Version 1.0
07/2024

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.

Table des matières

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 : *Belgische Accreditatie-instelling* (Organisme d'accréditation belge)
- CAB : *Conformity Assessment Body* (organisme d'évaluation de la conformité)
- CCB : Centre pour la Cybersécurité Belgique (autorité nationale de cybersécurité & CSIRT national)
- CSIRT : Centre de réponse aux incidents de cybersécurité (*Computer Security Incident Response Team)* (en Belgique le CSIRT national est le CCB)
- CyFun® : Référentiel Cyberfondamentaux (*Cyberfundamentals Framework*), disponible sur SafonwebAtWork
- 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. 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 d'être au moins considéré comme 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 répondent à la notion de 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 répondent à la notion de « moyenne entreprise » au sens de la Recommandation 2003/361/CE ;
- soit repris dans l'annexe II et qui répondent aux notions de moyenne ou de grande entreprise, au sens de la Recommandation 2003/361/CE ;

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 service repris dans les annexes prend en considération le caractère principal ou accessoire de l'activité concernée, une entité tombe dans le champ d'application de

la loi **même si le service essentiel qu'elle fournit n'est qu'une partie accessoire de toutes ses activités.**

Pour plus d'informations, voir les sections suivantes.

1.3. Comment calculer la taille d'une entité ?

Art. 3, §§ 1 et 2 loi NIS2

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 lorsqu'elle :

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

Pour l'application de ces seuils des 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 grande entreprise**, sans que cela ait d'impact sur la qualification d'une organisation en tant que moyenne entreprise.

Une organisation est qualifiée de grande entreprise, lorsqu'elle :

- soit occupe 250 personnes ou plus (salariés, personnel temporaire ou intérimaire, exploitants, associés, etc.) - effectif calculé par unité de travail par année (UTA) ;
- soit 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.

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 1.14.2. et le guide détaillé sur le calcul de la taille pour plus de détails.

1.4. 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 déterminé** 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 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 1.14.3. pour plus de détails et le test champ d'application NIS2.

1.5. 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.

1.6. 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 entité relève de plusieurs secteurs. 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 qualifiée comme une entité essentielle ;
- L'entité relèvera alors potentiellement 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 (que celui de l'administration publique) des annexes de la loi relève uniquement de ce secteur (et non simultanément de ce secteur et du secteur de l'administration publique).

1.7. 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 4.3.

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.).

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

D'initiative ou sur proposition de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité (CCB) peut identifier une entité comme essentielle ou importante, quelle que soit sa taille, dans les cas suivants :

Art. 11 loi NIS2

1. l'entité est le seul prestataire, en Belgique, d'au moins un service essentiel au maintien d'activités sociétales ou économiques critiques, notamment 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.

Un projet de décision d'identification est communiqué à l'entité concernée et ensuite aux éventuelles entités fédérées concernées ainsi qu'aux autorités sectorielles, qui rendent un avis non publié endéans les soixante jours.

En cas d'avis défavorable d'une autorité sectorielle et si le CCB souhaite maintenir son projet de décision, le projet de décision, accompagné de l'avis, est soumis au Comité stratégique du renseignement et de la sécurité (créé par l'arrêté royal du 22 décembre 2020) qui rend un avis contraignant. En fonction de cet avis, le CCB procédera, ou non, à l'identification.

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.

1.9. Quel est le champ d'application territorial de la loi ? Quid en cas d'entités actives dans plusieurs pays (multinationales, ...) ?

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.

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 »*.

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 ou d'une filiale ayant la personnalité juridique.

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

1) La loi belge s'applique aux fournisseurs de réseaux de communications électroniques publics et fournisseurs de services de communications électroniques accessibles au public quand ils fournissent leur service en Belgique ;
2) La loi belge s'applique aux fournisseurs de services DNS, registres de noms de domaine de premier niveau, entités fournissant des services d'enregistrement de noms de domaine, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données, fournisseurs de réseaux de diffusion de contenu, fournisseurs de services gérés, fournisseurs de services de sécurité gérés, ainsi qu'aux fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux, lorsqu'ils ont leur établissement principal en Belgique ou leur représentant pour l'Union européenne en Belgique*;
3) La loi belge s'applique à toutes les entités de l'administration publique qui ont été créés par la Belgique.

La notion d'« établissement principal » vise l'établissement où l'entité prend les décisions liées aux mesures de gestion des risques de cybersécurité. Si on ne peut pas déterminer cet endroit ou qu'il est hors-UE, on vise alors l'établissement où l'entité conduit ses opérations de cybersécurité. Si cet endroit est à nouveau indéterminable, la notion vise l'établissement avec le plus grand nombre d'employés.

(*) Si une entité visée au point 2) n'est pas établie dans l'UE, mais y fournit ses services, elle doit désigner un représentant qui est établi dans un État membre où elle fournit ses services. Si ce représentant se trouve en Belgique, l'entité sera considéré comme ayant son établissement principal en Belgique.

Si une entité dispose de plusieurs établissements répartis dans plusieurs pays différents de l'Union européenne, elle sera soumise aux lois de transposition dans chacun des Etats membres concernés. Les différentes autorités nationales compétentes collaboreront ensemble dans le cadre de l'inspection et de la notification des incidents significatifs.

1.10. 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 Resiliance 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.

Le champ d'application de NIS2 et DORA se chevauchent pour certaines 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, la norme juridique spécifique (ici le Règlement DORA) s'appliquent plutôt que la norme juridique générale (ici la directive NIS2).

Toutefois, il est prévu que les entités du secteur bancaire et financier qui relèvent à la fois du champ d'application du Règlement DORA et de la directive NIS2 doivent s'enregistrent comme les autres entités NIS2.

Enfin, les incidents significatifs notifiés par les entités DORA seront transmis aux autorités NIS2.

1.11. Est-ce que les infrastructures critiques (ou entités critiques identifiés dans le cadre de la directive CER) tombent dans le champ d'application de la loi NIS2 ?

Art. 9, 5° et 25, §2 loi NIS2

Oui, l'exploitant d'une ou plusieurs infrastructure(s) critique(s) identifié dans le cadre de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (ou comme entités critiques au sens de la directive 2022/2557 – directive CER) est considéré comme une entité essentielle au sens de la loi NIS2.

Les autorités NIS2 et les autorités compétentes en vertu de la loi du 1er juillet 2011 (et de la directive CER) 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.

1.12. 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

Le secteur de l'enseignement ne figure pas explicitement dans les annexes I et II de la loi NIS2.

Par contre, des établissements d'enseignement publics, comme par exemple des universités ou des hautes écoles, pourraient entrer dans la définition d'une « entité de l'administration publique ». Pour cela, il faut que ces derniers :

- remplissent le critère de taille (voir section 1.3.) ;
- soient établies en Belgique (voir section 1.9.) ;
- rencontre la définition d'une entité de l'administration publique à l'article 8, 34° loi NIS2 ;
- dépendent de l'État fédéral ou des entités fédérées ;

Par ailleurs, un établissement d'enseignement pourrait également être qualifié de « prestataire de soins de santé » au sens de l'annexe I de la loi NIS2 (par exemple, un hôpital universitaire).

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

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.

Pour toutes les entités qui ne sont pas dans le cas précité, les codes NACE ne constituent pas une base valable pour déterminer si une entité tombe dans le champ d'application de la loi NIS2. Certains codes NACE peuvent être utilisés de manière préliminaires par les entités, mais une vérification plus approfondie de leur activité économique exacte est nécessaire afin de déterminer si elles relèvent ou non du champ d'application souvent plus restrictif de la loi NIS2.

1.14. 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. Mon organisation exploite-t-elle une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ?
    b. Mon organisation est-elle un opérateur de services essentiels ou un fournisseur de services numériques (loi NIS1) ?
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.

1.14.1. 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 organisation concernée.

A. Mon organisation exploite-t-elle une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ?

L'article 3, §4 de la loi NIS2 précise que la loi s'applique automatiquement aux entités identifiées comme exploitants d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (et dans le futur aux entités critiques au sens de la directive CER), quelle que soit leur taille.

Les exploitants d'une infrastructure critique ne doivent donc pas analyser si leur organisation entre ou non dans le champ d'application de la directive NIS2 : ils sont automatiquement qualifiés en tant qu'entités essentielles.

B. Mon organisation est-elle un opérateur de services essentiels (OSE) ou un fournisseur de services numériques (FSN) ?

Les entités identifiées comme opérateurs de services essentiels (OSE) ou qui étaient fournisseurs de services numériques (FSN) dans le cadre de la 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 (loi NIS1) seront soumis aux dispositions de la loi NIS2. En effet, le champ d'application de la directive NIS2 s'est construite sur base des secteurs de la directive NIS1.

Les OSE doivent, en absence d'une identification formelle par le CCB, satisfaire au critère de taille (voir le point suivant). Les FSN, eux, devaient déjà être au moins des moyennes entreprises sous la Recommandation 2003/361/CE.

1.14.2. 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 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'affaire 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'affaire 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'affaire. Il s'agit donc d'une petite ou micro entreprise.

Exemple 2 : une entreprise de 80 UTA (moyenne) a un chiffre d'affaire 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'affaire. 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 :

- Une moyenne entreprise a un effectif entre 50 et 249 UTA ou a un chiffre d'affaires annuel / 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 elles 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 1.3.).

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.

[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.

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 (essentiel) ;
- fournisseurs de services de communications électroniques accessibles au public (essentiel) ;
- entités identifiées comme critiques au niveau national en vertu de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures 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.

1.14.3. 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 usés 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 1.6.).

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 1.14.2. précédente):

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

1.14.4. 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 de la loi NIS2 belge sont expliqués à la section 1.9.

1.14.5. 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 1.8.

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 3.8.

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, 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 créés 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.

2.2. Les entités publiques locales sont-elles soumises aux obligations de la loi ?

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

Les entités publiques locales (communes, provinces, intercommunales, CPAS, régies, etc.) ne sont pas automatiquement soumises aux exigences de la loi NIS2. 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 sont soumises aux dispositions de la loi NIS2 lorsqu'elles fournissent un service repris à l'annexe I ou II de la loi et dispose d'une taille supérieure à celle d'une petite entreprise.

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.

2.3. 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 entités publiques régionales et communautaires font parties des entités de l'administration publique visées par la loi NIS2. 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.

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 ;
- la formation des organes de direction (section 4.13.) ;
- 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.

On peut souligner que le référentiel CyFun® du CCB est aligné sur les travaux du Groupe de coopération NIS à ce sujet.

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.

3.3. Quelles sont les obligations en matière 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.

La notification se fait en plusieurs étapes (voir section 3.3.3.): 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.

Un incident significatif est défini come : « *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*.»

En pratique, le CCB fournira des recommandations sur les hypothèses où une notification est requise et sur la procédure à suivre.

3.3.2. 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 incident significatifs qui pourraient nuire aux services que cette dernière leur fournit. Elle communique également aux destinataires qui sont potentiellement affectés par une cybermenace importante toutes les corrections et mesures que ceux-ci peuvent appliquer en réponse.

Art. 34, §2 loi NIS2

3.3.3. 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 aura lieu via la procédure établie sur le site du CCB.

3.3.4. 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.

3.3.5. 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. 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'APD peut se faire sur leur site internet.

3.5. 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.

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

3.6. 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.

3.7. Comment s'enregistrent les entités NIS2 ?

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.

3.8. Comment gérer en tant qu'entité les relations avec ses fournisseurs et prestataires directs ? (*supply chain*)

Les entités couvertes par la loi NIS2 doivent prendre des mesures appropriées et proportionnées pour sécuriser leur réseau et leurs systèmes d'information.

Art. 30, §3, 4° loi NIS2

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.

Si les exigences de la loi NIS2 ne s'appliquent qu'aux entités NIS2, celles-ci devront néanmoins s'assurer que leurs fournisseurs et prestataires directs mettent en œuvre des mesures similaires. Pour assurer le respect de ses obligations légales, une entité NIS2 peut contractuellement demander à ses fournisseurs ou prestataires de disposer de l'une des certifications reconnues dans le cadre de la loi NIS2 : CyFun® ou ISO 27001.

3.9. Quel est le degré de confidentialité des informations échangées ?

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.

Art. 26 loi NIS2

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 seront 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 secteur 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. Certains cadres de référence peuvent-ils 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 (4.3.).

4.2.1. Le CyberFundamentals (CyFun®) Framework

Le cadre des CyberFundamentals, développé par le CCB, est basé sur plusieurs cadres ou normes de cybersécurité couramment utilisés, dont NIST CSF, ISO 27001 / ISO 27002, CIS Controls et IEC 62443.

Il se compose du niveau de départ Small et de plusieurs niveaux d'assurance : Basic, Important et Essential (pour répondre au mieux aux risques auxquels une organisation peut être exposée). Un outil permet de sélectionner le niveau le plus appropriée à appliquer.

Ce référentiel est disponible gratuitement et publiquement sur notre site Safeonweb@Work.

4.2.2. ISO/IEC 27001

La norme européenne ISO/IEC 27001 est une norme technique internationalement reconnue qui fixe l'approche générale et structurée à adopter pour disposer d'une gestion de la sécurité de n'importe quel système d'informations. Il s'agit donc d'une norme de base fixant les principes généraux pour la mise en œuvre de toute mesure de sécurité d'un système d'information et est applicable dans tous les secteurs.

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.

4.3. Comment se déroulera le contrôle des entités concernées ?

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 réalisé 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 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 4.10.

4.4. 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 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 27001, il est accrédité par un organisme d'accréditation qui a signé la convention de reconnaissance mutuelle (MLA) dont relève la norme ISO 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.

Les CAB jouent un rôle important dans notre économie pour assurer que des entreprises répondent correctement aux exigences règlementaires qui leurs sont imposées.

4.5. 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 différents situations sur ce sujet);
- Supervision et inspection (conjointe ou déléguée) ;
- Amendes administratives.

4.6. Comment une entité peut-elle prouver qu'elle est en conformité avec ses obligations ?

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.

Art. 42 loi NIS2

Art. 5, §1 arrêté royal NIS2

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

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 toute les mesures requises en s'appuyant sur une table de concordance (mapping) avec l'un des deux référentiels précités.

4.7. Est-ce qu'une entité peut utiliser un niveau d'assurance CyFun® inférieur au niveau assorti à sa catégorie d'entité?

Art. 7 arrêté royal NIS2

Oui, l'arrêté royal laisse la possibilité à une entité de recourir à un niveau CyFun® inférieur (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 que 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.

4.8. 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 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.

4.9. À partir de quand les entités concernées devront appliquer les obligations de la loi ?

Art. 13 & 75 loi NIS2

Art. 22-23 arrêté royal NIS2

La loi et l'arrêté royal NIS2 seront en vigueur à partir du 18 octobre 2024. Dès lors et sauf exception, **toutes les obligations** de la loi et de l'AR s'appliqueront aux entités essentielles et importantes (mesures de cybersécurité, notification d'incidents, etc.) **à partir de cette date**.

Par dérogation, l'obligation d'enregistrement fera l'objet d'une mise en œuvre progressive dans le temps. Le délai dépend du type d'entité (voir section 3.7.) :

- En principe, les entités ont **5 mois** pour s'enregistrer après l'entrée en vigueur de la loi.
- Pour les entités relevant de certains secteurs liés aux technologies de l'information et de la communication (fournisseurs cloud, services DNS, centres de données, etc.), le délai pour s'enregistrer est de **2 mois** après l'entrée en vigueur de la loi.

Par dérogation, l'évaluation régulière de la conformité des entités essentielles suivra également une mise en œuvre progressive et différenciée en fonction du référentiel choisi :

- **18 mois après l'entrée en vigueur de la loi**, soit avant le 18 avril 2026 :
  - Celles qui déterminent qu'elles doivent se conformer aux niveaux d'assurance CyFun® Basic ou Important doivent faire effectuer une vérification par un CAB accrédité et agrée pour CyFun®. Celles qui déterminent qu'elles doit se conformer au niveaux d'assurance CyFun® Essential doivent également faire effectuer une telle vérification Basic ou Important ;
  - Celles qui ont choisi une certification ISO 27001 doivent transmettre le champ d'application et de la déclaration d'applicabilité au CCB ;
  - Celles qui ont choisi l'inspection par le CCB doivent transmettre l'auto-évaluation CyFun® ou la politique de sécurité de l'information, le champ d'application et la déclaration d'applicabilité ISO 27001 au CCB.
- **30 mois après l'entrée en vigueur de la loi**, soit avant le 18 avril 2027 :
  - Celles qui déterminent qu'elles doivent se conformer au niveau d'assurance CyFun® Essential doivent, en plus de la vérification Basic ou Important précitée, acquérir une certification par un CAB accrédité et agrée pour CyFun® ;
  - Celles qui ont choisi une certification ISO 27001 doivent acquérir une certification par un CAB accrédité et agrée pour ISO 27001 ;
  - Celles qui ont choisi l'inspection par le CCB doivent transmettre un état de l'avancement de la mise en 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 supervisera les entités importantes, en respectant une période similaire de 18 mois après l'entrée en vigueur de la loi (pour leur permettre d'atteindre complètement le niveau requis).

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.

4.10. Quelles sont les modalités de l'inspection ?

Art. 44 et s. 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 27001 ou des CyberFundamentals (voir section 4.3.).

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 possible. 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.

4.11. Est-ce que les mesures et les amendes administratives sont proportionnelles ? Quelles sont les montants des amendes ?

L'objectif des mesures et amendes administratives est de renforcer le niveau de cybersécurité des entités essentielles et importantes. *Art. 59 loi NIS2*
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.

4.12. Quelles autres mesures administratives peuvent-elles être prises ?

4.12.1. Mesures de base

Les mesures administratives suivantes peuvent être imposées aux entités essentielles et importantes :

Art. 58 loi NIS2

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.

4.12.2. 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 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.

4.13. Quelles sont les obligations et responsabilités du management ?

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 obligation en matière de mesure de gestion des risques, l'organe de direction en est responsable.

Art. 31 & 61 loi NIS2

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 impact 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.

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

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

D'un point de vue de droit européen, la Cour de justice a rappelé à plusieurs reprises : premièrement, que si un mot ou un concept n'est pas définit dans l'instrument légal, qu'on doit retenir son sens usuel ; et deuxièmement, sauf indication contraire, que chaque concept dans le droit européen devrait être revêtu de la même définition. Une telle définition peut être trouvé dans la directive 2013/36, à l'article 3, §1, (7) : « *l'organe ou les organes d'un établissement, qui sont désignés conformément au droit national, qui sont compétents pour définir la stratégie, les objectifs et la direction globale de l'établissement et qui assurent la supervision et le suivi des décisions prises en matière de gestion et, en ce compris, les personnes qui dirigent effectivement les activités de l'établissement*».

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.

5. Autres

5.1. La Commission européenne doit-elle encore adopter des actes d'exécution ?

Oui, un acte d'exécution qui doit nécessairement être adopté par la Commission européenne au plus tard pour le 17 octobre 2024 vise un nombre limité d'entités soumise à la directive pour lesquelles certaines modalités sont prévues au niveau européen de manière harmonisée.

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.

Ces dispositions mentionnent également que la Commission doit suivre, dans la mesure du possible, les normes européennes et internationales ainsi que les spécifications techniques pertinentes. La Commission doit également échanger des conseils et coopérer avec le groupe de coopération et l'ENISA sur ces projets d'actes d'exécution.

Concrètement, le futur acte d'exécution devrait viser exclusivement les éléments suivants (la Commission a fait part de sa volonté si possible d'adopter les deux types de précisions dans un seul acte) :

- détails sur les exigences techniques et méthodologiques liées aux mesures de gestion des risques pour ces entités spécifiques ;
- détails sur la notion d'incident significatif pour ces entités spécifiques, à l'exclusion des fournisseurs de services de confiance (*trust service providers*).

L'ENISA et les groupes de travail (*workstreams*) du groupe de coopération NIS travaillent actuellement à fournir des conseils à la Commission en préparation de la procédure de Comitologie.

Sur base de ces échanges, la Commission va formuler une proposition d'acte d'exécution qui sera ensuite partagée et discutée au sein du Comité NIS2 (une fois celui-ci formellement constitué). Le Comité devra suivre les règles en matière de comitologie visée dans le Règlement (UE) n° 182/2011.