entrent pas dans le champ d'application en tant que prestataires de soins de santé.

1.22.5.5. Les entités fabriquant des dispositifs médicaux sont-elles concernées par la loi NIS2 ?

Les entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs critiques en cas d'urgence de santé publique), au sens de l'article 22 du règlement (UE) 2022/123, relèvent de l'annexe I, secteur 5. Santé de la loi NIS2.

Ce règlement fait référence à une liste (« liste des dispositifs médicaux critiques en cas d'urgence de santé publique ») qui doit être établie par le groupe de pilotage exécutif sur les pénuries de dispositifs médicaux (« groupe de pilotage sur les pénuries de dispositifs médicaux ») en cas d'urgence. Elle fait référence à des catégories de dispositifs médicaux considérés comme critiques dans le contexte de l'urgence de santé publique. Actuellement, aucune liste de ce type n'est encore disponible.

Etant donné que la liste des dispositifs médicaux critiques en cas d'urgence de santé publique est sujette à des mises à jour et que la reconnaissance d'une urgence de santé publique peut être clôturer, il est possible qu'une entité importante deviennent une entité essentielle pour la durée où un ou plusieurs des dispositifs médicaux qu'elle fabrique fait partie de la liste des dispositifs médicaux critiques en cas d'urgence de santé publique.

Les entités qui fabriquent des dispositifs médicaux peuvent également relever de l'annexe II, secteur 5, sous-secteur a) Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro. Pour plus d'informations sur ce sous-secteur, voir la section 1.22.13).

En outre, la plupart des entités qui fabriquent des dispositifs médicaux font partie de la chaîne d'approvisionnement d'entités NIS2 (par exemple, les prestataires de soins de santé de l'annexe I, secteur 5). Les entités couvertes par la loi NIS2 doivent prendre des mesures appropriées et proportionnées pour sécuriser leur réseau et leurs systèmes d'information. L'une de ces mesures 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. Pour plus d'informations sur les obligations relatives à la chaîne d'approvisionnement, voir la section 3.14.

1.22.5.6. Est-ce que les pharmacies sont visées par NIS2 ?

Les pharmacies peuvent potentiellement relever de plusieurs secteurs de la loi, principalement le secteur de la santé.

Tout d'abord, compte tenu de la définition d'un prestataire de soins de santé et de professionnel de la santé, comme expliqué dans la section 1.22.5.1, les pharmaciens en Belgique peuvent, dans certaines situations, administrer des injections et des vaccins. Ces actes peuvent être considérés comme des services de santé, ce qui fait entrer les pharmacies en question dans le

champ d'application de NIS2. Tout dépend donc ici de la question de savoir si le pharmacien fournit ou non des « services de santé ».

Par ailleurs, la directive 2011/24/UE se réfère à la directive 2001/83/CE pour fournir une définition de médicaments. Cette dernière définit un médicament à son article 1er, 2., comme :

« *a) toute substance ou composition présentée comme possédant des propriétés curatives ou préventives à l'égard des maladies humaines; ou*

b) toute substance ou composition pouvant être utilisée chez l'homme ou pouvant lui être administrée en vue soit de restaurer, de corriger ou de modifier des fonctions physiologiques en exerçant une action pharmacologique, immunologique ou métabolique, soit d'établir un diagnostic médical; »

Etant donné que les pharmaciens sont considérés comme des professionnels de la santé dans le scope de la directive 2005/36/CE, et que, dans le cadre de leur profession, ils prescrivent, dispensent et fournissent des médicaments et des dispositifs médicaux, les pharmacies devrait être considérées comme des prestataires de soins de santé tels que définis à l'article 3, g), de la directive 2011/24/UE, et devrait dès lors être couvert par l'annexe I, secteur de la santé, de la loi NIS2.

Deuxièmement, les pharmacies pourraient théoriquement être des "Entités exerçant des activités de recherche et de développement dans le domaine des médicaments" si elles recherchent et développent leurs propres produits pharmaceutiques (voir section 1.22.5.7, point A.). Ces activités de R&D sont toutefois principalement réservées aux entreprises spécialisées dans la recherche pharmaceutique.

Troisièmement, les pharmacies peuvent également être des « Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de l'annexe I, section C, division 21 » de NACE Rév. 2 (voir section 1.22.5.7, point B.), si elles possèdent le code NACE nécessaire.

Quatrièmement, les pharmacies pourraient entrer dans le secteur 3. Fabrication, production ou distribution de produits chimiques à l'annexe II à travers la production d'articles ou la distribution de substances ou de mélanges. Pour plus d'informations, voir la section 1.22.11.

Enfin, les pharmacies pourraient théoriquement relever de l'annexe II, secteur 5. Fabrication si elles fabriquent des dispositifs médicaux. Pour plus d'informations, voir la section 1.22.13.2.

En tant que pharmacie, ces cinq possibilités différentes doivent être analysées afin de déterminer si elles relèvent ou non de NIS2. Pour ces cinq possibilités, une pharmacie doit au moins être une entreprise de taille moyenne (voir section 1.5).

1.22.5.7. D'autres entreprises du secteur de la santé ou de la chaîne d'approvisionnement pharmaceutique pourrait tomber sous NIS2 ?

A. Entités exerçant des activités de recherche et de développement dans le domaine des médicaments

Les entités menant des activités de recherche et de développement dans le domaine des médicaments telles que définies à l'article 1er, point 2), de la directive 2001/83/CE relèvent de l'annexe I, secteur Santé. Il s'agit des entités menant des activités de recherche et de développement de :

> *« a) toute substance ou composition présentée comme possédant des propriétés curatives ou préventives à l'égard des maladies humaines ; ou*
>
> *b) toute substance ou composition pouvant être utilisée chez l'homme ou pouvant lui être administrée en vue soit de restaurer, de corriger ou de modifier des fonctions physiologiques en exerçant une action pharmacologique, immunologique ou métabolique, soit d'établir un diagnostic médical »*

Il est important de noter que les organismes de recherche peuvent également tomber sous l'annexe II, secteur 7. Recherche. Pour plus d'informations, voir la section 1.22.14.

B. Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques

Les entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques visés à la section C, division 21 de NACE Rév. 2 relèvent de l'annexe I, secteur Santé. Ces entités ont les codes NACE suivants :

- 21.10 Fabrication de produits pharmaceutiques de base
- 21.20 Fabrication de préparations pharmaceutiques

Le code NACE d'une organisation belge peut par exemple être vérifié sur le site web de la Banque Carrefour des Entreprises.

C. Entités fabriquant, produisant ou distribuant des produits chimiques

Ces entités relèvent du secteur chimique à l'annexe II. Pour plus d'informations, voir la section 1.22.11.

D. Grossistes en produits pharmaceutiques (vente de produits pharmaceutiques)

La vente de produits pharmaceutiques, aux consommateurs ou aux entreprises, n'est pas explicitement visée dans les annexes de la loi NIS2. Toutefois, elle pourrait relever de la distribution de produits chimiques si les critères et les définitions sont respectés, comme expliqué dans la section 1.22.11.2.

E. Services de livraison de médicaments par coursier

La livraison par coursier de médicaments ne relève pas de l'annexe I, secteur 5. Santé. Dans certains cas, cependant, ils peuvent relever du secteur 1. Services postaux et d'expédition de l'annexe II.

Pour plus d'informations, voir la section 1.22.9.

F. Caisses d'assurance sociale

Les caisses d'assurance sociale ne sont pas explicitement visées dans les annexes de la loi NIS2. Si ces institutions sont privées et qu'elles ne fournissent que ce service, elles ne sont pas incluses dans le champ d'application de NIS2.

Toutefois, les administrations publiques de la sécurité sociale pourraient relever du secteur Administration publique de l'annexe I si les différents critères sont établis. Pour plus d'informations, voir la section 2.1.

G. Fournisseurs de logiciels liés à la santé

Comme pour les fournisseurs d'autres logiciels, les définitions des fournisseurs de services informatiques en nuage et des fournisseurs de services gérés doivent être analysées. Pour plus d'informations, voir respectivement les sections 1.22.7.1 et 1.22.8. Par ailleurs, les fournisseurs de logiciels liés à la santé peuvent également être soumis aux obligations de la chaîne d'approvisionnement (pour plus d'informations, voir la section 3.14).

H. Réseaux de données de santé (eHealth)

Les fournisseurs de réseaux de données de santé (tels que CoZo, Réseau de Santé Wallon ou Réseau de Santé Bruxellois) n'entrent pas dans les définitions du secteur de la santé de l'annexe I.

Toutefois, ces types d'entités pourraient entrer dans les définitions du secteur Infrastructure numérique, par exemple en tant que fournisseurs de services de centres de données, fournisseurs de services d'informatique en nuage ou fournisseurs de services gérés. Pour cela, elles doivent être au moins une entreprise de taille moyenne. Ces types d'entités doivent donc vérifier si leurs activités correspondent aux définitions de ce secteur. Pour plus d'informations, voir les sections 1.22.7 et 1.22.8 ci-dessous.

La question de savoir si elles peuvent également relever du secteur de l'administration publique dépend de leur nature juridique. Le plus important est qu'il doit s'agir de personnes morales de droit publique. Pour plus d'informations, voir la section 2.1.

1.22.5.8. Les entités SOH tombent-elles dans le champ d'application de la loi NIS2 ? (Règlement 2024/1938)

Le règlement (UE) 2024/1938 du Parlement européen et du Conseil du 13 juin 2024 établit des mesures qui fixent des normes élevées de qualité et de sécurité pour l'ensemble des substances d'origine humaine (SOH) destinées à des applications humaines ainsi que pour les activités liées à ces substances. Le règlement s'applique activités liées aux SOH ayant une incidence directe sur la qualité, la sécurité ou l'efficacité de ces substances, telles que listées à l'article 2, 1), c), et impose des obligations aux entités nommées entités SOH.

Le considérant n°15 du règlement (UE) 2024/1938 explique que les SOH sont fréquemment transformées avant leur distribution ou, dans un contexte autologue, avant l'application humaine. La transformation peut avoir plusieurs objectifs tels que la séparation physique ou la purification en certains éléments, par exemple par centrifugation du sang pour préparer les concentrés érythrocytaires.

Dans le secteur de la santé, conformément à l'annexe 1, (5), de la loi NIS2, les entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de l'annexe I, section C, division 21, du NACE rev. 2 sont couverts, et la classe « Fabrication de produits pharmaceutiques de base » inclut entre autres la transformation de sang (« Processing of blood »).

Dès lors, les entités SOH qui transforment le sang peuvent être considérées comme tombant dans le champ d'application de la loi NIS2.

1.22.5.9. Les prestataires de soins de santé pour animaux tombent-ils dans le champ d'application de NIS2 ?

Conformément à l'article 3, § 1er, lu conjointement avec l'annexe 1, (5), de la loi NIS2, les « prestataires de soin de santé » au sens de l'article 3, point g), de la directive 2011/24/UE rentrent dans le champ d'application de la loi NIS2 lorsqu'ils sont qualifiés de moyennes entreprises au sens de l'article 2 de l'annexe de la recommandation 2003/361/CE ou qu'ils excèdent le plafond des moyennes entreprises.

Les considérants n°1 et 2 de la directive 2011/24/UE explique que la base légale de la directive 2011/24/UE a été choisie afin d'assurer un niveau élevé de protection de la santé humaine. De plus, les soins de santé, définis à l'article 3, a), de la directive 2011/24/UE, se réfèrent à la notion de patients, et l'article 3, h), de cette même directive, définit le patient comme « toute personne physique qui cherche à bénéficier ou bénéficie de soins de santé dans un État membre ».

Dès lors, la loi NIS2 ne s'appliquent aux prestataires de soins de santés pour animaux, tels que les vétérinaires.

1.22.6. Annexe I - 6. Eau potable

Ce secteur couvre les « fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive (UE) 2020/2184 [...], à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens ».

1.22.6.1. Quelles organisations peuvent être qualifiées de "fournisseurs et distributeurs d'eau destinée à la consommation humaine" ?

Les termes "eau destinée à la consommation humaine" sont définis à l'article 2, paragraphe 1, de la directive (UE) 2020/2184. Cela couvre :

« a) toutes les eaux, soit en l'état, soit après traitement, destinées à la boisson, à la cuisson, à la préparation d'aliments, ou à d'autres usages domestiques dans des lieux publics comme dans des lieux privés, quelle que soit leur origine et qu'elles soient fournies par un réseau de distribution, à partir d'un camion-citerne ou d'un bateau-citerne, ou en bouteilles ou en récipients, y compris les eaux de source;
b) toutes les eaux utilisées dans les entreprises du secteur alimentaire pour la fabrication, la transformation, la conservation ou la commercialisation de produits ou de substances destinés à la consommation humaine ; ».

L'annexe de la loi NIS2 ajoute qu'elle exclut les distributeurs pour lesquels la distribution d'eau destinée à la consommation humaine n'est qu'une partie non essentielle de leur activité générale de distribution d'autres produits et biens. Le mot « essentielle » pourrait être interprété comme suit : la distribution d'eau serait « essentielle » si le distributeur ne pouvait pas poursuivre efficacement ses activités sans distribuer de l'eau destinée à la consommation humaine.

Des exemples d'organisations incluses dans la définition sont ainsi les entreprises qui vendent de l'eau (en bouteille) et qui seraient incapables de poursuivre efficacement leurs activités si la vente de cette eau cessait. Voir également la section 1.22.12 sur la production et la distribution de denrées alimentaires.

1.22.7. Annexe I - 8. Infrastructure numérique

1.22.7.1. Qu'est-ce qu'un fournisseur de services d'informatique en nuage ?

Art. 8 de la loi NIS2 ; considérant 33 de la directive NIS2 ; analyse d'impact NIS2

L'article 8, 29° de la loi NIS2 définit un fournisseur de services d'informatique en nuage comme "un service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits."

Le considérant 33 de la directive NIS2 clarifie ce point : « *Les services d'informatique en nuage devraient couvrir les services numériques qui permettent la gestion sur demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits. Les ressources informatiques comprennent des ressources telles que les réseaux, les serveurs ou d'autres infrastructures, les systèmes d'exploitation, les logiciels, le stockage, les applications et les services* ».

Ce considérant fournit également les définitions suivantes :

- Le terme « accès large à distance » est utilisé pour décrire le fait que les capacités en nuage sont fournies sur le réseau et que l'accès à celles-ci se fait par des mécanismes encourageant le recours à des plateformes clients légères ou lourdes disparates, y compris les téléphones mobiles, les tablettes, les ordinateurs portables et les postes de travail.
- Le terme « modulable » renvoie aux ressources informatiques qui sont attribuées d'une manière souple par le fournisseur de services en nuage, indépendamment de la localisation géographique de ces ressources, pour gérer les fluctuations de la demande.
- Le terme « ensemble variable » est utilisé pour décrire les ressources informatiques qui sont mises à disposition et libérées en fonction de la demande pour pouvoir augmenter ou réduire rapidement les ressources disponibles en fonction de la charge de travail.
- L'expression « pouvant être partagées » est utilisée pour décrire les ressources informatiques qui sont mises à disposition de nombreux utilisateurs qui partagent un accès commun au service, le traitement étant effectué séparément pour chaque utilisateur bien que le service soit fourni à partir du même équipement électronique.
- Le terme « distribué » est utilisé pour décrire les ressources informatiques qui se trouvent sur des ordinateurs ou des appareils en réseau différents, qui communiquent et se coordonnent par transmission de messages.

« *Les modèles de services liés à l'informatique en nuage comprennent, entre autres, les infrastructures services (IaaS), les plateformes services (PaaS), les logiciels services (SaaS) et les réseaux services (NaaS). Les modèles de déploiement de l'informatique en nuage devraient inclure les modèles privés, communautaires, publics et hybrides en nuage. Les services d'informatique en nuage et les modèles de déploiement revêtent le même sens que celui des conditions de service et des modèles de déploiement définis dans la norme ISO/CEI 17788:2014. La capacité des utilisateurs de l'informatique en nuage de se fournir eux-mêmes unilatéralement en capacités informatiques, comme du temps de serveur ou du stockage en réseau, sans aucune intervention humaine de la part du fournisseur de service d'informatique en nuage, pourrait être décrite comme une gestion sur demande* » (considérant 33).

Dans l'analyse d'impact de 2020 sur la directive NIS2[3] , la Commission européenne a donné des exemples d'entreprises pouvant être qualifiées de fournisseurs de services d'informatique en nuage. Les fournisseurs de SaaS, IaaS et PaaS sont explicitement mentionnés :

- *"SaaS: instant computing infrastructure, provisioned and managed over the internet Examples: Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting*
- *IaaS: cloud computing model that provides virtualized computing resources over the internet. Examples: DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)*
- *PaaS: cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development. A PaaS provider hosts the hardware and software on its own infrastructure. Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift."*

Les éléments de la liste ci-dessus sont des exemples et ne sont donc pas exhaustifs.

Les fournisseurs de services d'informatique en nuage sont donc définis de manière large et comprennent les fournisseurs de SaaS, IaaS et PaaS.

La fourniture de services de maintenance, de déploiement et d'hébergement ne sont pas des critères inclus dans la définition et ne devrait dès lors pas entrer en ligne de compte dans la qualification d'une organisation de fournisseur de services d'informatique en nuage.

1.22.7.2. Qu'est-ce qu'un fournisseur de services de centres de données ?

Un fournisseur de services de centre de données est défini à l'article 8, 30° de la loi NIS2, comme un fournisseur « [d']un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental ».

Le considérant 35 de la directive NIS2 précise en outre : « *Il se peut que les services proposés par les fournisseurs de services de centre de données ne soient pas fournis sous la forme de service d'informatique en nuage. En conséquence, il se peut que les centres de données ne fassent pas partie d'une infrastructure d'informatique en nuage. Afin de gérer l'ensemble des risques qui menacent la sécurité des réseaux et des systèmes d'information, la présente directive devrait dès lors couvrir les fournisseurs de services de centres de données qui ne sont pas des services d'informatique en nuage*. [...]
Le terme «service de centre de données» ne devrait pas s'appliquer aux centres de données internes propres à une entreprise et exploités par l'entité concernée pour ses propres besoins. »

L'exception mentionnée à la fin du considérant ne s'applique pas si, au sein d'un groupe d'entreprises, l'une des entreprises fournit des services de centre de données à une autre entreprise.

[3] Commission staff working document. Impact assessment report accompanying the document "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148", SWD(2020) 345 final, 16 December 2020, part 2/3, en ligne sous https://ec.europa.eu/newsroom/dae/redirection/document/72178, page 45.

1.22.7.3. Que signifie exactement fournisseur de service DNS

Un fournisseur de service DNS est défini à l'article 8, 19°, de la loi NIS2 comme « *une entité qui fournit :*

a) des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l'internet; ou
b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines; »

La loi définit un "système de nom de domaine" ou "DNS" comme « *un système hiérarchique et distribué d'affectation de noms qui permet l'identification des services et des ressources internet, ce qui rend possible l'utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources* » (art. 8, 18°, loi NIS2).

Des organisations qui ne font que **revendre/enregistrer des noms de domaines de tiers**, **ne tombent quant à eux pas dans cette définition** mais sont qualifiées d'entités fournissant des services d'enregistrement de noms de domaine, définies comme « *un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire* » (art. 8, 21°, loi NIS2).

1.22.8. Annexe I - 9. Gestion des services TIC (B2B) : Qu'est-ce qu'un fournisseur de services gérés (helpdesk, B2B, etc.) ?

L'article 8, 38° de la loi NIS2 définit un fournisseur de services gérés (MSP) comme : « *une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance* ».

Il est important de noter que deux termes de cette définition sont également définis par la loi NIS2 ou d'autres instruments juridiques :

- « Produit TIC » : « *un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information (Règlement (UE) 2019/881, article 2, 12))* »;
- On entend par « réseau et systèmes d'information » :
    a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;
    b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; ou
    c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance.

La définition d'un fournisseur de services gérés est relativement large et comporte trois conditions différentes :

1) Soit l'installation, la gestion, l'exploitation ou l'entretien ;
2) De produits TIC, de réseaux, d'infrastructures, d'applications ou de tout autre réseau et système d'information ;
3) Via une assistance ou une administration active (sur place ou à distance).

Ces trois conditions doivent être cumulées pour entrer dans le champ de la définition. Les activités/tâches énumérées dans la définition ne s'excluent pas mutuellement. Plusieurs d'entre elles peuvent être effectuées par la même entité. Il n'y a pas d'autres conditions à prendre en compte pour vérifier si un organisme est un prestataire de services gérés. Par exemple, la dénomination "fournisseur de services gérés" ne doit pas être utilisée explicitement dans un contrat.

Voici quelques exemples de fournisseurs de services gérés :

- un service d'assistance (helpdesk) fournissant un soutien opérationnel aux utilisateurs d'un réseau ou d'une application par le biais d'une assistance à distance ;
- un développeur de logiciels qui fournit une assistance à distance pour l'installation et/ou la maintenance de ses applications ;
- un service de maintenance des réseaux d'un client et d'autres activités réalisées dans les locaux du client.

Pour les besoins de cette définition, ni le fait qu'une application TIC ou un produit TIC spécifique, gérée ou entretenue par un fournisseur de service, soit utiliser uniquement en interne par ce fournisseur du service dans le cadre de la fourniture d'un service à ses clients (ou à certains clients spécifiques), ni le fait que le client lui-même puisse utiliser une telle application, de manière temporaire ou indéfinie, n'est pertinent. Le critère qui importe est que l'application soit gérée ou entretenue dans le contexte de la provision de services par le fournisseur de services à ses clients.

De plus, ni la loi NIS2 ni la directive NIS2 ne différencie différents types d'entretien. En tant que tel, tout type d'entretien, dans le sens usuel du mot, est couvert.

À côté de la définition, le terme « interentreprises » (B2B) dans l'annexe I de la loi NIS2 doit être compris comme faisant référence à toutes les relations entre les prestataires de services et d'autres organisations/professionnels (entreprises, autorités publiques, artisans, professions, associations, entités au sein du même groupe, etc.), par opposition aux services fournis au grand public/aux particuliers (B2C) Le fait qu'une entité ne réalise pas de profit ou d'usage commercial ne semble pas être un critère d'exclusion de ce secteur.

L'interprétation des concepts d'« assistance » et d'« administration active » est également importante pour la définition d'un fournisseur de services gérés. Comme il est d'usage dans l'interprétation juridique des textes européens, s'il n'y a pas de définition dans l'instrument juridique concerné, les termes doivent être compris dans leur sens usuel.

L'interprétation de ces deux concepts pourrait ainsi être la suivante :

- Pour « assistance », le terme pourrait couvrir l'action de fournir un soutien. Dans le contexte d'un MSP, cela pourrait inclure l'aide aux clients lorsqu'ils rencontrent des problèmes ou lorsqu'ils ont besoin de conseils. Le terme serait donc de nature plus réactive. Il pourrait également inclure le dépannage, les meilleures pratiques, l'aide à l'installation et à la configuration, etc.

- Pour « administration active », le concept semble être intrinsèquement plus proactif. Dans le contexte d'un MSP, l'« administration » en particulier semble inclure la gestion et la supervision des systèmes, applications, réseaux, etc. d'un client. Elle pourrait également inclure la surveillance des systèmes, la maintenance et les mises à jour régulières, ainsi que la garantie générale du bon fonctionnement des réseaux et systèmes d'information concernés, sans que le client ne le demande nécessairement.

« À distance » signifie simplement que cela n'est pas fait dans les locaux du client (cela pourrait donc se faire depuis les bureaux d'une organisation).

Veuillez également vous référer à la section 1.16.7.

1.22.9. Annexe II - 1. Services postaux et d'expédition : Les services de coursiers et/ou la distribution de médicaments relèvent-ils de ce secteur ?

Ce secteur couvre les prestataires de services postaux tels que définis à l'article 2, point 1a), de la directive 97/67/CE, y compris les prestataires de services d'expédition. Cette directive contient plusieurs définitions :

- Prestataires de services postaux : « *une entreprise qui fournit un ou plusieurs services postaux* »
- Services postaux : « *des services qui consistent en la levée, le tri, l'acheminement et la distribution des envois postaux* »

Pour savoir si cela couvre également les services de messagerie, il faut également consulter la loi du 26 janvier 2018 relative aux services postaux (loi postale). Cette dernière contient les définitions suivantes :

- Envoi postal : « *un envoi portant une adresse sous la forme définitive dans laquelle il doit être acheminé par le prestataire de services postaux et dont le poids n'excède pas 31,5 kg* ».
- Colis postal ou colis : « *un envoi postal contenant des marchandises, avec ou sans valeur commerciale, autre qu'un envoi de correspondance, d'un poids maximal de 31,5 kg* »

La livraison d'un médicament par un coursier relève de la loi postale (et donc aussi de NIS2) si elle répond aux critères légaux, ce qui s'avère souvent être le cas au regard des critères définissant la notion de colis : poids inférieur à 31.5 kg, produit non exclu des services postaux par l'article 24, § 1er, 6° de l'arrêté royal du 14 mars 2022 relatif aux services postaux (il ne s'agit pas d'un stupéfiant ou d'un psychotrope, comme le flunitrazépam, et il ne s'agit pas d'un produit contrefait, etc.), le médicament doit être emballé, et l'emballage doit porter l'adresse du destinataire (ou un code permettant d'identifier le lieu de distribution).

La livraison de marchandises en vrac, non individualisées, ne répond pas à la définition d'un colis postal et ceux qui effectuent ces livraisons ne sont donc pas des prestataires de services postaux relevant de ce secteur de la loi NIS2.

1.22.10. Annexe II – 2. Gestion des déchets : Que couvre la notion de « déchets » ? Cela se réfère-t-il uniquement aux déchets ménagers ?

Ce secteur couvre les « [e]ntreprises exécutant des opérations de gestion des déchets au sens de l'article 3, point 9), de la directive 2008/98/CE du Parlement européen et du Conseil [...], à

l'exclusion des entreprises pour lesquelles la gestion des déchets n'est pas la principale activité économique ».

L'article 3, point 9), de la directive 2008/98/CE définit la « gestion des déchets » comme « *la collecte, le transport, la valorisation (y compris le tri), et l'élimination des déchets, y compris la surveillance de ces opérations ainsi que la surveillance des sites de décharge après leur fermeture et notamment les actions menées en tant que négociant ou courtier* ».

La notion de « déchets » est définie à l'article 3, point 1), de la même directive, comme « *toute substance ou tout objet dont le détenteur se défait ou dont il a l'intention ou l'obligation de se défaire* ».

Parmi les définitions de cette directive, se trouvent également :

- Valorisation : « *toute opération dont le résultat principal est que des déchets servent à des fins utiles en remplaçant d'autres matières qui auraient été utilisées à une fin particulière, ou que des déchets soient préparés pour être utilisés à cette fin, dans l'usine ou dans l'ensemble de l'économie. L'annexe II énumère une liste non exhaustive d'opérations de valorisation* » (art. 3, point 15))
- Recyclage : « *toute opération de valorisation par laquelle les déchets sont retraités en produits, matières ou substances aux fins de leur fonction initiale ou à d'autres fins. Cela inclut le retraitement des matières organiques, mais n'inclut pas la valorisation énergétique, la conversion pour l'utilisation comme combustible ou pour des opérations de remblayage* » (art. 3, point 17))

En conséquence, la gestion des déchets ne se limite pas à la collecte ou au transport de déchets ménagers. Cela inclut également les autres types de gestion des déchets, tel que le recyclage de métaux.

1.22.11. Annexe II - 3. Fabrication, production et distribution de produits chimiques

Ce secteur couvre les « Entreprises procédant à la fabrication de substances et à la distribution de substances ou de mélanges au sens de l'article 3, points 9 et 14, du règlement (CE) n° 1907/2006 du Parlement européen et du Conseil [(REACH)], et entreprises procédant à la production d'articles au sens de l'article 3, point 3), dudit règlement, à partir de substances ou de mélanges ».

1.22.11.1. Qu'entend-on par "substances" et "mélanges

Art. 3, points (1) & (2) Règlement REACH

Une **substance** est définie comme « *un élément chimique et ses composés à l'état naturel ou obtenus par un processus de fabrication, y compris tout additif nécessaire pour en préserver la stabilité et toute impureté résultant du processus mis en œuvre, mais à l'exclusion de tout solvant qui peut être séparé sans affecter la stabilité de la substance ou modifier sa composition* ».

Un **mélange** est défini comme « *un mélange ou une solution composés de deux substances ou plus* ».

En se référant aux entreprises qui fabriquent **des substances** et distribuent **des substances** ou des **mélanges** dans le secteur "fabrication, production et distribution de produits chimiques", la

loi NIS2 semble se référer à toutes les substances chimiques, qu'il s'agisse de produits chimiques industriels potentiellement dangereux ou de produits utilisés dans la vie quotidienne.

1.22.11.2. Quels types d'entités relèveraient du champ d'application de NIS2 en tant qu'entreprises fabriquant des substances et distribuant des substances ou des mélanges ?

Un fabricant au sens de REACH est « t*oute personne physique ou morale établie dans la Communauté qui fabrique une substance dans la Communauté* ». Les substances et les mélanges doivent être compris comme expliqué dans la section 1.22.11.1.

L'analyse d'impact de NIS2 fournit des aspects qualitatifs à l'appui de l'inclusion dans le champ d'application du framework NIS, faisant ainsi référence aux produits chimiques dangereux. Bien qu'absente du texte juridique, la référence aux produits chimiques dangereux dans l'analyse d'impact semble indiquer que l'intention des législateurs n'était pas d'inclure les entreprises qui fabriquent ou distribuent tout type d'élément chimique.

Il est également nécessaire d'examiner l'obligation d'enregistrement établie par le règlement REACH, car cette obligation est un instrument clé pour garantir l'objectif du règlement REACH. Comme le précisent les considérants (17) à (19) du règlement REACH, toutes les informations disponibles et pertinentes sur les substances telles quelles ou contenues dans des préparations ou des articles doivent être collectées afin de faciliter l'identification des propriétés dangereuses, et des recommandations sur les mesures de gestion des risques doivent être systématiquement transmises tout au long des chaînes d'approvisionnement, dans la mesure où cela est raisonnablement nécessaire, afin de prévenir les effets néfastes sur la santé humaine et sur l'environnement.

La responsabilité de la gestion des risques liés aux substances devrait incomber aux personnes physiques ou morales qui fabriquent, importent, mettent sur le marché ou utilisent ces substances. Par conséquent, les dispositions relatives à l'enregistrement devraient obliger les fabricants et les importateurs à produire des données sur les substances qu'ils fabriquent ou importent, à utiliser ces données pour évaluer les risques liés à ces substances et à élaborer et recommander des mesures appropriées de gestion des risques. Pour s'assurer qu'ils respectent effectivement ces obligations, ainsi que pour des raisons de transparence, l'enregistrement devrait les obliger à soumettre un dossier contenant toutes ces informations à l'Agence européenne des produits chimiques. Les substances enregistrées devraient pouvoir circuler sur le marché intérieur.

Le champ d'application de cette définition concerne ainsi principalement les entités concernées par l'obligation d'enregistrement au titre du règlement REACH.

Bien que d'autres organisations non soumises à l'obligation d'enregistrement puissent également être qualifiées d'entreprises **fabriquant des substances** et **distribuant des substances ou des mélanges** au sens de l'article 3, points (9) et (14) de REACH, il a été convenu au niveau de l'UE que ces entreprises ne sont pas les entités critiques visées dans le secteur chimique de la directive NIS2. Par conséquent, une approche de supervision moins stricte peut leur être appliquée.

En Belgique, les entités qui tombent sous la définition d'un fabricant ou d'un distributeur, mais qui ne sont pas tenues de s'enregistrer en vertu du règlement REACH, restent des entités NIS2 (essentielles ou importantes), mais sont soumises à une supervision moins stricte. En pratique,

elles doivent toujours s'enregistrer, notifier les incidents significatifs et appliquer des mesures de cybersécurité, mais l'utilisation d'un **niveau d'assurance inférieur du CyberFundamentals** (**CyFun®**) **Framework** (par exemple, Basic) pour se conformer à leurs obligations sera considéré comme proportionné. Cette solution tient compte de l'impact sociétal et économique plutôt limité de leurs services.

1.22.11.3. Un détaillant serait-il couvert par la distribution de substances ou de mélanges ?

En vertu de l'annexe II, point (3) de la loi NIS2, la définition du terme distribution de produits chimiques renvoie à l'article 3, point (14) du règlement (CE) 1907/2006 (règlement REACH).

Conformément à ce règlement, on entend par distributeur « *toute personne physique ou morale établie dans la Communauté, y compris un détaillant, qui n'exécute que des opérations de stockage et de mise sur le marché d'une substance, telle quelle ou contenue dans un mélange pour des tiers* ». Le point (12) de l'article 3 du règlement REACH définit la notion de "mise sur le marché" comme « *le fait de fournir un produit ou de le mettre à la disposition d'un tiers, à titre onéreux ou non* » et précise que « [t]oute importation est assimilée à une mise sur le marché ». La définition englobe la mise à disposition d'un produit, qu'il s'agisse ou non de la première fois que le produit est introduit sur le marché.

Par conséquent, un détaillant de substances ou de mélanges chimiques relève de cette définition du distributeur (à condition que les autres éléments d'applicabilité soient remplis).

1.22.11.4. Quels types d'entités relèveraient du champ d'application de NIS2 en tant qu'entreprises produisant des articles à partir de substances ou de mélanges ?

Les entreprises qui produisent des articles à partir de substances ou de mélanges, tels que définis à l'article 3, point (3), du règlement (CE) n° 1907/2006 (règlement REACH), entrent dans le champ d'application de la loi NIS2, lorsqu'elles sont considérées comme des entreprises de taille moyenne ou qu'elles dépassent les plafonds fixés pour les entreprises de taille moyenne.

L'article 3, point (4), du règlement REACH définit le terme **« producteur d'un article »** comme « *toute personne physique ou morale qui fabrique ou assemble un article dans la Communauté* ». Par conséquent, une entité est un producteur d'articles si elle produit des articles au sein de l'UE, indépendamment de la manière dont l'article est produit et de sa mise sur le marché.

Pour la définition des articles, la loi NIS2 se réfère à l'article 3, point (3), du règlement REACH. Selon l'article 3, point (3), du règlement REACH, on entend par **article «** *un objet auquel sont donnés, au cours du processus de fabrication, une forme, une surface ou un dessin particuliers qui sont plus déterminants pour sa fonction que sa composition chimique* ». Les vêtements, les revêtements de sol, les meubles, les bijoux, les journaux et les emballages en plastique sont des exemples d'articles.

Toutefois, pour déterminer dans quelle mesure **les producteurs d'articles** entrent dans le champ d'application de la loi NIS2, il faut tenir compte du fait que la première colonne de l'annexe II, point (3), de la loi NIS2 définit le secteur comme « la fabrication, la production et la distribution de produits chimiques » et fixe ainsi une limite au champ d'application de la troisième colonne de l'annexe II, point (3), dans la mesure où les produits chimiques doivent faire l'objet de l'activité

de fabrication, de production et de distribution des entités visées dans la troisième colonne de l'annexe II, point (3).

En outre, la loi NIS2 définit un secteur distinct pour la fabrication à l'annexe II, point (5), où elle limite le champ d'application aux fabricants de dispositifs médicaux, de dispositifs médicaux de diagnostic in vitro, de produits informatiques, de produits électroniques, de produits optiques, d'équipements électriques, de machines et d'équipements n.c.a., de véhicules à moteur, de remorques, de semi-remorques et d'autres équipements de transport. Étant donné que la définition des articles au titre du règlement REACH est très large, la spécification du champ d'application du secteur de la fabrication conformément à l'annexe II, point (5), serait vidée de son sens si toute entreprise effectuant la production d'articles tels que définis à l'article 3, point (3), du règlement REACH était considérée comme étant dans le champ d'application de l'annexe II, point (3), de la loi NIS2.

Par conséquent, les types d'entités visées dans la troisième colonne de l'annexe II, point 3, qui opèrent dans ce secteur en tant qu'entreprises produisant des articles, tels que définis à l'article 3, point 3, du règlement REACH, à partir de substances ou de mélanges, ne devraient pas couvrir les entités qui relèvent également du secteur de la « fabrication » conformément à l'annexe II, point 5.

Le champ d'application de cette définition concerne ainsi principalement les entités concernées par l'obligation d'enregistrement et de notification des substances contenues dans les articles au titre du règlement REACH.

En ce qui concerne les autres entités qui ne sont pas soumises à l'obligation d'enregistrement ou de notification des substances contenues dans des articles et qui pourraient également qualifiées d'entreprises produisant des articles à partir de substances ou de mélanges, à la lumière des considérations susmentionnées, il a été convenu au niveau de l'UE que ces entreprises ne sont pas les entités critiques visées par la directive NIS2 dans le secteur des produits chimiques. Par conséquent, une approche de supervision moins stricte peut leur être appliquée.

En Belgique, les entités qui répondent à la définition d'une entreprise effectuant la production d'articles à partir de substances ou de mélanges, mais qui ne sont pas tenues de s'enregistrer ou de notifier leurs substances au titre du règlement REACH, restent des entités NIS2 (essentielles et importantes), mais sont soumises à une supervision moins stricte. En pratique, elles doivent toujours s'enregistrer, signaler les incidents significatifs et appliquer des mesures de cybersécurité, mais l'utilisation d'un **niveau d'assurance inférieur du CyberFundamentals (CyFun®) Framework** (par exemple, Basic) pour se conformer à leurs obligations sera considéré comme proportionné. Cette solution tient compte de l'impact sociétal et économique plutôt limité de leurs services.

1.22.11.5. Les prestataires de services logistiques/transitaires tombent-ils dans le secteur chimique s'ils transportent des substances, mélanges ou articles ?

Un transitaire (ou commissionnaire de transport) / prestataire de services logistiques gère temporairement les infrastructures de stockage et les niveaux de stocks pendant le transport. Aucune substance n'est fabriquée par le transitaire.

Pour ce qui relève de la distribution de substances chimiques, le règlement REACH définit un « distributeur » comme suit : « *toute personne physique ou morale établie dans la Communauté,*

y compris un détaillant, qui n'exécute que des opérations de stockage et de mise sur le marché d'une substance, telle quelle ou contenue dans un mélange, pour des tiers ». Le règlement définit également la « *mise sur le marché* » *comme « le fait de fournir un produit ou de le mettre à la disposition d'un tiers, à titre onéreux ou non. Toute importation est assimilée à une mise sur le marché* ».

Selon les explications fournies par l'Agence européenne des produits chimiques sur son site web, « *vous êtes un distributeur* [selon REACH] *si vous vous approvisionnez d'une substance chimique ou d'un mélange au sein de l'EEE, la stockez et la mettez sur le marché pour une tierce personne (y compris sous votre propre marque sans modifier la composition chimique d'une quelconque manière)* » (traduction libre)[4].

En conséquence, le simple stockage temporaire de substances ou de mélanges chimiques pour des parties tierces ne suffit pas pour qualifier une organisation de « distributeur » s'il n'y a pas également un approvisionnement au sein de l'EEE et une mise sur le marché. Les transitaires/prestataires de services logistiques qui ne font que fournir le service mentionné ci-dessus ne tombent pas dans le secteur chimique sous NIS2.

1.22.12. Annexe II - 4. Production, transformation et distribution des denrées alimentaires

Ce secteur couvre les entreprises alimentaires telles que définies à l'article 3, point (2), du règlement (CE) n° 178/2002 du Parlement européen et du Conseil, qui exercent des activités de distribution en gros, ainsi que de de production et de transformation industrielles. Une entreprise du secteur alimentaire est définie comme « *toute entreprise publique ou privée assurant, dans un but lucratif ou non, des activités liées aux étapes de la production, de la transformation et de la distribution de denrées alimentaires* ».

L'annexe II de la loi NIS2 ajoute qu'elle ne couvre que les entreprises alimentaires « qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles ». L'accent est mis ici sur la distribution en gros, ce qui implique un facteur B2B (par opposition à B2C). Cet accent vise à exclure le commerce de détail du champ d'application. De même, l'expression "production et transformation industrielles" vise à limiter la production et la transformation à la production et à la transformation de denrées alimentaires à grande échelle.

Il suffit que l'entreprise alimentaire exerce l'une des activités suivantes pour relever de ce secteur : **la distribution en gros, la production industrielle ou la transformation industrielle de denrées alimentaires**. Ces éléments ne sont pas cumulatifs, mais constituent des conditions alternatives.

Comme expliqué à la section 1.8, il suffit que l'une de ces trois activités soit simplement une activité accessoire d'une organisation.

1.22.12.1. Que couvre la notion de « denrées alimentaires » ?

La définition au niveau européen de « denrées alimentaires », telle qu'utilisée sous NIS2, découle du règlement 178/2002. La régulation dispose ce qui suit :

[4] https://echa.europa.eu/distributor-communication-supply-chain-who

« *Aux fins du présent règlement, on entend par «denrée alimentaire» (ou «aliment»),* ***toute substance ou produit, transformé, partiellement transformé ou non transformé, destiné à être ingéré ou raisonnablement susceptible d'être ingéré par l'être humain****.*

Ce terme recouvre les boissons, les gommes à mâcher et toute substance, y compris l'eau, intégrée intentionnellement dans les denrées alimentaires au cours de leur fabrication, de leur préparation ou de leur traitement. Il inclut l'eau au point de conformité défini à l'article 6 de la directive 98/83/CE, sans préjudice des exigences des directives 80/778/CEE et 98/83/CE.

Le terme «denrée alimentaire» ne couvre pas*:*

a) les aliments pour animaux;
b) les animaux vivants à moins qu'ils ne soient préparés en vue de la consommation humaine;
c) les plantes avant leur récolte;
d) les médicaments au sens des directives 65/65/CEE et 92/73/CEE du Conseil;
e) les cosmétiques au sens de la directive 76/768/CEE du Conseil;
f) le tabac et les produits du tabac au sens de la directive 89/622/CEE du Conseil;
g) les stupéfiants et les substances psychotropes au sens de la Convention unique des Nations unies sur les stupéfiants de 1961 et de la Convention des Nations unies sur les substances psychotropes de 1971;
h) les résidus et contaminants;
i) *les dispositifs médicaux au sens du règlement (UE) 2017/745 du Parlement européen et du Conseil*. » (nous soulignons).

Une définition aussi large couvre les suppléments alimentaires, telles que les vitamines. Le site web officiel de l'Autorité européenne de sécurité des aliments fournit les informations suivantes :

« *Les compléments alimentaires sont des sources concentrées d'éléments nutritifs (minéraux ou vitamines par exemple) ou d'autres substances ayant un effet nutritionnel ou physiologique, commercialisés sous forme de « dose » (pilules, comprimés, gélules, liquides sous forme de doses mesurées). [...] Dans l'Union européenne, les compléments alimentaires sont réglementés en tant qu'aliments. [...] Conformément à la législation alimentaire générale de l'UE (règlement (CE) 178/2002), les compléments alimentaires sont considérés comme des produits alimentaires* »[5].

Etant donné que la définition de « denrées alimentaires » exclue les aliments pour animaux, les producteurs d'aliments pour animaux ne sont pas couverts par le secteur de la production, transformation et distribution des denrées alimentaires.

1.22.12.2. Que couvre la notion de « distribution en gros » ?

Etant donné que cette notion n'est pas spécifiquement définie par la loi NIS2 ou la directive NIS2, elle doit être comprise dans son sens usuel.

Une explication quant à la signification de « distribution en gros » peut être trouvée dans NACE Rev. 2, Partie IV, Section G (p. 221)[6] :

[5] https://www.efsa.europa.eu/fr/topics/topic/food-supplements
[6] https://ec.europa.eu/eurostat/fr/web/products-manuals-and-guidelines/-/ks-ra-07-015

« ***Le commerce de gros*** *consiste en la revente (vente sans transformation) d'articles et de produits neufs ou d'occasion à des détaillants, d'entreprise à entreprise, comme à des usagers industriels et commerciaux, à des collectivités et à des utilisateurs professionnels, ou à d'autres grossistes, ou à des intermédiaires qui achètent ces articles et des produits pour le compte de ces détaillants, ces usagers, ces collectivités etc., ou pour les leur vendre. Les principales activités incluses sont celles des marchands en gros, c'est-à-dire des grossistes qui prennent possession des marchandises qu'ils vendent, des négociants en gros, des dépositaires, des distributeurs industriels, des exportateurs, des importateurs et des coopératives d'achat, des succursales et des bureaux de vente (mais pas des magasins de détail) qui sont tenus par des unités de fabrication ou d'exploitation minière indépendamment de leurs usines ou mines dans le but de commercialiser leurs produits et qui ne se contentent pas de répondre à des commandes par expédition directe depuis les usines ou mines. Sont également inclus les courtiers, commissionnaires et agents ainsi que les centrales d'achat et les coopératives qui commercialisent des produits agricoles.*

Les marchands en gros se chargent fréquemment d'opérations telles que l'assemblage, le tri, le calibrage de marchandises en grandes quantités, le fractionnement, le reconditionnement, la redistribution en petites quantités, par exemple: de produits pharmaceutiques, l'entreposage, la réfrigération, la livraison et l'installation des marchandises, la promotion au bénéfice de leurs clients et la conception d'étiquettes.

La vente au détail *est la revente (vente sans transformation) au public de biens neufs ou d'occasion essentiellement destinés à la consommation des particuliers ou des ménages, par des magasins, des grands magasins, des comptoirs et des kiosques, des maisons de vente par correspondance, des colporteurs et des marchands ambulants, des coopératives de consommateurs, des maisons de vente aux enchères, etc. La plupart des détaillants prennent possession des marchandises qu'ils vendent mais certains agissent en tant qu'intermédiaires pour un commerçant principal et vendent en consignation ou sur la base de commissions* ».

1.22.12.3. Les supermarchés relèvent-ils du secteur alimentaire de l'annexe II, secteur 4 de NIS2 ?

Comme indiqué à la section 1.22.12, le secteur de la production, de la transformation et de la distribution de denrées alimentaires est axé sur la distribution en gros, la production industrielle ou la transformation industrielle de denrées alimentaires. Les supermarchés font en principe que du commerce de détail. En général, ils ne relèvent ainsi pas de l'annexe II, point 4.

Toutefois, lorsqu'une chaîne de supermarchés produit certains produits alimentaires à grande échelle (par exemple, sous son propre label), l'entité qui produit ces biens relève de la production industrielle et donc de ce secteur. Le fait que l'entité produise ces produits alimentaires dans le seul but d'approvisionner ses propres supermarchés ne change rien à la qualification dans ce secteur. Les autres entités du groupe de supermarchés feront partie de la chaîne d'approvisionnement de cette entité. Pour plus d'informations sur la chaîne d'approvisionnement, voir la section 3.14.

1.22.12.4. Les restaurants relèvent-ils de l'annexe II, secteur 4 de NIS2 ?

Comme mentionné dans la section 1.22.12, le secteur de la production, de la transformation et de la distribution de denrées alimentaires est axé sur la distribution en gros, la production industrielle ou la transformation industrielle de denrées alimentaires. En principe, les

restaurants n'entrent pas dans ces trois possibilités et ne relèvent donc pas du secteur 4 de l'annexe II de la loi NIS2.

Toutefois, lorsqu'une chaîne de restaurants produit certains produits alimentaires à grande échelle (par exemple, sous son propre label), l'entité qui produit ces biens relève de la production industrielle et donc de ce secteur. Le fait que l'entité produise ces produits alimentaires dans le seul but d'approvisionner ses propres restaurants ne change rien à la qualification dans ce secteur. Les autres entités d'un groupe de restaurants font partie de la chaîne d'approvisionnement de cette entité. Pour plus d'informations sur la chaîne d'approvisionnement, voir la section 3.14.

1.22.13. Annexe II - 5. Fabrication

1.22.13.1. Que signifie « fabrication » ?

Le mot fabrication doit être compris comme un *concept autonome du droit de l'Union européenne* (pour lequel le cadre juridique national n'en impacte pas l'interprétation). Cependant, en l'apparente absence de jurisprudence de la Cour de Justice de l'Union européenne qui définisse ce concept, il devrait être interprété conformément au sens habituel que ce terme revêt dans le langage courant, tout en prenant en compte le contexte dans lequel ce concept est utilisé ainsi que la finalité des règles au sein desquelles ce concept est mobilisé.

Le code NACE reste vague et NACE Rev. 2 ne fournit que des exemples (sans véritable définition) en page 114 (section C)[7] :

« *Cette section comprend* ***la transformation physique ou chimique de matériaux, substances ou composants en nouveaux produits****, même si ce critère ne suffit pas à définir l'industrie manufacturière (voir ci-dessous l'observation relative au recyclage des déchets). Les matériaux, substances ou composants transformés sont des matières premières produites par l'agriculture, la sylviculture, la pêche ou les industries extractives ainsi que des produits issus d'autres activités manufacturières. L'altération substantielle, la rénovation et la reconstruction de biens sont généralement considérées comme activités manufacturières.*

Le produit résultant d'une opération de transformation peut être fini, c'est-à-dire qu'il est prêt à être utilisé ou consommé ou il peut être semi-fini, c'est-à-dire qu'il entre dans la composition d'une autre fabrication. Par exemple, le produit du raffinage de l'alumine est la matière de base utilisée dans la production primaire d'aluminium; l'aluminium primaire est la matière de base pour la fabrication du fil d'aluminium; et le fil d'aluminium est la matière de base utilisée pour la fabrication de produits manufacturés à partir de ce fil.

La fabrication de composants spécialisés et de pièces, accessoires et fixations de machines et équipements est, en règle générale, rangée dans la même classe que la fabrication des machines et équipements auxquels les pièces et accessoires sont destinés. La fabrication de composants et pièces non spécialisés de machines et équipements, tels que moteurs, pistons, générateurs, assemblages électriques, valves, engrenages, roulements, est rangée dans la classe d'activité manufacturière appropriée, sans tenir compte des machines et équipements auxquels ces éléments pourraient être intégrés. Toutefois, la fabrication de composants spécialisés et

[7] https://ec.europa.eu/eurostat/fr/web/products-manuals-and-guidelines/-/ks-ra-07-015

d'accessoires par moulage ou extrusion de matières plastiques est comprise dans le groupe 22.2.

L'assemblage des composants de produits manufacturés est considéré comme une activité manufacturière. Celle-ci comprend l'assemblage des produits manufacturés à partir de composants fabriqués par l'unité qui l'exécute ou de composants Achetés [...] » (nous soulignons).

Plus d'informations sont disponibles en page 114 de NACE Rev. 2 (FR).

1.22.13.2. Que signifie « fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro » ?

Les entités qui fabriquent des dispositifs médicaux tels que définis à l'article 2, point 1), du règlement (UE) 2017/745 et les entités qui fabriquent des dispositifs médicaux de diagnostic in vitro tels que définis à l'article 2, point 2), du règlement (UE) 2017/746, à l'exception des entités qui fabriquent des dispositifs médicaux visés à l'annexe I, point 5, cinquième tiret, de la loi NIS2, relèvent de ce sous-secteur de l'annexe II. 5. Fabrication.

Un dispositif médical est défini comme suit : *« tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales précises suivantes:*

- *diagnostic, prévention, surveillance, prédiction, pronostic, traitement ou atténuation d'une maladie,*
- *diagnostic, contrôle, traitement, atténuation d'une blessure ou d'un handicap ou compensation de ceux-ci,*
- *investigation, remplacement ou modification d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique,*
- *communication d'informations au moyen d'un examen in vitro d'échantillons provenant du corps humain, y compris les dons d'organes, de sang et de tissus,*
- *et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens.*

Les produits ci-après sont également réputés être des dispositifs médicaux :

- *les dispositifs destinés à la maîtrise de la conception ou à l'assistance à celle-ci;*
- *les produits spécifiquement destinés au nettoyage, à la désinfection ou à la stérilisation des dispositifs visés à l'article 1er, paragraphe 4, et de ceux visés au premier alinéa du présent point ».*

Un dispositif médical *in vitro* est défini comme suit : « *tout dispositif médical qui consiste en un réactif, un produit réactif, un matériau d'étalonnage, un matériau de contrôle, une trousse, un instrument, un appareil, un équipement, un logiciel ou un système, utilisé seul ou en association, destiné par le fabricant à être utilisé in vitro dans l'examen d'échantillons provenant du corps humain, y compris les dons de sang et de tissus, uniquement ou principalement dans le but de fournir des informations sur un ou plusieurs des éléments suivants :*

a) concernant un processus ou état physiologique ou pathologique ;
b) concernant des déficiences congénitales physiques ou mentales ;
c) concernant la prédisposition à une affection ou à une maladie ;

d) permettant de déterminer si un traitement donné est sûr pour des receveurs potentiels et compatible avec eux ;
e) permettant de prévoir la réponse ou les réactions à un traitement ;
f) permettant de définir ou de suivre des mesures thérapeutiques.

Les récipients pour échantillons sont également réputés être des dispositifs médicaux de diagnostic in vitro; »

En outre, les entités qui fabriquent des dispositifs médicaux considérés comme essentiels en cas d'urgence de santé publique peuvent également relever de l'annexe I, point 5 "Santé". Pour plus d'informations, voir la section 1.22.5.5.

Outre la situation décrite ci-dessus, la plupart des entités fabriquant des dispositifs médicaux font partie de la chaîne d'approvisionnement d'entités NIS2 (par exemple, les prestataires de soins de santé de l'annexe I, secteur 5). Les entités couvertes par la loi NIS2 doivent prendre des mesures appropriées et proportionnées pour sécuriser leur réseau et leurs systèmes d'information. L'une de ces mesures 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. Pour plus d'informations sur les obligations relatives à la chaîne d'approvisionnement, voir la section 3.14).

1.22.14. Annexe II - 7. Recherche

Les organismes de recherche tombent sous l'annexe II, 7. Recherche et sont définis comme « une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement ».

1.22.14.1. Les organismes de recherche couvrent-ils également les sponsors ?

Les organismes de recherche relèvent de l'annexe II, 7. Recherche et sont définis comme indiqué ci-dessus.

La directive NIS2 fournit un contexte à cette définition dans son considérant 36 :

> *Les activités de recherche jouent un rôle clé dans le développement de nouveaux produits et processus. Nombre de ces activités sont menées par des entités qui partagent, diffusent ou exploitent les résultats de leurs recherches à des fins commerciales. Ces entités peuvent donc être des acteurs importants dans les chaînes de valeur, ce qui fait de la sécurité de leurs réseaux et systèmes d'information une partie intégrante de la cybersécurité globale du marché intérieur. L'expression «organismes de recherche» devrait s'entendre comme incluant les entités qui concentrent l'essentiel de leurs activités sur la conduite de la recherche appliquée ou du développement expérimental, au sens du Manuel de Frascati 2015 de l'Organisation de coopération et de développement économiques: Lignes directrices pour le recueil et la communication des données sur la recherche et le développement expérimental, en vue d'exploiter leurs résultats à des fins commerciales, telles que la fabrication ou la mise au point d'un produit ou d'un processus, la fourniture d'un service, ou la commercialisation d'un produit, d'un processus ou d'un service.*

Selon le manuel de Frascati (2015), la recherche appliquée est une investigation originale entreprise en vue d'acquérir de nouvelles connaissances, et le développement expérimental est un travail systématique, s'appuyant sur les connaissances acquises par la recherche et l'expérience pratique et produisant des connaissances supplémentaires, qui vise à produire de nouveaux produits ou processus ou à améliorer les produits ou processus existants.

Cela étant, la directive NIS2 délimite ces définitions en introduisant la condition supplémentaire que les activités de recherche doivent être menées en vue d'exploiter les résultats de cette recherche à des fins commerciales, telles que la fabrication ou la mise au point d'un produit ou d'un processus, la fourniture d'un service, ou la commercialisation d'un produit, d'un processus ou d'un service.

La finalité commerciale est définie au sens large comme englobant *la fabrication ou la mise au point d'un produit ou d'un processus, la fourniture d'un service, ou la commercialisation*. Si l'objectif des activités de recherche est de produire un nouveau produit, la recherche a une finalité commerciale.

Les services fournis par les sponsors ne comprennent pas les activités de recherche appliquée ou de développement expérimental, mais seulement le financement d'activités de recherche par une autre organisation. Par conséquent, ces organisations qui ne fournissent pas de services NIS2 proprement dits, n'entrent pas dans le champ d'application de la loi NIS2.

1.22.14.2. Les établissements d'enseignement sont-ils des "organismes de recherche" ?

Comme l'indique la définition mentionnée à la section 1.22.14, les établissements d'enseignement sont explicitement exclus. Cependant, ces derniers pourraient toujours tomber sous NIS2 s'ils font partie du secteur public. Pour plus d'informations, voir la section 2.7.

2. Secteur public

2.1. Quel est le champ d'application de la loi pour le secteur public ?

Art. 8, 34° et Annexe I, secteur 10 (Administration publique) loi NIS2

Art. 8, 34° de la loi définit une « entité de l'administration publique » comme une autorité administrative visée à l'article 14, § 1er, alinéa 1er, des lois coordonnées sur le Conseil d'État qui satisfait aux critères suivants :

a) elle n'a pas de caractère industriel ou commercial;
b) elle n'exerce pas à titre principal une activité énumérée dans la colonne type d'entité d'un autre secteur ou sous-secteur de l'une des annexes de la loi;
c) elle n'est pas une personne morale de droit privé.

Pour la définition d'une entité de l'administration publique, l'article 6, 35) de la directive précise que la notion doit être reconnue comme telle conformément au droit national, à l'exclusion de la justice, des parlements et des banques centrales. Ainsi, il a été choisi de faire référence à des notions existantes en droit belge qui couvrent les entités concernées afin de ne pas multiplier l'application de notions différentes.

En l'occurrence, la définition reprend la notion d'autorité administrative visée à l'article 14, §1er, alinéa 1er, des lois coordonnées du 12 janvier 1973 sur le Conseil d'État (voir section 2.2), à laquelle sont rajoutés les critères de ne pas avoir de caractère industriel ou commercial, de ne pas exercer à titre principal une activité relevant de l'un des autres secteurs ou sous-secteurs repris dans les annexes de la loi et de ne pas être une personne morale de droit privé.

Il faut combiner à cette définition les catégories d'entités type reprises à l'annexe I, secteur 10 (Administration publique) :

- Entités de l'administration publique qui dépendent de l'Etat fédéral ;
- Entités de l'administration publique qui dépendent des entités fédérées, identifiés conformément à l'article 11, § 2 de la loi ;
- Les zones de secours au sens de l'article 14 de la loi du 15 mai 2007 relative à la sécurité civile ou le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale créé par l'ordonnance du 19 juillet 1990 portant création d'un Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale.

La notion de dépendance (qui « dépendent de ») est inspirée de l'article 5 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Elle permet d'englober notamment des entités qui font partie d'un niveau de pouvoir car elles ont été créées par ces autorités publiques, leur activité est financée majoritairement par ces autorités publiques, la gestion est soumise à un contrôle de ces autorités publiques, ou encore dont plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités.

Comme l'indique la définition de l'art. 8, 34°, une entité publique qui fournit à titre principal un service figurant dans un autre secteur ou sous-secteur de l'une des annexes de la loi (par exemple, une intercommunale active dans le secteur de l'Energie ou de l'eau potable, un hôpital

public, un organisme public fournisseur de service TIC, etc.) relève alors des règles de ce secteur et non du secteur de l'administration publique.

Voir également les sections suivantes de ce chapitre pour plus de détails.

2.2. Qu'est-ce qu'une "autorité administrative" ?

Selon la jurisprudence du Conseil d'Etat, une personne morale de droit public est automatiquement qualifiée d'autorité administrative au sens de l'article 14, § 1er des lois coordonnées du 12 janvier 1973 sur le Conseil d'Etat, si elle exerce des compétences relevant du pouvoir exécutif.

Pour déterminer si une personne morale de droit privé peut être qualifiée d'autorité administrative, les critères suivants sont appliqués :

1) créée ou approuvée par les autorités fédérales, fédérées, provinciales ou municipales ;
2) chargée d'un service public ;
3) ne fait pas partie du pouvoir judiciaire ou législatif ;
4) son opération est déterminée et contrôlée par les pouvoirs publics ;
5) elle peut prendre des décisions obligatoires à l'égard de tiers.

Ces cinq critères doivent être cumulativement rencontrés pour qu'une personne morale de droit privée soit qualifiée d'autorité administrative.

2.3. Qu'en est-il des organisations du secteur public actives dans un autre secteur NIS2 (comme un hôpital public, une intercommunale ou une maison de repos publique) ?

Comme l'indique la définition de l'art. 8, 34° (voir section 2.1), une entité publique qui fournit principalement un service énuméré dans un autre secteur ou sous-secteur d'une des annexes de la loi **est soumise aux règles de ce secteur et non à celles du secteur de l'administration publique.**

Cela inclus par exemple :

- une intercommunale fournissant du gaz et/ou de l'électricité ;
- une intercommunale qui fournit de l'eau potable ;
- une intercommunale de gestion des déchets ;
- un hôpital public ;
- une maison de repos publique ;
- un organisme public de services TIC ;
- un service postal public ;
- un aéroport public ;
- etc.

Si ces exemples font partie d'une administration publique locale (même entité juridique), l'ensemble de l'organisation tombera dans le champ d'application de la loi dans le (les) secteur(s) concerné(s) uniquement. Les administrations publiques locales ne font en effet pas partie du

secteur de l'administration publique à l'annexe I de la loi NIS2. Voir la section 2.4 ci-dessous pour plus d'informations sur les administrations publiques locales.

Si une administration publique qui dépend de l'Etat fédéral ou des entités fédérées fournit également un service (pas à titre principal) couvert par un autre secteur NIS2 (même entité juridique), elle tombera dans les deux secteurs et devra appliquer les obligations les plus strictes de ces secteurs (et donc s'enregistrer dans les deux secteurs). Lorsque les administrations publiques qui dépendent des entités fédérées tombent dans plusieurs secteurs, elles ne doivent pas attendre d'être identifiées pour appliquer les obligations découlant de la loi NIS2 et s'enregistrer.

2.4. Est-ce que les administrations publiques locales entrent dans le champ d'application de la loi ?

Art. 8, 34° Annexe I, secteur 10 (Administration publique) loi NIS2

Les administrations/entités publiques locales (communes, provinces, intercommunales, CPAS, régies, etc.) **ne sont pas automatiquement soumises aux exigences de la loi NIS2**. En effet, elles ne sont pas explicitement listées dans les annexes de la loi NIS2 dans le secteur public.

Même si les administrations publiques locales telles que celles énumérées ci-dessus répondent à la définition de l'article 8, 34° (voir section 2.1), elles ne dépendent ni de l'Etat fédéral, ni des entités fédérées.

Conformément au principe de l'autonomie locale consacré par l'article 162 de la Constitution, les administrations locales ne doivent pas être considérées, malgré l'exercice d'un contrôle de tutelle ou de leur financement, comme des administrations publiques qui dépendent des entités fédérées ou de l'Etat fédéral au sens de l'annexe I de la loi NIS2.

Toutefois, ces entités locales entrent dans le champ d'application de la loi NIS2 lorsqu'elles fournissent un service figurant à l'annexe I ou II de la loi (autre que dans le secteur Administration publique) et qu'elles sont au moins qualifiées d'entreprises de taille moyenne. Leur qualification d'entité essentielle et importante au sens de la loi dépend alors du service fourni et de leur taille (voir également la section 1.5).

Les entités publiques locales peuvent également faire l'objet d'une identification par le biais de l'article 11, § 1 (désignation par l'autorité nationale de cybersécurité - CCB), moyennant le respect des procédures de concertation prévues par l'article 11, § 3. L'initiative d'une telle identification pourrait être effectuée à la demande de l'autorité nationale de cybersécurité, de l'entité concernée ou encore d'une Région.

2.5. Les entités publiques régionales ou communautaires sont-elles soumises aux obligations de la loi ?

Art. 11, §2-3 et Annexe I, secteur 10 (Administration publique) loi NIS2

Les administrations publiques régionales et communautaires font partie du secteur de l'administration publique couvert par la loi NIS2, où elles sont explicitement mentionnées comme des "entités de l'administration publique dépendant d'entités fédérées". Cela inclut notamment les administrations publiques fédérées, mais aussi diverses entités publiques créées, financées ou gérées d'une autre manière par le niveau fédéré, à condition qu'elles soient conformes à la définition de l'article 8, 34° de la loi NIS2 (voir section 2.1).

Néanmoins, une procédure d'identification formelle doit être réalisée au préalable par l'autorité nationale de cybersécurité (CCB). Il s'agit d'évaluer, sur base d'une analyse des risques, les entités qui fournissent des services dont la perturbation pourrait avoir un impact important sur des activités sociétales ou économiques critiques.

Conformément à l'article 11, § 2 et 3 de la loi NIS2, cette identification s'effectue en concertation avec les entités publiques concernés et les gouvernements des entités fédérées. A l'issue de cette procédure, l'entité publique régionale ou communautaire peut être désignée comme une entité essentielle ou une entité importante.

Si une entité de l'administration publique qui dépend d'une entité fédérée est également active dans un autre secteur de la loi NIS2, le processus d'identification décrit ci-dessus n'est pas nécessaire pour que la loi NIS2 s'applique (voir également la section 2.3).

Voir la section 2.8 pour des informations sur l'enregistrement.

2.6. Quel personnel dois-je prendre en compte pour calculer la taille de mon entité de l'administration publique (locale) ?

Tant qu'elle n'est pas formellement identifiée comme une entité NIS2 et en fonction des services fournis, une administration publique fédérée ou une administration publique locale peut être amenée à calculer sa taille.

Les entités publiques doivent prendre en compte l'ensemble du personnel travaillant **au sein de l'entité juridique** de ladite entité publique. Selon le guide de l'utilisateur sur la définition d'une PME de la Commission européenne, *« [l]e critère des effectifs couvre le personnel employé à temps plein, à temps partiel ou de manière saisonnière et inclut les catégories suivantes:*

- *des salariés ;*
- *les personnes travaillant pour l'entreprise auprès de laquelle elles ont été détachées et qui sont assimilées à des salariés au regard du droit national (il peut aussi s'agir de personnel temporaire ou intérimaire)* ;
- *les propriétaires exploitants ;*
- *les associés exerçant une activité régulière dans l'entreprise et bénéficiant d'avantages financiers de la part de l'entreprise ».*

Cela n'inclut pas :

- *« les apprentis ou les étudiants en formation professionnelle bénéficiant d'un contrat d'apprentissage ou de formation professionnelle ;*
- *les salariés en congé de maternité ou en congé parental ».*

L'effectif de base nécessaire au calcul du size-cap (voir section 1.5) est exprimé en UTA (unités de travail annuel). Le nombre de personnes ayant travaillé dans l'entreprise considérée ou pour le compte de cette entreprise à temps plein pendant toute l'année considérée compte pour une unité. Le travail des personnes n'ayant pas travaillé toute l'année, ou ayant travaillé à temps partiel, quelle que soit sa durée, ou le travail saisonnier, est compté comme fractions d'UTA.

Dans ce contexte, une personne qui a travaillé dans le cadre d'un contrat à durée déterminée ou d'une mission pendant une partie de l'année seulement doit être comptabilisée comme une fraction d'unité sur la base du nombre de jours travaillés au cours de l'année précédente (divisé par le nombre de jours de travail au cours de l'année).

Le personnel mis à disposition par un CPAS pour travailler dans une organisation en vertu de l'article 60, § 7 de la loi organique du 8 juillet 1976 relative aux CPAS est inclus dans le calcul de l'effectif en tant qu'intérimaire.

Il est important de noter que les dispositions relatives à la consolidation des données des entreprises partenaires et liées de la recommandation 2003/361/CE **ne s'appliquent pas** aux administrations publiques. Cela signifie que seules les données de l'administration elle-même doivent être prises en compte. Si, par exemple, une commune qui fournit des services d'eau potable possède également une école, elle ne doit prendre en compte les données de l'école que si celle-ci fait partie de la même entité juridique que la commune.

2.7. Est-ce qu'un établissement d'enseignement tombe dans le champ d'application de la loi ?

Annexes I et II & art. 8, 34° loi NIS2

D'une part, le secteur de l'éducation ne figure pas explicitement dans les annexes I et II de la loi NIS2. Les établissements d'enseignement privé n'entrent donc pas explicitement dans le champ d'application de la loi NIS2.

En revanche, les établissements **publics** d'enseignement, tels que les universités publiques ou les écoles secondaires publiques, **pourraient** être inclus dans la définition d'une « entité de l'administration publique ». Pour ce faire, ils doivent :

- répondre au critère de taille (voir section 1.5) ;
- être établi en Belgique (voir section 1.14) ;
- répondre à la définition d'une entité de l'administration publique dans l'article 8 de la loi NIS2 (voir sections 2.1 et 2.2) ;
- dépendre de l'État fédéral ou des entités fédérées (voir section 2.1) ; et
- s'ils dépendent des entités fédérées : être identifiés conformément à l'art. 11, § 2 (voir section 2.5).

En outre, un établissement d'enseignement public ou privé pourrait également être qualifié de « prestataire de soins de santé » (voir section 1.22.5.1) au sens de l'annexe I de la loi NIS2 si, par exemple, il gère un hôpital universitaire qui fait partie de la même entité juridique (si ce n'est pas le cas, seul l'hôpital entrera dans le champ d'application si le size-cap est atteint) ou si

l'établissement d'enseignement offre des soins particuliers à ses étudiants, ce qui pourrait correspondre à la définition de prestataire de soin de santé. Un tel établissement pourrait aussi être qualifié de producteur d'électricité, par exemple s'il a des panneaux solaires sur le toit de son établissement (voir la section 1.22.1.1).

Les établissements d'enseignement publics qui rentrent déjà dans le champ d'application de NIS2 dans un autre secteur ne doivent pas être identifiés au travers de l'article 11. § 2, de la loi NIS2.

2.8. Quand et comment les entités du secteur public doivent-elles s'enregistrer ?

Selon les entités concernées du secteur public, différents régimes s'appliquent :

- Pour les entités publiques qui dépendent de l'Etat fédéral, le délai normal d'enregistrement (jusqu'au 18 mars 2025) s'applique depuis l'entrée en vigueur de la loi.
- Pour les entités publiques qui dépendent d'entités fédérées, le délai d'enregistrement est égal à 5 mois après que l'entité concernée a été formellement identifiée par le CCB (lettre de notification).
- Pour les zones de secours, le délai d'enregistrement normal (jusqu'au 18 mars 2025) s'applique depuis l'entrée en vigueur de la loi.

Il est important de noter que ces délais ne s'appliquent que si l'organisation concernée relève uniquement du secteur de l'administration publique. Si elle relève également d'un autre secteur, des délais plus stricts peuvent s'appliquer.

L'enregistrement se fait sur notre plateforme Safeonweb@Work (voir section 3.13.1).

2.9. Les sanctions s'appliquent-elles aux entités du secteur de l'administration publique ? Qu'en est-il si l'organisation appartient également à un autre secteur ?

Selon l'article 62 de la loi NIS2, toutes les mesures administratives indiquées dans la section 4.18.1 peuvent être prises en réponse à une violation de la loi par les entités du secteur de l'administration publique. Cependant, ces entités ne peuvent pas être soumises aux amendes administratives indiquées à la section 4.17 et à certaines mesures administratives spécifiques indiquées à la section 4.18.2.

Ces affirmations sont également valables si une entité de l'administration publique appartient à la fois au secteur de l'administration publique et à un autre secteur NIS2 (le régime le plus favorable l'emporte sur l'autre).

Toutefois, une entité publique qui exerce principalement une activité figurant dans la colonne des types d'entités d'un autre secteur ou sous-secteur peut faire l'objet d'amendes administratives et de mesures administratives spécifiques (parce qu'elle ne répond pas à la définition d'une entité de l'administration publique).

2.10. Quel cadre normatif les administrations publiques devraient-elles utiliser pour implémenter leurs mesures de cybersécurité ?

Le CCB recommande officiellement aux administrations publiques d'utiliser le CyFun® (*CyberFundamentals Framework*) dans sa directive 01/2024 (FR) et 01/2025 (FR).

Toutes les directives du CCB sont disponibles (en FR et NL) sur son site web : https://ccb.belgium.be/regulation.

2.11. Comment les deux régimes de responsabilités NIS2 s'appliquent-ils dans le secteur de l'administration publique ?

La loi NIS2 explicite, dans ses articles 31, § 1er, et 61, alinéa 2, que ces dispositions en matière de responsabilités n'affectent pas, ne portent pas préjudice aux règles préexistantes en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

La loi du 10 février 2003 relative à la responsabilité des et pour les membres du personnel au service des personnes publiques établit les conditions selon lesquelles les fonctionnaires peuvent être tenus responsables, tout en leur fournissant une protection pour certaines de leurs actions au travers de régimes de limitation ou d'exclusion de responsabilité.

Pour ce qui relève de la responsabilité personnelle de personnes physiques responsables de, ou agissant en tant que représentantes d'entités NIS2 du secteur de l'administration publique (« fonction managériale »), leur statut légal doit être examiné :

- soit elles sont des agents statutaires subordonnés à l'entité publique, auquel cas elles bénéficient de la protection fournit par l'article 2 de la loi du 10 février 2003 précitée pour les fautes qui ne sont pas des fautes lourdes ;
- soit elles sont des agents contractuels, auquel cas elles sont couvertes par l'article 18 de la loi du 3 juillet 1978 relative aux contrats de travail ;
- soit elles sont des représentants sans relation de subordination à la personnalité juridique régie par le droit public.

Pour les personnes couvertes par la loi du 10 février 2003 précitée, la responsabilité individuelle visée à l'article 61, alinéa 1er, sera donc applicable aux managers en cas de dol, de faute lourde, ou de faute mineure avec un caractère habituel.

2.12. A quels organes d'une commune les deux régimes de responsabilités s'appliquent-ils ?

La présente section n'est pertinente que pour les communes qui entrent dans le champ d'application de NIS2 (voir la section 2.4).

Selon les différentes législations existantes en Belgique (spécificités relatives à la Flandre, la Wallonie, Bruxelles-capitale, et la Communauté germanophone), différents organes au sein des communes ont différentes compétences, tâches et responsabilités.

Il ressort des interactions que le CCB a eu avec les représentants des parties prenantes locales, qu'aucun organe spécifique ne correspond aux deux régimes de responsabilité établis par la loi NIS2. En effet, la cybersécurité n'est pas une matière spécifiquement dévolue à un organe en particulier (Conseil, Collège, Bourgmestre ou administration générale avec Directeur), la cybersécurité s'étend à travers les compétences de plusieurs organes.

Par exemple :

- La compétence du Conseil (Collège pour la Communauté germanophone) d'approuver le cadre général du système de contrôle interne organisationnel établi et supervisé par le Directeur général ;
- La compétence générale du Conseil en matière d'intérêt communal, en l'absence d'attribution explicite à un autre organe ;
- La compétence du Bourgmestre d'assurer l'exécution des lois, décrets, règlements et décisions établis par l'Etat, les Régions, les Communautés, le Conseil provincial et le Collège provincial, à moins que cette responsabilité soit formellement dévolue au Collège communal ou au Conseil communal ;
- La compétence du Conseil en matière d'approbation des critères selon lesquels des services et des fournitures peuvent être commandés (qui peuvent inclure des mesures de cybersécurité).

Etant donné une telle disparité de compétences, chaque commune concernée par NIS2 devrait vérifier en interne, selon sa situation concrète, quels organes sont susceptibles de remplir les conditions du régime de responsabilité établi par la loi.

Une interprétation possible du régime de responsabilité serait que le Bourgmestre est responsable selon l'article 61 de la loi NIS2, étant donné son rôle de représentant de la Commune ainsi que sa tâche de superviser l'exécution de la législation fédérale, et que le Conseil détient la responsabilité et l'obligation visées à l'article 31 de la loi NIS2, étant donné son rôle de supervision et d'approbation du système de contrôle organisationnel (où la plupart des mesures de cybersécurité seraient implémentées).

Il devrait être noter dans tous les cas que les régimes de responsabilités s'appliquent sans préjudice des règles en matière de responsabilité du secteur public (voir notamment la section 2.11).

3. Obligations

3.1. Quelles sont les obligations légales pour les entités concernées ?

Plusieurs obligations à charge des entités essentielles et importantes découlent de la loi NIS2 :

- l'adoption de mesures de cybersécurité adéquates ;
- la notification des incidents significatifs dans les délais ;
- l'enregistrement auprès des autorités compétentes (plateforme du CCB pour la plupart des entités) ;
- la formation des membres des organes de direction (section 3.9.) ;
- la réalisation d'évaluations périodiques de la conformité (obligatoires pour les entités essentielles et volontaire pour les entités importantes) ;
- le partage d'informations et la collaboration avec les autorités compétentes.

Ces différentes obligations sont expliquées dans les sections suivantes.

3.2. Quelles sont les obligations en matière de mesures de cybersécurité ?

Art. 30, 31 et 42 loi NIS2

Les entités essentielles et importantes doivent prendre les mesures (techniques, opérationnelles et organisationnelles) appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

Il est important de souligner que, contrairement à la loi NIS1, **le champ d'application de la loi NIS2 porte sur l'ensemble de l'entité concernée** et non uniquement sur ses activités reprises dans les annexes de la loi.

Pour faciliter la mise en œuvre pratique de ces mesures de cybersécurité, le CCB a d'ores et déjà développé et mis gratuitement à la disposition des entités concernées un référentiel : le « Cyberfundamentals Framework » (CyFun®) avec différents niveaux et un outil d'analyse permettant de déterminer le niveau le plus adéquat à suivre. La loi et son arrêté d'exécution offriront aux entités essentielles et importantes qui décideront d'utiliser le référentiel CyFun® ou la norme internationale ISO/IEC 27001 (avec le champ d'application conforme à NIS2 – à savoir tous les réseaux et systèmes d'information), une **présomption de conformité** au regard des mesures de sécurité.

Les mesures minimales contenues dans la loi sont fondées sur une approche « tous risques » qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et portent au moins sur :

1. les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;
2. la gestion des incidents;

3. la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises;
4. la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs;
5. la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités;
6. des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;
7. les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité;
8. des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement;
9. la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;
10. l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins;
11. une politique de divulgation coordonnée des vulnérabilités.

Les mesures devant être adoptées par les entités essentielles et importantes doivent être **appropriées et proportionnées**. Sur ce point, il est important de préciser que pour éviter que la charge financière et administrative imposée aux entités essentielles et importantes ne soit disproportionnée, il convient que les mesures de gestion des risques en matière de cybersécurité soient **proportionnées aux risques** auxquels le réseau et le système d'information concernés sont exposés. À cet égard, les entités prennent notamment en compte **l'état de l'art** de ces mesures ainsi que, s'il y a lieu, des **normes** européennes ou internationales pertinentes, et du **coût de mise en œuvre** de ces mesures.

Il convient de noter que certaines entités NIS2 doivent suivre le règlement d'exécution 2024/2690 de la Commission du 17 octobre 2024 détaillant les exigences techniques et méthodologiques des mesures de gestion des risques cybersécurité (voir section 5.1).

3.3. Quelles sont les obligations en matière de notification des incidents ?

Plus d'informations sur la notification d'incidents sont disponibles sur notre site web et dans notre guide de notification des incidents.

3.3.1. Règles générales

Art. 8, 5° et 57° ; 34 et 35 loi NIS2

Un incident est défini par la loi comme *« un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles »*.

En cas **d'incident significatif**, l'entité doit le notifier au CSIRT national (CCB) et, dans certains cas, aux destinataires de leurs services.

Consultez notre guide de notification des incidents pour plus de détails sur les incidents "significatifs".

La notification se fait en plusieurs étapes (voir section 3.3.4.) : d'abord une alerte précoce dans les 24 heures qui suivent la découverte de l'incident (*early warning*), puis une notification d'incident en bonne et due forme dans les 72 heures suivants la découverte de l'incident (*initial assessment of the incident*), et enfin un rapport final au plus tard 1 mois après la notification d'incident (*final report*). Entre temps, le CSIRT national peut requérir des rapports intermédiaires.

Le CCB a élaboré un guide complet indiquant quand et comment un incident doit être notifié. La dernière version du guide est disponible sur notre site web ou via ce lien direct : https://ccb.belgium.be/fr/open-media/688/download.

Les incidents NIS2 peuvent être signalés au CCB via sa plateforme : http://notif.safeonweb.be/.

De plus amples informations sont également disponibles à l'adresse suivante : https://ccb.belgium.be/fr/cert/signaler-un-incident.

3.3.2. Quand un incident est-il "significatif" ?

La loi NIS2 prévoit l'obligation pour toutes les entités entrant dans son champ d'application de notifier au CCB tout incident pouvant être considéré comme "significatif". Un tel incident est défini dans la loi comme suit :

"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."*

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

Les notifications obligatoires ne concernent donc uniquement les réseaux et systèmes d'information dont dépend l'entité concernée pour fournir le(s) service(s) énuméré(s) dans les annexes de la loi. Un incident affectant un système d'information isolé sans rapport avec la fourniture des services susmentionnés ne doit donc pas être notifié.

Deuxièmement, l'impact doit être significatif, c'est-à-dire provoquer ou être susceptible de provoquer au moins l'une des trois situations suivantes :

- **perturbation opérationnelle grave** d'un des services fournis (dans les secteurs ou sous-secteurs énumérés aux annexes I et II de la loi NIS2) ;
- **perte financière pour l'entité concernée** ;
- **des dommages matériels, physiques ou moraux considérables à d'autres personnes physiques ou morales**.

De plus amples informations sur la notification d'incidents sont disponibles dans notre **guide de notification d'incidents NIS2.**[8]

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

3.3.3. Destinataires d'une notification obligatoire d'incident significatif

En principe, chaque entité NIS2 doit notifier un incident au CCB uniquement. Ce dernier transmettra les notifications aux éventuelles autorités sectorielles ainsi qu'au Centre de crise (pour les entités essentielles).

Art. 34, § 1 loi NIS2

Cette règle connait néanmoins une exception pour les entités tombant sous le Règlement DORA dans le secteur bancaire et le secteur des finances. Les entités de ces deux secteurs notifient leur incident, selon le cas, à la Banque Nationale de Belgique (BNB) ou à l'Autorité des services et marchés financiers (FSMA) qui transmettent automatiquement la notification d'incident au CCB.

Le cas échéant, l'entité notifie aux destinataires de son service les incidents significatifs qui pourraient nuire aux services que cette dernière leur fournit. Elle communique également aux destinataires susceptibles d'être affectés par une cybermenace importante les mesures ou corrections que ces destinataires sont en mesure d'appliquer en réponse à cette menace. Le cas échéant, les entités informent également ces destinataires de la cybermenace importante elle-même.

Art. 34, § 2 loi NIS2

3.3.4. Procédure de notification d'un incident

La notification des incidents significatifs se déroule en plusieurs étapes :

Art. 35 loi NIS2

1. sans retard injustifié et tout au plus dans les **24 heures** après avoir pris connaissance de l'incident significatif, l'entité transmet une alerte précoce ;
2. sans retard injustifié et tout au plus dans les **72 heures** (24h pour les prestataires de services de confiance) après avoir pris connaissance de l'incident significatif, l'entité communique une notification d'incident ;
3. **à la demande** du CSIRT national ou, le cas échéant, de l'éventuelle autorité sectorielle concernée, l'entité communique un rapport intermédiaire ;
4. au plus tard **un mois** après la notification d'incident visée au 2., l'entité transmet un rapport final ;
5. si le rapport final ne peut être transmis car l'incident est encore en cours, l'entité transmet un rapport d'avancement puis, dans le mois suivant le traitement définitif de l'incident, le rapport final.

En pratique, la notification d'un incident peut être faite via notre plateforme : http://notif.safeonweb.be/.

[8] https://ccb.belgium.be/fr/open-media/688/download
Voir également l'acte d'exécution de la Commission (section 5.1).

3.3.5. Informations à transmettre lors d'une notification d'un incident

Les différentes étapes de notification comportent différentes informations à transmettre :

Art. 35 loi NIS2

- L'alerte précoce indique si l'on suspecte que l'incident significatif pourrait avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière. Cette alerte précoce inclut uniquement les informations nécessaires pour porter l'incident à la connaissance du CSIRT, et permet à l'entité concernée de demander une assistance, si nécessaire.
  Cette alerte ne doit pas détourner les ressources de l'entité effectuant la notification des activités liées à la gestion des incidents qui devraient avoir la priorité, afin d'éviter que les obligations de notification des incidents ne détournent les ressources de la gestion des incidents importants ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard.
- La notification d'incident dans les 72h a pour objectif de mettre à jour les informations communiquées dans le cadre de l'alerte précoce. Elle fournit également une évaluation initiale de l'incident, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles.
  Comme pour l'alerte précoce, la notification d'incident ne doit pas détourner les ressources de l'entité, afin d'éviter que les obligations de notification des incidents ne détournent les ressources de la gestion des incidents significatifs ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard.
- Le rapport intermédiaire contient les mises à jour pertinentes de la situation.
- Le rapport final doit comprendre une description détaillée de l'incident, y compris de sa gravité et de son impact; le type de menace ou la cause profonde qui a probablement déclenché l'incident; les mesures d'atténuation appliquées et en cours; et le cas échéant, l'impact transfrontière de l'incident.
- Le rapport d'avancement contient autant que possible les informations qui devraient se trouver dans le rapport final et qui sont en la possession de l'entité au moment de la communication du rapport d'avancement.

3.3.6. Règles de confidentialité qui s'appliquent aux informations transmises lors d'un incident

L'entité NIS2 et ses sous-traitants limitent l'accès aux informations relatives aux incidents, au sens de la loi NIS2, aux seules personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec cette loi.

Art. 26, §§ 3 & 4 loi NIS2

Cette règle vaut également pour le CCB (CSIRT national), le NCCN et l'autorité sectorielle.

Les informations fournies au CCB, au NCCN et à l'autorité sectorielle par une entité NIS2 peuvent être échangées avec des autorités d'autres États membres de l'Union européenne et avec d'autres autorités belges lorsque cet échange est nécessaire à l'application de dispositions légales.

Cette transmission d'informations se limite toutefois à ce qui est pertinent et proportionné à l'objectif de cet échange, dans le respect du Règlement UE 2016/679 (RGPD), de la confidentialité des informations concernées, de la sécurité et des intérêts commerciaux des entités NIS2.

3.4. Où puis-je signaler un incident NIS2 ?

Tous les incidents NIS2 peuvent être signalés via notre formulaire de notification en ligne : http://notif.safeonweb.be/.

De plus amples informations sur le signalement des incidents sont disponibles sur notre site web.

Consultez également notre guide de notification des incidents pour plus de détails sur les incidents "significatifs".

3.5. Que se passe-t-il si un incident se produit et qu'il implique aussi des données à caractère personnel ?

Comme cela est déjà le cas actuellement, les notifications d'incident dans le cadre de la loi ne vont pas remplacer les éventuelles notifications dans le cas d'une violation de données à caractère personnel, par exemple à l'Autorité de protection des données (APD). Deux notifications distinctes seront toujours nécessaires.

Toutefois, la loi prévoit une collaboration renforcée entre l'autorité nationale de cybersécurité et les autorités de protection des données. Cette collaboration pourrait conduire au développement d'outils communs.

Une notification à l'autorité de protection des données compétente peut se faire via son site internet.

3.6. Est-il possible de notifier volontairement des incidents ou des cybermenaces ?

Art. 38 loi NIS2

Oui. Le CSIRT national (CCB) peut également recevoir, à titre volontaire, des entités soumises ou non à la loi NIS2, des notifications d'incidents, des cybermenaces ou encore des incidents évités.

Une cybermenace désigne « toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes ».

Un incident évité est un « un événement qui aurait pu compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s'est pas produite ».

Ces notifications volontaires sont traitées de la même manière que les notifications obligatoires, mais les notifications obligatoires peuvent néanmoins être prioritaires.

Une notification volontaire n'a pas pour effet direct d'entraîner une inspection de l'entité qui a émis la notification ou de lui imposer des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas émis la notification.

Voir à cet égard la procédure expliquée à la section 3.3.

3.7. Que se passe-t-il si mon fournisseur ou une entreprise de mon groupe a un incident ? Qui doit faire une notification ? Que se passe-t-il si l'incident se produit dans plusieurs États membres ?

Chaque organisation qui tombe sous NIS2 et qui est touchée par un incident significatif doit le notifier séparément aux autorités NIS2 compétentes dans l'UE. Toutes les autres organisations peuvent également notifier volontairement leurs incidents au CCB via la plateforme mentionnée à la section 3.3.1.

Si l'incident affectant le fournisseur ou une autre entreprise du groupe devient également un incident significatif pour l'entité NIS2 concernée, cette dernière doit alors le signaler. Les entités NIS2 et leurs fournisseurs ou entreprises partenaires doivent communiquer ensemble et s'informer mutuellement des incidents de cybersécurité affectant la fourniture de leurs services.

Si l'incident significatif affecte plusieurs entreprises (ou une seule entreprise) établies dans plusieurs États membres différents, l'incident devra être notifié conformément aux règles de compétence, comme expliqué à la section 1.14. Il est possible que l'incident doive être déclaré dans plusieurs États membres dans certains cas exceptionnels (par exemple, une entreprise dotée d'une entité juridique établie dans plusieurs États membres et pas seulement dans le cadre de l'exception relative à l'établissement principal). Dans la pratique, un incident n'affecte souvent qu'un seul État membre et l'entité devra donc le notifier que dans un seul État membre.

3.8. Qu'est-ce qui est couvert par les deux régimes de responsabilité de la loi (art. 31 et 61) ?

Voir également les sections 3.9 et 3.10 ci-dessous.

L'article 31, § 1 de la loi NIS2 prévoit que les organes de direction sont responsables des violations de l'article 30 (mesures de cybersécurité) par leurs entités. Selon la théorie de l'organe, la responsabilité de la personne morale est en principe engagée par l'action de ses organes, comme le prévoit l'article 2:49 du Code des sociétés et des associations.

Toutefois, la théorie de la responsabilité cumulative est applicable à la responsabilité civile, notamment dans les conditions et limites fixées par les articles 2:56 à 2:58 du Code des sociétés et associations, de sorte que la responsabilité civile des membres des organes de direction (des membres des organes d'administration à tout le moins) peut être engagée à la double condition que la faute soit de nature extracontractuelle et excède manifestement le comportement raisonnable d'administrateurs normalement prudents et diligents se trouveraient placés dans les mêmes circonstances.

En outre, l'article 61, alinéa 1 de la loi NIS2 établit une responsabilité spécifique pour toute personne physique responsable d'une entité essentielle ou importante ou agissant en tant que représentant légal d'une entité essentielle ou importante sur la base du pouvoir de la représenter, de prendre des décisions en son nom ou d'exercer son contrôle, en vertu de leur pouvoir de veiller au respect à ce que l'entité se conforme à cette loi. Ces personnes sont responsables des manquements à leur obligation de veiller au respect de la loi NIS2.

Du point de vue des mesures administratives, la loi NIS2 permet, en cas de violations répétées, d'interdire temporairement à toute personne physique exerçant des responsabilités dirigeantes au niveau du directeur général ou du représentant légal dans l'entité essentielle concernée d'exercer des responsabilités dirigeantes dans cette entité, jusqu'à ce que l'entité essentielle concernée ait pris les mesures nécessaires pour remédier aux manquements ou pour se conformer aux exigences de l'autorité compétente à l'origine de l'application de ces mesures d'exécution (article 60, alinéa 1, 2°, et alinéa 2, loi NIS2 ; voir également la section 4.18.2).

Enfin, on peut noter que la loi NIS2 n'empêche pas l'application de toute responsabilité pénale. La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques qui sont auteurs des mêmes faits ou qui y ont participé.

À l'exception de la disposition relative aux mesures administratives, qui ne s'applique qu'aux entités essentielles, les éléments exposés ci-dessus sont applicables aux entités essentielles et importantes.

3.9. Quelles sont les obligations et responsabilités du management ?

Art. 31 & 61 loi NIS2

Les organes de direction des entités NIS2 doivent approuver les mesures de gestion des risques en matière de cybersécurité et superviser leur mise en œuvre. Si l'entité viole ses obligations en matière de mesure de gestion des risques, l'organe de direction en est responsable.

Les membres des organes de direction sont obligés de 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 leurs impacts sur les services fournis par l'entité concernée.

Les responsables et/ou représentants légaux d'une entité NIS2 doivent avoir le pouvoir de veiller au respect de la loi par l'entité. Ils sont responsables de leurs manquements à ce devoir.

L'objectif de cette responsabilisation est de transformer la cybersécurité en un sujet qui a réellement de l'importance pour les entités concernées.

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 fonctions de direction au niveau du directeur général ou du représentant légal dans une entité NIS2 peuvent être temporairement empêchées d'exercer des responsabilités de direction dans cette entité, en cas de violation des exigences de la loi NIS2.

3.10. Qu'est-ce qu'un « organe de direction » ?

La notion d'« organe de direction » n'est pas définie dans la directive.

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

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, 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.

3.11. Quel devrait être le contenu de la formation du management ?

La formation des membres de l'organe de direction a pour but de leur permettre d'exercer correctement les fonctions qui leur sont attribuées par la loi, à savoir approuver les mesures de gestion des risques en matière de cybersécurité et superviser la mise en œuvre de ces mesures. Il n'y a pas d'indication sur les exigences exactes en matière de formation. Son contenu et sa durée sont donc laissés à la discrétion des entités.

Notre CyberFundamentals Framework contient des informations sur le processus de formation, notamment en termes de contenu et de public cible. Au niveau Important, par exemple, la section sur la formation se trouve à partir de la page 28 (CyFun® 2023).

En tant qu'autorité de supervision, le CCB ne peut pas proposer de formations pour les entités NIS2, ni recommander des programmes de formation spécifiques.

3.12. Quelles sont les conditions légales pour pouvoir bénéficier du cadre protecteur lors de la recherche et le signalement de vulnérabilités (hacking éthique) ?

Art. 22 et 23 loi NIS2

La loi NIS2 reprend les dispositions de la loi NIS1, qui prévoit un cadre protecteur (*safe harbour)* pour les « hackers éthiques » ou « lanceurs d'alertes numériques ».

Pour pouvoir bénéficier de ce cadre, la personne doit :

- Agir sans intention frauduleuse ni dessein de nuire ;
- Adresser une notification simplifiée dans les 24 heures suivant la découverte de la vulnérabilité tant au CSIRT national qu'à l'organisation responsable ;
- Adresser une notification complète dans les 72 heures suivant la découverte aux mêmes destinataires ;
- N'agir que dans les limites du nécessaire et de la proportionnalité pour vérifier l'existence d'une vulnérabilité et pour la rapporter ;
- S'abstenir de rendre publique une vulnérabilité sans l'accord du CSIRT national.

De plus, pour pouvoir rechercher des vulnérabilités sur les réseaux et systèmes d'information de certaines autorités telles que les services de renseignements, la Défense, les autorités judiciaires, etc., les hackers éthiques doivent au préalable conclure un accord avec ces entités.

Le CCB fournit sur son site internet des informations générales sur le hacking éthique, avec notamment une page dédiée à la procédure de signalement.

3.13. Quelles sont les obligations en matière d'enregistrement ?

3.13.1. Comment les entités NIS2 s'enregistrent-elles ?

Les entités essentielles et importantes devront s'enregistrer sur le portail du CCB, Safeonweb@Work.

Art. 13 loi NIS2

Le délai pour s'enregistrer dépend du type d'entité. En principe, les entités essentielles et importantes, ainsi que les fournisseurs de services d'enregistrement de noms de domaine, ont **5 mois** pour s'enregistrer après l'entrée en vigueur de la loi, soit pour le **18 mars 2025**. Lors de l'enregistrement, elles doivent fournir les informations suivantes :

1. leur dénomination ainsi que leur numéro d'enregistrement auprès de la BCE ou un enregistrement équivalent dans l'Union européenne ;
2. leur adresse et leurs coordonnées actualisées, y compris leur adresse de courrier électronique, leurs plages d'IP et leur numéro de téléphone ;
3. le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II de la loi ;
4. le cas échéant, une liste des États membres dans lesquels elles fournissent des services relevant du champ d'application de la loi.

Une exception existe pour les entités qui auraient déjà communiquées ces informations à une autorité sectorielle NIS2 en vertu d'une obligation légale. Dans ce cas-là, les informations doivent simplement être complétées auprès de cette autorité. Si les informations changent, elles doivent être communiquées dans un délai de deux semaines.

Un régime légèrement adapté existe pour les types d'entités suivantes :

Art. 14 loi NIS2

- fournisseurs de services DNS ;
- registres des noms de domaine de premier niveau ;
- entités qui fournissent 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 ;
- fournisseurs de places de marché en ligne ;
- moteurs de recherche en ligne ;
- plateformes de services de réseaux sociaux.

Elles doivent s'enregistrer dans les **2 mois** après l'entrée en vigueur de la loi, soit pour le **18 décembre 2024**, et communiquer les informations suivantes :

1. leur nom ;
2. leur secteur, sous-secteur et type d'entité concernés, visés à l'annexe I ou II, le cas échéant ;
3. l'adresse de leur établissement principal et de leurs autres établissements légaux dans l'Union ou, s'ils ne sont pas établis dans l'Union, de leur représentant ;
4. leurs coordonnées actualisées, y compris les adresses de courrier électronique et les numéros de téléphone et, le cas échéant, celles de leur représentant ;
5. les États membres dans lesquels ils fournissent leurs services relevant du champ d'application de la loi ;
6. leurs plages d'IP.

Elles doivent également informer le CCB des modifications de ces informations.

3.13.2. Comment est-ce que je peux enregistrer mon organisation ?

Tous les détails pratiques relatifs à la procédure d'enregistrement sont expliqués dans notre guide d'enregistrement NIS2 disponible en ligne.

En bref : les représentants légaux d'une organisation mentionnée dans la Banque Carrefour des Entreprises (BCE) (recherchez votre organisation ici) peuvent se connecter à la plateforme My eGov Role Management afin de fournir les autorisations nécessaires à un citoyen belge pour enregistrer une organisation sur notre plateforme Safeonweb@Work. Toutes les informations sont disponibles dans le guide.

3.13.3. Comment savoir si mon organisation est déjà enregistrée ?

La personne indiquée à la section 3.13.2 doit se connecter à la plateforme pour vérifier.

3.13.4. Comment puis-je modifier mes informations d'enregistrement sur la plateforme ?

La personne visée à la section 3.13.2 doit se connecter à la plateforme. Une fois connectée et l'organisation sélectionnée, elle peut, dans le *dashboard* (ou tableau de bord), cliquer sur « Informations sur l'organisation » sur la gauche, où elle pourra modifier les informations.

3.13.5. Quelles sont les entités qui doivent s'enregistrer dans un groupe de sociétés ? Seule la holding peut-elle s'enregistrer ?

Au sein d'un groupe de sociétés, toutes les organisations/entités juridiques distinctes (même potentiellement la holding - en fonction des services fournis) qui tombent sous NIS2 **doivent**

s'enregistrer individuellement. La holding ne peut pas s'enregistrer à la place des sociétés de son groupe.

3.13.6. Que se passe-t-il si mon organisation a des départements ou des sous-entités qui sont des types d'entités différents ?

Si ces départements ou sous-entités font tous partie de la même entité juridique, cette dernière doit s'enregistrer en tant que tous les différents types d'entités pour lesquelles elle se qualifie.

Si les différentes sous-entités sont des entités juridiques distinctes qui remplissent toutes les conditions requises pour être considérées comme une "entité" au sens de NIS2 (voir la section 1.4), elles doivent toutes s'enregistrer séparément.

3.13.7. Les organisations dans la chaîne d'approvisionnement des entités NIS2 doivent-elles s'enregistrer ?

Seules les organisations entrant dans le champ d'application de NIS2 doivent s'enregistrer. Il est possible que des organisations faisant partie de la chaîne d'approvisionnement d'entités NIS2 ne soient pas elles-mêmes des entités NIS2 et ne doivent donc pas s'enregistrer.

Pour plus d'informations sur la chaîne d'approvisionnement, voir la section 3.14.

3.13.8. Comment une organisation établie en dehors de la Belgique peut-elle s'enregistrer ? Comment un représentant légal peut-il enregistrer une organisation ?

Il existe deux situations exceptionnelles dans lesquelles les organisations situées en dehors de la Belgique doivent s'enregistrer :

1) Elles fournissent des services ou des réseaux de communication électronique en Belgique (voir section 1.14) ;
2) Elles relèvent du régime de juridiction de l'établissement principal (voir section 1.14), sont établies en dehors de l'UE, fournissent des services en Belgique, choisissent la Belgique comme lieu d'enregistrement dans l'UE et y désignent un représentant légal.

Dans ces deux situations, si les organisations ne parviennent pas à s'inscrire via le site web Safeonweb@Work, elles doivent contacter le CCB à l'adresse suivante : info@ccb.belgium.be.

3.13.9. Est-ce que je dois m'enregistrer à nouveau si mon organisation tombait déjà sous NIS1 ?

Oui, l'organisation doit se réenregistrer.

3.13.10. Comment est-ce que je peux prouver que mon organisation est bien enregistrée ?

Les organisations NIS2 peuvent demander au CCB, via info@ccb.belgium.be, de leur fournir un document attestant de leur enregistrement. Il est obligatoire d'indiquer le **numéro BCE (Banque**

Carrefour des Entreprises) dans l'email envoyé au CCB. Les confirmations d'enregistrement ne seront envoyées qu'aux adresses emails possédant le même nom de domaine que celui utilisé pour le point de contact durant l'enregistrement NIS2. Le CCB peut demander une autorisation formellement signée de l'organisation avant d'accéder à la requête.

Ce processus manuel sera remplacé dans le futur par un document téléchargeable sur la plateforme.

3.13.11. Que fera le CCB des organisations qui ne s'enregistrent pas ?

Sur la base des informations dont elle dispose en tant qu'autorité fédérale, la CCB tentera de manière proactive de rechercher et de contacter les entités qui ne se sont pas enregistrées. Il est important de noter que les entités qui ne se sont pas enregistrées pourraient être considérées comme ayant enfreint la loi NIS2 et s'exposer à des mesures administratives et des amendes appropriées.

3.14. Supply chain : Comment gérer en tant qu'entité les relations avec ses fournisseurs et prestataires directs ?

Art. 30, §3, 4° loi NIS2

Dans le cadre de la liste minimale des mesures de gestion des risques de cybersécurité, les entités couvertes par la loi NIS2 doivent prendre des mesures appropriées et proportionnées pour sécuriser leur réseau et leurs systèmes d'information.

L'une de ces mesures est la sécurité de la chaîne d'approvisionnement de l'entité concernée. Celle-ci comprend les aspects liés à la sécurité concernant les relations entre chaque entité et **ses fournisseurs ou prestataires de services directs**.

L'impact de cette obligation peut être ressenti de deux points de vue : Non seulement elle implique que les entités NIS2 doivent imposer des mesures de gestion des risques de cybersécurité aux organisations de leur(s) chaîne(s) d'approvisionnement (telles que les fournisseurs et les sous-traitants) et les superviser, mais elle implique également que les entités n'entrant pas dans le 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 elles-mêmes le soin de vérifier si les organisations dans leur 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 démonstration du respect de l'obligation de la chaîne d'approvisionnement.

Pour les contrats en cours avec les fournisseurs et les prestataires de services, il incombe à l'entité d'évaluer les dispositions actuellement en vigueur et de s'assurer qu'elles sont conformes aux obligations. Il se peut que les contrats existants doivent être révisés. L'entité NIS2 doit mettre en place des garanties contractuelles suffisantes au cas où l'organisation dans sa chaîne d'approvisionnement ne respecterait pas ses obligations. Voir la ligne du temps dans la section 4.14 pour savoir pour quand les contrats doivent être adaptés.

Pour choisir le niveau CyFun® approprié à imposer aux fournisseurs et aux prestataires de services, l'entité NIS2 devra procéder à une évaluation des risques et imposer le niveau le plus approprié en fonction des résultats obtenus. L'outil d'évaluation des risques CyFun® pourrait être utilisé à cette fin.

Pour toutes les entités n'entrant pas dans le 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 afin de se préparer à l'éventualité où elles entrent dans la chaîne d'approvisionnement d'une entité NIS2. Là encore, elles peuvent avoir recours au CyFun® Framework pour identifier et mettre en œuvre les mesures concrètes qu'elles pourraient être amenées à prendre.

Ni le fait que l'entité NIS2 soit propriétaire d'une organisation faisant partie de sa chaîne d'approvisionnement, ni la taille de cette dernière ont une incidence sur le champ d'application de cette obligation. Elles peuvent seulement avoir un impact sur l'évaluation des risques de la chaîne d'approvisionnement des entités NIS2.

Pour la gestion des incidents provenant des fournisseurs, voir la section 3.7. Voir également la section 3.9 sur la responsabilité des organes de direction en matière de mesures de gestion des risques de cybersécurité.

3.15. Quelle sont les obligations de confidentialité à respecter ?

Art. 26 loi NIS2

Les autorités compétentes, les entités essentielles ou importantes et leurs sous-traitants, limitent l'accès aux informations dans le cadre de la loi NIS2 aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec l'exécution de la loi.

Les informations fournies aux autorités compétentes par les entités essentielles ou importantes, peuvent néanmoins être échangées avec des autorités de l'Union européenne, avec des autorités belges ou des autorités étrangères, lorsque cet échange est nécessaire à l'application de dispositions légales.

Les informations échangées se limitent à ce qui est pertinent et sont proportionnées à l'objectif de cet échange, notamment dans le respect du règlement (UE) 2016/679 (RGPD). Cet échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités essentielles ou importantes.

Art. 27 loi NIS2

La loi prévoit néanmoins la possibilité de volontairement échanger des informations pertinentes en matière de cybersécurité, dont notamment les informations relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, etc. Cet échange se déroule sous certaines conditions dans le cadre de communautés d'échange d'informations, mis en œuvre au moyen d'accords de partage d'informations.

4. Contrôle / Supervision

4.1. Quelles sont les autorités compétentes ?

Art. 15, 16 et s. loi NIS2 et art. 3 arrêté royal NIS2

4.1.1. Le Centre pour la Cybersécurité Belgique (CCB)

L'autorité nationale de cybersécurité (CCB) est responsable de la coordination et du suivi de la loi. À cette fin, la loi combine les missions existantes du CCB avec les ajouts prévus par la directive NIS2, notamment en ce qui concerne la supervision des entités. Le CCB est responsable de la supervision des entités essentielles et importantes (avec l'aide des autorités sectorielles) et il est le point de contact central pour l'implémentation de NIS2.

L'équipe nationale de réponse aux incidents de sécurité informatique (CSIRT national) fait également partie de l'autorité nationale de cybersécurité. Les entités NIS2 sont tenues de signaler les incidents significatifs à ce CSIRT.

4.1.2. Les autorités sectorielles

Les autorités sectorielles suivantes ont été désignées :

1. **pour le secteur de l'énergie** : le Ministre fédéral ayant l'Energie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur);
2. **pour le secteur des transports** :
    a. En ce qui concerne le secteur du transport, à l'exception du transport par eau : le Ministre fédéral compétent pour le Transport, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur);
    b. En ce qui concerne le transport par eau: le Ministre fédéral compétent pour la Mobilité maritime, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur);
3. **pour le secteur de la santé** :
    a. En ce qui concerne les entités exerçant des activités de recherche et de développement dans le domaine des médicaments ; les entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques ; et les entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique : l'Agence fédérale des médicaments et des produits de santé (AFMPS);
    b. le Ministre fédéral ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration;
4. **pour le secteur des infrastructures digitales :** Institut belge pour les postes et les télécommunications (IBPT) ;

5. **pour ce qui concerne les prestataires de services de confiance** : le Ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration;
6. **pour le secteur des fournisseurs numérique** : le Ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration;
7. **pour les secteurs de l'espace et de la recherche** : le Ministre fédéral de la politique scientifique ou par délégation de celui-ci, un membre dirigeant du personnel de son administration ;
8. **pour de l'eau potable** : le Comité national de sécurité pour la fourniture et la distribution d'eau potable ;
9. **pour le secteur bancaire** : la Banque nationale de Belgique (BNB) ;
10. **pour le secteur de l'infrastructure des marchés financiers** : l'Autorité des services et marchés financiers (FSMA) ;
11. **pour le sous-secteur de la fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro, du secteur de la fabrication :** l'Agence fédérale des médicaments et des produits de santé.

Les autorités sectorielles ont un certain nombre de compétences. Pour plus d'informations, voir la section 4.5.

Les entités couvertes par une autorité sectorielle peuvent s'adresser à cette dernière pour obtenir des informations, de l'aide, etc.

4.1.3. Le Centre de Crise National (NCCN)

Le Centre de crise national est également associé à la mise en œuvre de la loi NIS2 notamment pour ce qui concerne la notification des incidents, la gestion des crises cyber, ainsi que les mesures de sécurité physique mises en œuvre par les exploitants d'infrastructures critiques et entités critiques (soumis à la directive CER).

4.2. Quels cadres de référence peuvent être utilisés par les entités NIS2 pour démontrer leur conformité ?

Les entités essentielles qui sont soumises à une obligation d'évaluation périodique de la conformité peuvent choisir d'utiliser l'un des deux cadres de références mentionnés dans l'arrêté royal NIS2.

Art. 5, § 1 arrêté royal NIS2

L'usage de ces cadres pour le contrôle est expliqué dans la section suivante (4.4.).

4.2.1. Le CyberFundamentals (CyFun®) Framework

Le CyberFundamentals (CyFun®) Framework[9] compile une série de mesures concrètes visant à :

- protéger les données ;
- réduire considérablement le risque des cyberattaques les plus courantes ;

[9] https://cyfun.be

- 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. 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 qui est disponible gratuitement et publiquement sur notre site web.

4.2.2. ISO/IEC 27001

ISO/IEC 27001 est une norme reconnue internationalement, relative aux systèmes de gestion de la sécurité des informations (ISMS). Elle fournit un cadre pour les organisations de tous les secteurs de gérer et protéger leurs système d'informations.

Sa dernière version date de 2022, mais elle est reprise dans l'arrêté royal sans indication de date afin de permettre d'appliquer toujours sa version la plus récente.

En Belgique, le NBN (Bureau de normalisation) est l'organisme national de normes. Il joue un rôle central dans le développement, la publication, et la dissémination de normes en Belgique.

Vous pourrez trouver plus d'informations sur la norme NBN EN ISO/IEC 27001, l'adoption nationale belge de la norme internationale ISO/IEC 27001, sur le site web de la NBN : https://www.nbn.be/fr.

4.3. Où est-ce que je peux trouver plus d'informations à propos de CyFun® ?

Toutes les informations, tous les documents, toute la guidance, etc. sont centralisés sur le site https://cyfun.be.

CyFun® dispose également de son propre FAQ, disponible à l'adresse suivante : https://atwork.safeonweb.be/cyberfundamentals-frequently-asked-questions-faq.

4.4. Comment se déroulera le contrôle des entités concernées ? Est-ce que le CCB propose des certifications CyFun® ?

Art. 39 et s. loi NIS2

Art. 6-13 arrêté royal NIS2

Lorsque l'on parle du contrôle/supervision dans le cadre de la loi, il faut distinguer les deux catégories d'entités : les entités essentielles et les entités importantes.

Les entités essentielles sont obligatoirement soumises à une évaluation périodique de la conformité. Cette évaluation est réalisée sur base du choix effectué par l'entité entre trois options :

- soit une certification CyberFundamentals (CyFun®) octroyée par un organisme d'évaluation de la conformité (OEC/CAB) agrée par le CCB (après accréditation par BELAC) ;
- soit une certification ISO/IEC 27001, délivrée par un organisme d'évaluation de la conformité accrédité par un organisme d'accréditation qui a signé la convention de reconnaissance mutuelle (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 agrée par le CCB ;
- soit une inspection par le service d'inspection du CCB (ou par un service d'inspection sectoriel).

Le service d'inspection peut également à tout moment procéder à un contrôle des entités essentielles (en l'absence d'incident – *ex ante* – et après un incident ou avec suffisamment de preuves du non-respect de la loi à disposition – *ex post*).

Pour les entités importantes, la supervision est uniquement réalisée de manière « *ex post* » par le service d'inspection, c'est-à-dire après un incident ou au vu d'éléments de preuve, d'indications ou d'informations selon lesquels une entité importante ne respecterait pas ses obligations (art. 48, § 2 loi NIS2). Elles ne sont donc, en principe, pas soumises à une évaluation périodique de la conformité. Mais ces entités peuvent néanmoins se soumettre de manière volontaire au même régime que les entités essentielles.

Pour les modalités de l'inspection réalisée par le service d'inspection, voir section 4.15.

Le CCB ne procède pas à des évaluations périodiques de la conformité qui pourraient conduire à une présomption de conformité, et ne délivre donc pas non plus de certifications CyFun®. Seuls les CABs peuvent le faire.

4.5. Une organisation doit-elle obtenir une certification ou une vérification CyFun® si elle souhaite utiliser la norme ISO/IEC 27001 ?

Non, une certification ou une vérification de CyFun® n'est pas une étape intermédiaire nécessaire pour recevoir une certification ISO/IEC 27001.

Cependant, il est possible d'obtenir un label CyFun® en utilisant une certification ISO/IEC 27001 existante avec le champ d'application (et *Statement of Applicability*) approprié. Pour ce faire, les documents nécessaires doivent être téléchargés via l'onglet "Labels" du tableau de bord de votre organisation enregistrée sur Safeonweb@Work.

4.6. Qu'est-ce qu'un organisme de contrôle de la conformité (OEC/CAB) ?

Un organisme d'évaluation de la conformité (*Conformity Assessment Body* – « CAB » en anglais) est un organisme qui est chargé de contrôler et certifier le respect des exigences reprises dans le référentiel CyFun® ou la norme ISO/IEC 27001 (appliquée dans le cadre de la loi NIS2) par les entités NIS2 soumises à l'évaluation périodique de conformité (obligatoire pour les entités essentielles, volontaire pour les entités importantes).

Dans le cadre de CyFun®, il est accrédité par l'autorité d'accréditation belge (BELAC) et agréé par le CCB. Dans le cadre de ISO/IEC 27001, il est accrédité par un organisme d'accréditation qui a signé la convention de reconnaissance mutuelle (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 agrée par le CCB. Plus d'informations sont disponibles dans les conditions d'autorisation des CABs sur notre site web.

4.7. Où puis-je trouver plus d'informations sur ou pour les CABs ?

Toutes les informations relatives à l'accréditation en Belgique sont disponibles sur le site officiel de BELAC : https://economie.fgov.be/fr/themes/qualite-securite/accreditation.

Des informations complémentaires pour les CABs dans le cadre de CyFun® sont disponibles sur notre site web : https://atwork.safeonweb.be/fr/organismes-devaluation-de-la-conformite-cab.

La liste des CAB accrédités et agréés pour NIS2 en Belgique est disponible sur notre site web : https://atwork.safeonweb.be/open-media/1101/download (lien de téléchargement).

4.8. Quelles sont les missions des autorités sectorielles ?

Les autorités sectorielles jouent également un rôle dans le cadre de la loi NIS2, en raison de leur connaissance et de leur expertise particulière de chacun des secteurs concernés. Elles peuvent intervenir, le cas échéant, dans les missions suivantes :

Art. 11, 13, 24, 25, 33, 34, 39, 44, 51 et 52 loi NIS2

- Identification additionnelle (consulter et proposer) ;
- Enregistrement des entités ;
- Organisation d'exercices sectoriels ;
- Analyse et gestion des conséquences d'un incident pour un secteur ;
- Participation à certains travaux du groupe de coopération NIS ;
- Sensibilisation des entités de leurs secteurs ;
- Coopération au niveau national ;
- Mesures supplémentaires de gestion des risques de cybersécurité ;
- Notification des incidents (transmissions des incidents significatifs notifiée par le CSIRT national aux autorités sectorielles, consultation dans différentes situations sur ce sujet) ;
- Supervision et inspection (conjointe ou déléguée) ;
- Amendes administratives.

4.9. Comment une entité peut-elle prouver qu'elle est en conformité avec ses obligations ? Qu'est-ce qu'une présomption de conformité ?

Art. 42 loi NIS2

Art. 5, § 1 arrêté royal NIS2

Dans le cadre de l'évaluation périodique de la conformité – obligatoire pour les entités essentielles – il sera possible pour l'entité d'obtenir une certification ou un label, permettant de présumer, jusqu'à preuve du contraire, que l'entité est en conformité avec ses obligations en matière de cybersécurité.

Cette certification sera basée sur les deux référentiels mentionnés dans l'arrêté royal : les CyberFundamentals (CyFun®) ou la norme internationale ISO/IEC 27001 (avec le bon champ d'application et *Statement of Applicability*). Voir à cet égard également la section 4.2.

Il est important de noter que **le champ d'application** d'une certification doit être **identique au champ d'application de la loi NIS2**, c'est-à-dire qu'il doit inclure tous les réseaux et systèmes d'information d'une organisation, sinon la certification ne permettra pas à une organisation de bénéficier d'une présomption de conformité.

Bien entendu, une entité pourra également utiliser un autre référentiel ou norme technique pour mettre en œuvre ses exigences légales de cybersécurité. Elle ne bénéficiera alors pas de la présomption de conformité et devra démontrer concrètement au service d'inspection qu'elle applique toutes les mesures requises en s'appuyant sur une table de concordance (mapping) avec l'un des deux référentiels précités.

4.10. Pouvez-vous limiter la portée d'une certification ou d'une vérification aux seuls services et activités liés à NIS2 ?

Comme indiqué à la section 4.9, la portée d'une certification ou d'une vérification ne peut être inférieure à la portée de la loi NIS2, qui couvre l'ensemble de l'organisation.

4.11. Est-ce qu'une entité peut utiliser un niveau d'assurance CyFun® inférieur au niveau assorti à sa catégorie d'entité ? Est-ce que cela modifie sa qualification NIS2 ?

Art. 7 arrêté royal NIS2

L'arrêté royal NIS2 laisse la possibilité à une entité de recourir à un niveau CyFun® inférieur à sa qualification NIS2 (par exemple, l'usage du niveau d'assurance Important pour une entité essentielle) pour autant qu'elle puisse le justifier objectivement sur base de son analyse des risques. Ce choix demeure l'entière responsabilité de l'entité concernée et **n'a pas d'impact sur sa qualification juridique en tant qu'entité essentielle ou importante**. Il convient de souligner que ce choix peut être remis en cause à tout moment par le service d'inspection dans le cadre de ses missions de contrôle.

Le CCB propose un outil d'évaluation des risques disponible sur Safeonweb@Work pour qu'une entité puisse sélectionner en connaissance de cause le niveau d'assurance CyFun® qui lui convient.

4.12. Les organisations ont-elles besoin de l'accord du CCB pour utiliser un niveau inférieur de CyFun® ?

Non, les entités NIS2 ne doivent pas demander au CCB de confirmer leur analyse pour utiliser un niveau inférieur de CyFun®. Comme indiqué dans la section 4.11, chaque entité NIS2 est elle-même responsable de ce choix. La justification de ce choix doit uniquement être documentée en interne.

Lors d'une inspection, le service d'inspection pertinent peut contrôler le choix effectué par l'entité concernée.

4.13. Est-ce qu'une entité qui était un opérateur de service essentiel (OSE) sous NIS1 peut garder sa certification ISO27001 ?

Art. 8, 12 et 14-15 arrêté royal NIS2

Si une entité qui était opérateur de service essentiel (OSE) sous NIS1 dispose d'une certification ISO/IEC 27001, elle pourra utiliser sa certification dans le cadre d'une évaluation périodique de conformité NIS2. Au besoin, le champ d'application de la certification devra être élargi pour s'assurer que celle-ci couvre bien l'ensemble des réseaux et systèmes d'information de l'entité concernée.

La certification devra être effectuée par un organisme d'évaluation de la conformité, accrédité par BELAC en Belgique (ou par un autre organisme national européen accrédité si cette certification émane d'un autre État membre) et agrée par le CCB.

4.14. [Ligne de temps] À partir de quand les entités concernées devront appliquer les obligations de la loi ?

4.14.1. Organisations dans le champ d'application avant/au moment où la loi entre en vigueur

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 accorde aux entités un délai supplémentaire avant leur mise en application.

Art. 13 & 75 loi NIS2
Art. 22-23 arrêté royal NIS2

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.

Les entités importantes ne font pas l'objet d'une évaluation régulière de la conformité obligatoire (supervision *ex-post*). Dans le respect du caractère approprié et proportionné des mesures de cybersécurité, le service d'inspection prendra en compte leur évolution à travers le temps.

Si par exemple un cyberincident significatif se produit au début de l'année 2025, l'entité concernée devra prendre les mesures nécessaires pour le gérer et le notifier au CCB, sous le contrôle possible des services d'inspections compétents. C'est pourquoi nous encourageons toutes les entités NIS2 à ne pas attendre l'échéance du délai d'enregistrement et de leurs premières évaluations de la conformité pour mettre en œuvre les mesures requises.

4.14.2. Organisations dans le champ d'application après l'entrée en vigueur de la loi

Il est possible qu'une organisation tombe dans le champ d'application de la loi NIS2 après son entrée en vigueur. Dans ce cas, les délais mentionnés ci-dessus commencent à courir à partir du moment où l'entité entre dans le champ d'application.

Il en va de même pour les entités importantes qui deviennent des entités essentielles au cours de leur développement organisationnel : les délais indiqués ci-dessus s'appliquent dès que l'organisation devient une entité essentielle. Elle dispose alors également de deux semaines pour modifier son enregistrement sur la plateforme Safeonweb@work.

Veuillez vous référer à la section 1.5.2 pour ce qui concerne l'évolution de la taille des entreprises.

4.15. Quelles sont les modalités de l'inspection ?

Art. 44 loi NIS2

Le service d'inspection de l'autorité nationale de cybersécurité est chargé d'effectuer des inspections pour vérifier que les entités essentielles et importantes respectent les mesures de gestion des risques en matière de cybersécurité et les règles de notification des incidents.

Les inspections relatives aux entités essentielles peuvent être à la fois *ex ante* (proactives) et *ex post* (réactives). Elles sont effectuées par le service d'inspection de l'autorité nationale de cybersécurité ou par le service d'inspection sectoriel désigné (mesures sectorielles

spécifiques/complémentaires). Ces inspections peuvent, à la demande de l'autorité sectorielle, être effectuées ensemble par les autorités précitées.

Les entités essentielles sont de plus tenues de se soumettre à des évaluations périodiques de la conformité. Les entités importantes peuvent également se soumettre volontairement à une évaluation de la conformité sur base de la norme ISO/IEC 27001 ou des CyberFundamentals (CyFun®) (voir section 4.4.).

Les inspections *ex post* des entités importantes sont réalisées sur base d'indicateurs, tels que la survenance d'un incident ou des éléments objectives témoignant de manquements possibles. Là encore, cette inspection peut être effectuée par l'inspection du CCB, par l'inspection sectorielle désignée, ou par les deux. L'objectif des contrôles conjoints ou des contrôles déléguées aux inspections sectorielles étant de simplifier et de rationaliser les ressources de l'Etat.

Les inspecteurs pourront se rendre sur place, faire des constatations par procès-verbaux et rédiger des rapports. Sur base de ces constatations, une procédure pourra être lancée afin d'enjoindre l'entité de mettre fin à une violation et, le cas échant, de prendre les mesures administratives appropriées, allant de l'avertissement à l'amende administrative.

4.16. Que se passe-t-il si mon organisation ne peut pas prouver qu'elle est conforme après 18 mois ?

Lors de ses contrôles, le service d'inspection insistera beaucoup sur l'évolution d'une organisation à travers le temps vers son objectif. Il est donc très important que des preuves de progrès concrets vers la conformité puissent être apportées.

L'objectif premier du CCB est d'atteindre un niveau élevé de cybersécurité dans tout 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 ce projet de décision de sanction doit être accompagné d'une motivation suffisante. 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 minimum pour déterminer une sanction appropriée et proportionnée ; par exemple, la catégorie de l'entité, les infractions antérieures, la gravité de l'infraction, sa durée, les dommages, la négligence, etc.

Dans tous les cas, si l'entité n'est pas en conformité avec ses obligations, le service d'inspection compétent peut prendre des mesures appropriées et/ou infliger des amendes afin que l'organisation se mette en conformité avec la loi. En fonction de l'effet de ces mesures et/ou amendes sur le comportement de l'organisation, d'autres mesures et/ou amendes peuvent être prises jusqu'à ce que la conformité soit atteinte.

De plus amples informations sur les mesures et les amendes sont disponibles dans les sections 4.17 et 4.18.

4.17. Est-ce que les mesures et les amendes administratives sont proportionnelles ? Quelles sont les montants des amendes ?

Art. 59 loi NIS2

L'objectif des mesures et amendes administratives est de renforcer le niveau de cybersécurité des entités essentielles et importantes. Moyennant le respect des procédures prévues par la loi (dont l'audition de l'entité concernée, voir art. 51-57), une mesure ou une amende administrative peut être prononcée, de manière proportionnelle, en tenant compte de la gravité des manquements, de l'attitude de l'entité et d'éventuelle situation de récidive.

Les amendes administratives suivantes peuvent être imposées :

1. De 500 à 125.000 euros pour quiconque qui ne se conforme pas aux obligations d'information visées à l'article 12;
2. De 500 à 200.000 euros pour l'entité qui fait subir des conséquences négatives à une personne agissant pour son compte en raison de l'exécution, de bonne foi et dans le cadre de ses fonctions, des obligations découlant de la présente loi;
3. De 500 à 200 000 euros quiconque ne se conforme pas aux obligations de contrôle;
4. De 500 à 7.000.000 euros ou 1,4% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient (le montant le plus élevé étant retenu) : pour l'entité importante qui ne se conforme pas aux obligations relatives aux mesures de gestion des risques en matière de cybersécurité et/ou de notification d'incidents;
5. De 500 à 10.000.000 euros ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient (le montant le plus élevé étant retenu) : pour l'entité essentielle qui ne se conforme pas aux obligations relatives aux mesures de gestion des risques en matière de cybersécurité et/ou de notification d'incidents.

L'amende administrative est doublée en cas de récidive pour les mêmes faits dans un délai de trois ans.

Le concours de plusieurs manquements peut donner lieu à une amende administrative unique, proportionnelle à la gravité de l'ensemble des faits.

4.18. Quelles autres mesures administratives peuvent-elles être prises ?

4.18.1. Mesures de base

Art. 58 loi NIS2

Les mesures administratives suivantes peuvent être imposées aux entités essentielles et importantes :

1. émettre des avertissements concernant les violations de la loi par les entités concernées;
2. adopter des instructions contraignantes ou une injonction exigeant des entités concernées qu'elles remédient aux insuffisances constatées ou aux violations de la loi;
3. ordonner aux entités concernées de mettre un terme à un comportement qui viole la loi et de ne pas le réitérer;

4. ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité ou de respecter les obligations en matière de notification d'incidents énoncées, de manière spécifique et dans un délai déterminé;
5. ordonner aux entités concernées d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;
6. ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable;
7. ordonner aux entités concernées de rendre publics les aspects de violations de la loi de manière spécifique;

Lorsque l'entité concernée est une entité essentielle :

- le CCB peut désigner, pour une période déterminée, un responsable du contrôle ayant des tâches bien définies pour superviser le respect, par les entités concernées, des mesures de gestion des risques en matière de cybersécurité et de notification d'incidents ;
- les instructions contraignantes visées au point 2 concernent également les mesures nécessaires pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre.

4.18.2. Mesures supplémentaires

Si les mesures demandées ne sont pas prises dans le délai imparti, les mesures administratives suivantes peuvent être imposées aux entités essentielles :

Art. 60 et 62 loi NIS2

1. suspendre temporairement une certification ou une autorisation concernant tout ou partie des services pertinents fournis ou des activités pertinentes menées par l'entité concernée;
2. interdire temporairement à toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans l'entité concernée d'exercer des responsabilités dirigeantes dans cette entité.

Les suspensions ou interdictions temporaires visées au point 1 sont uniquement appliquées jusqu'à ce que l'entité concernée ait pris les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente à l'origine de l'application de ces mesures d'exécution.

Ces mesures additionnelles (suspension ou interdiction temporaire d'exercer des responsabilités dirigeantes) et les amendes administratives ne sont pas applicables aux entités du secteur de l'administration publique. Cela étant, les mesures de bases décrites à la section 4.18.1 sont bien applicables.

4.19. Puis-je utiliser la certification ISO 27001 de ma société mère pour prouver ma conformité avec NIS2 ?

La loi NIS2 s'applique de manière individuelle aux entités juridiques, pas aux groupes de sociétés. En conséquence, par principe, chaque entité NIS2 établie en Belgique doit respecter les mesures de la loi NIS2 belge. Si une entité NIS2 tombe dans le champ d'application de la loi, les obligations s'appliquent à l'entièreté de l'entité.

Le fait qu'une société sœur/mère possède une certification ISO 27001 n'est pas en soit suffisant pour démontrer qu'une filiale est conforme à la loi NIS2. Vu que le champ d'application de la loi NIS2 couvre l'entièreté de l'entité, toute certification doit en couvrir autant. En d'autres mots, le champ d'application et le *statement of applicability* (déclaration d'applicabilité) d'une certification ISO 27001 doit couvrir l'entièreté de l'entité NIS2 concernée. Une certification ISO 27001 pour plusieurs entités n'est techniquement possible qu'au travers d'une certification multi-site. La détermination du champ d'application relève de la responsabilité de l'entité.

La certification ISO 27001 doit aussi couvrir toutes les mesures minimales de gestion des risques en matière de cybersécurité fixées par la loi NIS2 et doit être effectuée par un CAB agréé par le CCB (les conditions de l'agréation sont disponibles sur notre site web CyFun®).

5. Autres

5.1. La directive NIS2 donne-t-elle un mandat à la Commission européenne pour un acte d'exécution ? Où puis-je le trouver ?

Art. 21, §5 & 23, § 11 Directive NIS2

Un règlement d'exécution a été adopté par la Commission. Il s'agit du Règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, 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, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance.

Ce règlement d'application est disponible sur Eur-Lex.

La directive NIS2 donne à la Commission européenne le pouvoir d'adopter des règlements d'application dans des cas spécifiques.

L'article 21, § 5, al. 1 de la directive, porte sur les **exigences techniques et méthodologiques liées aux mesures de gestion des risques** en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, 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, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance.

Article 23, § 11 de la directive, porte sur la **notion d'incident significatif** pour les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, 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, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux.

La directive NIS2 envisage également la possibilité (facultative) d'autres règlements d'exécution :

- un règlement d'exécution fixant des exigences techniques et méthodologiques ainsi que des exigences sectorielles pour d'autres types d'entités essentielles et importantes (art. 21, § 5, al. 2) ;
- un règlement d'exécution précisant plus en détail le type d'informations, le format et la procédure pour les notifications et les communications relatives aux notifications d'incidents (art. 23, § 11, al. 1) ;

- un règlement d'application détaillant la notion d'incident significatif pour d'autres types d'entités essentielles et importantes (art. 23, § 11, al. 2, in fine) ;

Cependant, il n'y a pas de projet pour ces règlements d'exécution pour le moment.

5.2. Existe-t-il au sein de l'organisation une personne spécifique chargée de mettre en œuvre les mesures de cybersécurité ?

La loi NIS2 ne nécessite pas de désigner une personne spécifique (comme un DPO dans le cadre du RGPD) au sein de l'organisation en charge de la mise en œuvre des exigences NIS2.

5.3. Existe-t-il une liste publique de toutes les entités essentielles et importantes ?

La directive NIS2 impose aux États membres de dresser une liste de toutes les entités essentielles et importantes et de communiquer des informations statistiques sur cette liste (nombre d'entités par secteur ou sous-secteur) au groupe de coopération NIS et à la Commission européenne.

Art. 3, § 3 à 6 de la directive NIS2

Toutefois, cette liste n'est pas accessible au public.

Tableau de correspondance

Version 1.0	Version 2.0	Version 2.1
1.1	1.1	1.1
	1.2	1.2
1.2	1.3	1.3
	1.4	1.4
1.3	1.5	1.5
		1.5.1
		1.5.2
	1.6	1.6
1.4	1.7	1.7
	1.8	1.8
1.5	1.9	1.9
1.6	1.10	1.10
1.7	1.11	1.11
1.8	1.12	1.12
	1.13	1.13
1.9	1.14	1.14
	1.15	1.15
	1.15.1	1.15.1
	1.15.2	1.15.2
	1.15.3	1.15.3
	1.15.4	1.15.4
	1.15.5	1.15.5
	1.16	1.16
	1.16.1	1.16.1
	1.16.2	1.16.2
	1.16.3	1.16.3
	1.16.4	1.16.4
	1.16.5	1.16.5
	1.16.6	1.16.6
	1.16.7	1.16.7
1.10	1.17	1.17
1.11	1.18	1.18
1.12	2.7	2.7
1.13	1.19	1.19
	1.20	1.20
1.14	1.21	1.21
1.14.1	1.21.1	1.21.1
	1.21.2	1.21.2
1.14.2	1.21.3	1.21.3
1.14.3	1.21.4	1.21.4
1.14.4	1.21.5	1.21.5

1.14.5	1.21.6	1.21.6
	1.22	1.22
	1.22.1	1.22.1
	1.22.1.1	1.22.1.1
		1.22.1.2
	1.22.1.2	1.22.1.3
	1.22.2	1.22.2
	1.22.2.1	1.22.2.1
		1.22.2.2
		1.22.3
		1.22.3.1
	1.22.3	1.22.4
		1.22.4.1
		1.22.4.2
		1.22.4.3
		1.22.4.4
		1.22.4.5
		1.22.4.6
		1.22.4.7
	1.22.4	1.22.5
	1.22.4.1	1.22.5.1
	1.22.4.2	1.22.5.2
	1.22.4.3	1.22.5.3
	1.22.4.4	1.22.5.4
	1.22.4.5	1.22.5.5
	1.22.4.6	1.22.5.6
	1.22.4.7	1.22.5.7
		1.22.5.8
		1.22.5.9
	1.22.5	1.22.6
	1.22.5.1	1.22.6.1
	1.22.6	1.22.7
	1.22.6.1	1.22.7.1
	1.22.6.2	1.22.7.2
		1.22.7.3
	1.22.7	1.22.8
	1.22.8	1.22.9
		1.22.10
	1.22.9	1.22.11
	1.22.9.1	1.22.11.1
	1.22.9.2	1.22.11.2
	1.22.9.3	1.22.11.3
	1.22.9.4	1.22.11.4
		1.22.11.5
	1.22.10	1.22.12

		1.22.12.1
		1.22.12.2
	1.22.10.1	1.22.12.3
	1.22.10.2	1.22.12.4
	1.22.11	1.22.13
		1.22.13.1
	1.22.11.1	1.22.13.2
	1.22.12	1.22.14
	1.22.12.1	1.22.14.1
	1.22.12.2	1.22.14.2
2.1	2.1	2.1
	2.2	2.2
	2.2	2.2
2.2	2.4	2.4
2.3	2.5	2.5
	2.6	2.6
	2.7	2.7
	2.8	2.8
	2.9	2.9
		2.10
		2.11
3.1	3.1	3.1
3.2	3.2	3.2
3.3	3.3	3.3
3.3.1	3.3.1	3.3.1
	3.3.2	3.3.2
3.3.2	3.3.3	3.3.3
3.3.3	3.3.4	3.3.4
3.3.4	3.3.5	3.3.5
3.3.5	3.3.6	3.3.6
	3.4	3.4
3.4	3.5	3.5
3.5	3.6	3.6
	3.7	3.7
	3.8	3.8
	3.11	3.11
3.6	3.12	3.12
3.7	3.13	3.13
	3.13.1	3.13.1
	3.13.2	3.13.2
	3.13.3	3.13.3
		3.13.4
	3.13.4	3.13.5
	3.13.5	3.13.6
	3.13.6	3.13.7

	3.13.7	3.13.8
	3.13.8	3.13.9
	3.13.9	3.13.10
	3.13.10	3.13.11
3.8	3.14	3.14
3.9	3.15	3.15
4.1	4.1	4.1
4.1.1	4.1.1	4.1.1
4.1.2	4.1.2	4.1.2
4.1.3	4.1.3	4.1.3
4.2	4.2	4.2
4.2.1	4.2.1	4.2.1
4.2.2	4.2.2	4.2.2
	4.3	4.3
4.3	4.4	4.4
	4.5	4.5
4.4	4.6	4.6
	4.7	4.7
4.5	4.8	4.8
4.6	4.9	4.9
	4.10	4.10
4.7	4.11	4.11
	4.12	4.12
4.8	4.13	4.13
4.9	4.14	4.14
		4.14.1
		4.14.2
4.10	4.15	4.15
	4.16	4.16
4.11	4.17	4.17
4.12	4.18	4.18
4.12.1	4.18.1	4.18.1
4.12.2	4.18.2	4.18.2
		4.19
4.13	3.9	3.9
4.14	3.10	3.10
5.1	5.1	5.1
	5.2	5.2
	5.3	5.3