DIRECTIVE NIS 2

Analyse Détaillée

Novembre 2023

ACN

Alliance pour la confiance numérique

SOMMAIRE

INTRODUCTION ..... 3.

La directive NIS (2016) : L'instauration d'un cadre européen de gestion de la cybersecurité 3
La directive NIS 2 (2023) repond au besoin d'ameliorer le niveau commun de la cybersecurité 4

I - ELARGISSEMENT DU CHAMP D'APPLICATION POUR COUVRIR TOUS LES SECTEURS ET INFRASTRUCTURES ..... 5.

I.A. Extension du périmètre et des domaines d'application pour inclure toutes les entités vulnérables 5

I.A.1. Le régime des « opérateurs » recatégorisé en « entités » pour englober toutes les parties vulnérables 5

I.A.2. Répartition des entités par secteurs d'activités critiques ou hautement critiques 6

I.A.3. Création de listes nationales des entités concernées 7

I.B. Distinction des entités par leur taille pour des exigences proportionnelles 8

I.C. La directive ne s'applique pas aux entités souveraines ou qui communiquent déjà leurs incidents 9

II - PLUS D'OBLIGATIONS IMPOSÉES SUR LES ENTITÉS PAR L'UNION EUROPÉENNE .....10.

II.A. Obligation de notifier les incidents à son CSIRT dans les délais impartis 10

II.B. Les exigences de gestion des risques harmonisées à l'échelle européenne 11

II.C. Chaque État membre intègre et supervise la sécurité physique de ses entités 12

III - RENFORCEMENT DE LA COOPÉRATION ENTRE LES ETATS MEMBRES ..... 13.

III.A. Organisation d'un cadre commun de divulgation des incidents et de gestion des risques 13

III.B. Recours aux schémas européens de certification obligatoires 14

SOMMAIRE

IV - RENFORCEMENT DES SANCTIONS PÉNALES ET PÉCUNIAIRES ..... 16.

IV.A. Harmonisation et imposition de mesures plus coercitives à l'échelle européenne 16

IV.B. Nouveauté : engagement de la responsabilité des organes de gestion et des dirigeants 17

IV.C. Des amendes proportionnelles et plus dissuasives 17

CONCLUSION ..... 18.

ANNEXES ..... 20.

Calendrier d'application de NIS 2 20

Détail des entités de secteurs heutement critiques désignés par NIS 2 (annexe 1) 21

Détails des secteurs critiques définis par NIS 2 (annexe 2) 29

Définitions 32

Sources 34

INTRODUCTION

La directive NIS (2016) : l'instauration d'un cadre européen de gestion de la cybersécurité

La directive NIS *(Security of Network and Information Systems)* publiée en juillet 2016 a pour objectif d'établir des mesures communes de sécurité des réseaux et des systèmes d'information à l'échelle de l'Union européenne dans le but de réduire les impacts des menaces dans les secteurs clés. En effet, le développement du numérique dans toutes les formes d'échanges a contribué à l'augmentation de la menace cyber. L'interconnexion des pays de l'Union et de leurs échanges accroit les points de vulnérabilités. L'organisation d'une coopération effective est née du besoin de se protéger de la propagation des attaques cyber dans le réseau européen, de prévenir leurs impacts sur la société et de sensibiliser les Etats membres au risque cyber.

La directive NIS a renforcé les capacités de coopération à l'échelle européenne en élaborant un cadre de gestion de la cybersécurité dans l'Union. Des groupes de travail opérationnels ont alors été créés dans le but de structurer les échanges entre les Etats membres. Les Etats membres sont notamment réunis, sur ce sujet, au sein du Groupe de coopération. Chacun a désigné une autorité nationale compétente en charge de la gestion des crises cyber pour faire partie du groupe EU-CyCLONe. Enfin, la directive NIS a permis la mise en place d'un réseau de CSIRTs *(Computer security incident response team)* composé des représentants nationaux des CSIRTs régionaux de chaque Etat membre. De plus, les Etats membres de l'Union européenne ont reçu l'obligation de définir une stratégie nationale de cybersécurité.

En France, l'Agence nationale de la sécurité et des systèmes d'information (ANSSI) assume le rôle à la fois d'autorité nationale compétente et de représentant national des CSIRT sous le nom de CERT-FR. Elle est un acteur déterminant de la transposition de la directive en stratégie nationale. Depuis NIS 1, l'ANSSI a eu la charge d'établir une liste d'opérateurs de services essentiels (OSE) au fonctionnement de l'économie et de la société européennes et de désigner des fournisseurs de services numériques (FSN) parmi les moteurs de recherche, les places de marché et les services de cloud. Ces entités sont comprises dans le champ d'application définit par la directive NIS 1, qui cible les grands acteurs économiques du marché intérieur de l'Union européenne selon les impacts économiques et sociétaux des services fournis. Elle impose à ces différents acteurs des obligations en matière de sécurité et de notification aux autorités désignées des incidents de sécurité informatique dans le but d'améliorer la continuité des services impactés.

La directive NIS 2 (2023) répond au besoin d'améliorer le niveau commun de cybersécurité

L'augmentation de la fréquence et des impacts des incidents a révélé des lacunes alors que le nombre d'OSE et de leurs systèmes d'information essentiels (SIE) identifiés dans le champ d'application est en augmentation. Les critères de définitions établis par NIS 1 excluent désormais des entités dont le dysfonctionnement pourrait pourtant porter atteinte à la sécurité du système économique et de la société des États membres.
En particulier, les chaines d'approvisionnement, les PME, les TPE, deviennent des voies de passage privilégiées des cyberattaquants alors qu'elles ne rentrent pas dans le champ d'application de la directive. Enfin, l'hétérogénéité dans les pratiques et les mises en œuvre de la directive NIS 1 entre les Etats membres est encore trop importante.

Dans le cadre de sa stratégie visant à renforcer le niveau global de cybersécurité des États membres et des entreprises dans l'Union, la Commission européenne a proposé une révision de la directive NIS permettant de protéger le marché intérieur de l'Union européenne et de réduire les divergences d'applications.

La directive NIS 2 a été publiée le 27 décembre 2022 au Journal officiel de l'Union européenne[1] et est entrée en vigueur le 17 janvier 2023. Les États membres ont jusqu'en octobre 2024 pour la transposer en politique nationale.

La directive NIS 2 s'inscrit dans le prolongement de NIS 1 pour garantir un cyberespace de confiance pour la société et l'économie en augmentant le niveau de cyber-résilience.
Elle favorise le partage d'informations et la capacité collective de préparation et de réponse aux attaques. Elle réponds au besoin d'harmoniser sa mise en œuvre entre les Etats membres de l'Union, de redéfinir son périmètre et de passer de la cybersécurité des opérateurs critiques à une cybersécurité de masse.
La directive NIS 2 implique donc plus d'entités et est plus exigeante envers les acteurs concernés.

[1] Journal Officiel de l'Union européenne, « 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 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE) », Lex Europa, 27 décembre 2022. URL : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC

I - Elargissement du champ d'application pour couvrir tous les secteurs et infrastructures

I.A. Extension du périmètre et des domaines d'application pour inclure toutes les entités vulnérables

I.A.1. Le régime des « opérateurs » recatégorisé en « entités » pour englober toutes les parties vulnérables

La directive NIS 2 élargit le champ d'application de NIS 1 dans le but de sécuriser l'ensemble des systèmes d'information vulnérables. Les opérateurs de services essentiels (OSE) et les fournisseurs de services numériques (FSN) définis dans le champ d'application de NIS 1 sont pour cela recatégorisés en entités essentielles (EE) et en entités importantes (EI). Le niveau « important » permet d'inclure davantage d'entités, qui ne sont donc plus restreintes aux services essentiels.

Les entités relèvent de l'Etat membre dans lequel elles sont établies, exceptés les fournisseurs de réseaux de communication électroniques qui relèvent du pays dans lequel ils établissent leur service. Les acteurs du numérique relèvent de la compétence de l'Etat membre où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité.

Toutes les entités désignées comme OSE par NIS 1 deviennent des entités essentielles dans NIS 2. L'Etat est également en mesure de désigner des entités comme essentielles. D'une manière générale, les grandes entreprises et les ETI des secteurs d'activités hautement critiques (définis à l'annexe 1 de la directive NIS 2)[2] sont des EE par défaut, à l'exception des prestataires de services de confiance qualifiés, des registres de noms de domaine de premier niveau et des fournisseurs de services DNS.

Les entités importantes (EI) sont toutes les entités qui entrent dans le champ d'application de la directive et qui ne sont pas des entités essentielles. Les grands groupes et les ETI sont des EI si leurs activités font partie des secteurs critiques (définis en annexe 2 de la directive)[3]. En outre, toutes les entreprises de tailles moyennes sont désignées comme des EI.

[2] *Annexe à la page 22*
[3] *Annexe à la page 30*

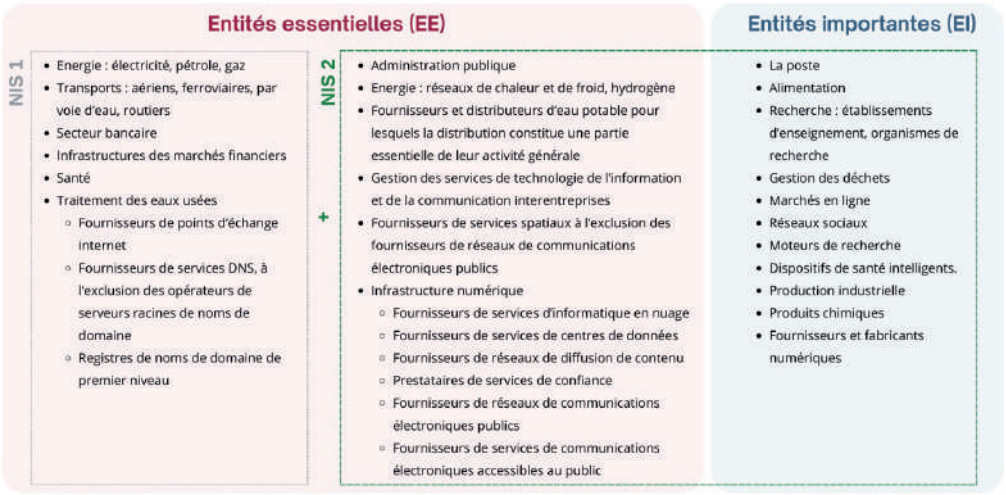
I.A.2. Répartition des entités par secteurs d'activités critiques ou hautement critiques

Les entités qui entrent dans le champ d'application de la directive NIS 2 sont classées selon leur domaine d'activité. La liste des secteurs et des activités concernés par les obligations en cybersécurité est ainsi agrandie. Les secteurs d'activités et leurs sous-secteurs sont répartis d'une part en secteurs hautement critiques (Annexe 1) et d'autre part en secteurs critiques (Annexe 2). Chaque secteur ou sous-secteur d'activité correspond à des activités métiers. Ce nouveau champ permet également de prendre en compte des secteurs qui ne rentraient pas dans le champ d'application de NIS 1, tel que les administrations publiques, l'énergie ou encore les fournisseurs et distributeurs d'eau potable. L'accent a notamment été mis sur la sécurité des chaînes d'approvisionnement numériques.

En particulier, en plus des activités exercées dans les secteurs hautement critiques, une entité est considérée comme essentielle dans le cas où :

- Ses services sont fournis par des :
  - fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public,
  - prestataires de services de confiance,
  - registres des noms de domaine de premier niveau et des fournisseurs de services de système de noms de domaine ;
- Elle détient des entités au sein desquelles une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité, la sûreté ou la santé publiques ou induire un risque systémique important ;
- Elle est une entité d'importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants dans l'État membre.
- Elle est une entité de l'administration publique des pouvoirs publics centraux ou elle est elle-même un pouvoir public central.

Entités entrant dans le champs d'application de NIS 2 selon le domaine d'activité



En France, NIS 2 s'applique à des milliers d'entités désormais régulées au sein de dix-huit secteurs (11 secteurs hautement critiques et 7 secteurs critiques)[4]. Près de 600 types d'entités différentes sont concernées, parmi elles des administrations centrales, des collectivités territoriales, des établissements d'enseignement, des entreprises allant des PME aux groupes du CAC40 ou encore des acteurs du numérique.

I.A.3. Création de listes nationales des entités concernées

La directive NIS 2 impose aux Etats membres d'établir, au plus tard le 17 avril 2025, une liste des entités essentielles et importantes, ainsi que des entités fournissant des services d'enregistrement de noms de domaines. Le nombre d'entités doit être communiqué à la Commission européenne et au Groupe de coopération[5].
La liste et les informations demandées aux entités doivent être régulièrement mises à jour par les Etats membres, au minimum tous les 2 ans. Pour chaque modification de données, les entités disposent de 15 jours pour notifier le changement. En France, les entités devront fournir à l'ANSSI les données suivantes[6] :

- Nom de l'établissement
- Adresse de l'établissement principal
- Adresse des autres établissements légaux
- Contact : adresse électronique, numéro de téléphone des représentants légaux
- Adresses IP
- Etats membres où des services sont fournis
- Secteurs d'activités concernés

[4] Détails des secteurs en Annexe I et II de la directive, disponibles en pages 17 et 20 de ce document.
[5] Commission européenne, « Lignes directrices de la Commission relatives à l'application de l'article 3, paragraphe 4, de la directive (UE) 2022/2555 (directive SRI 2) », 13 septembre 2023. URL : https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-34-directive-eu-20222555-nis-2-directive
[6] Commission européenne, « Lignes directrices de la Commission relatives à l'application de l'article 4, paragraphes 1 et 2, de la directive (UE) 2022/2555 (directive SRI 2) », 13 septembre 2023. URL : https://digital-strategy.ec.europa.eu/fr/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive

I.B. Distinction des entités par leur taille pour des exigences proportionnelles

La directive NIS 2 introduit un critère de taille afin d'adapter les niveaux d'exigences imposés aux entités concernées. Cette typologie permet de prendre en compte les différences de moyens et d'enjeux économiques entre les grandes entreprises, les PME et les TPE pour mettre en œuvre les obligations de mesures de sécurité. La taille des entités se réfère à la règlementation européenne[7].

Les organisations fournissant des services essentiels sont concernées par la directive quelle que soit leur taille. Les entités de taille moyenne et grande opérant dans les secteurs ou fournissant des services couverts par les domaines de la directive entreront également dans son champ d'application. De plus, le périmètre de la directive NIS 2 intègre toutes les entités de taille moyenne, intermédiaire ou grande réalisant des activités en lien avec une entité déjà concernée.

Les TPE sont concernées uniquement si elles rentrent dans l'une des catégories suivantes :

- Les services sont fournis par un réseau de communication électronique ou un service de communication au public en ligne, un tiers de confiance ou un service de noms de domaine.
- L'entité est l'unique fournisseur d'un service dans un État membre ou est particulièrement important à un niveau régional ou national.
- La disruption du service fourni par l'entité aurait un impact sur la sécurité et/ou la santé publiques ou pourrait induire des risques systémiques.
- L'entité est identifiée comme une infrastructure critique au sens de la directive CER[8].

La directive ne s'applique pas sur les micro-entreprises, excepté dans le cas où elles sont désignées par l'État membre dont elles relèvent comme entrant dans le champ d'application. Les États membres disposeront d'orientations appropriées de la part de la Commission européenne concernant les microentreprises et les petites entreprises concernées dans ce cas.

7 Critères de taille de l'UE : https://single-market-economy.ec.europa.eu/smes/sme-definition_en

8 Directive CER : directive européenne sur la résilience des entités critiques, publiée en même temps que la directive NIS 2 en décembre 2022 et applicable dès janvier 2023 pour remplacer la directive de 2008 sur les infrastructures européennes critiques. Le texte de la directive CER est disponible sur : https://data.consilium.europa.eu/doc/document/PE-51-2022-INIT/en/pdf

I.C. La directive ne s'applique pas aux entités souveraines ou qui communiquent déjà leurs incidents

Les entités déjà soumises à des mesures équivalentes à celles des obligations de la directive ne sont pas concernées, notamment dans les cas où un accès direct et automatique aux notifications d'incidents par les CSIRTs, par les autorités compétentes ou par les points de contact existe déjà. Les serveurs racines de noms de domaine ne sont pas non plus concernés.

Les entités de l'administration publique établies conjointement avec un pays tiers conformément à un accord international, comme les établissements diplomatiques et consulaires, ne sont pas comprises dans le champ d'application. La directive ne s'applique pas non plus sur les administrations et leurs prestataires relevant des pouvoirs d'ordre souverain, telles que la sécurité nationale, la sécurité publique, les pouvoirs législatifs, judiciaires et les banques centrales.

Enfin, la directive ne s'applique pas sur les fournisseurs de réseaux de télécommunications publics, sur les prestataires de services de confiance et sur les fournisseurs de services de noms de domaines et de services réseau.

Des entités qui ne sont pas considérées comme essentielles selon le nouveau régime appliqué peuvent toutefois être identifiées comme telles par les États membres et donc rentrer dans le champ d'application de la directive. Lorsqu'il y a un doute sur la caractérisation d'une entité, les États membres le déterminent en accord avec la législation européenne.

II. Plus d'obligations imposées sur les entités par l'Union européenne

II.A. Obligation de notifier les incidents à son CSIRT dans les délais impartis

Toutes les entités entrant dans le champ d'application de la directive doivent notifier tout incident ayant un impact important sur la fourniture de leurs services à son CSIRT régional et aux destinataires de leurs services. Les obligations de notification des incidents sont ainsi rationalisées, principalement lorsqu'il s'agit des incidents de cybersécurité majeurs et des vulnérabilités soulevées lors de l'investigation sur l'origine des complications.

Les CSIRT, les autorités compétentes et les points de contact uniques désignés par les Etats membres devraient être en mesure d'obtenir un accès immédiat aux notifications d'incidents transmises sans retard injustifié.

En France, l'ANSSI assure le rôle à la fois de point de contact unique, d'autorité nationale compétente et de représentant national des CSIRTs. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification. Les notifications volontaires des entités exclues du champ d'application demeurent recommandées et prises en compte.

Les entités disposent de 24h pour notifier une alerte précoce après avoir eu connaissance de l'incident important. Dans les 72h, une nouvelle notification d'incident permet de mettre à jour les informations et de fournir une évaluation initiale de l'incident puis de déterminer les indicateurs de compromission. Les entités devront ensuite communiquer une mise à jour et une évaluation initiale de l'incident, de sa gravité et de son impact. Un rapport final est soumis dans le mois suivant la notification d'incident, comprenant une description détaillée de l'incident, un bilan de son impact, de sa gravité, du type de menace ou de la cause profonde qui a pu en être l'origine, les mesures d'atténuation appliquées et en cours ainsi que, le cas échéant, l'impact transfrontière de l'incident. Les CSIRTs ou les autorités compétentes doivent répondre si possible dans les 24h après la notification de l'alerte précoce en fournissant un retour d'information initial sur l'incident important, des orientations et des conseils opérationnels sur des mesures d'atténuation à la demande de l'entité. Ils ont aussi la possibilité de demander un rapport intermédiaire comprenant des mises à jour de la situation.

Les incidents au niveau national doivent être notifiés et remontés à l'échelle de l'Union européenne. Le point de contact unique de chaque État membre soumet tous les trois mois un rapport de synthèse à l'ENISA comprenant les données anonymisées et agrégées sur les incidents et les cybermenaces.

La Commission définira le type d'informations et le format requis par le biais d'actes d'exécutions. De plus, si un incident concerne plusieurs États membres, le CSIRT ou les autorités compétentes ayant reçu la notification doivent informer l'ENISA et les autres États membres pouvant être affectés de l'incident en passant par le point de contact unique.

II.B. Les exigences de gestion des risques harmonisées à l'échelle européenne

Afin d'assurer la continuité et la résilience des systèmes d'information, la directive NIS 2 prévoit une règle de gestion des risques en matière de sécurité physique de la cybersécurité des entités essentielles et importantes. Cette règle concerne particulièrement les entités critiques devenues des entités essentielles et les entités appartenant au secteur des infrastructures numériques.
Ces mesures sont prévues afin de prémunir contre des évènements tels que le vol, les phénomènes naturels, les défaillances techniques, les erreurs humaines ou encore les actes malveillants.
NIS 2 impose à tous les États membres de veiller à ce que les entités concernées prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services. Les actes d'exécution établissant les exigences techniques, méthodologiques et certaines sectorielles sont établis par la Commission européenne, tandis que les exigences de sécurité des entités étaient assurées par les États membres dans la directive NIS 1. Les États membres veillent également à ce que les membres de leurs organes de direction suivent une formation. Les entités sont encouragées à dispenser des formations similaires à leur personnel pour pouvoir déterminer les risques et évaluer les pratiques de gestion des risques.
Le niveau de sécurité requis est adapté et élevé à travers l'application de normes européennes. Lors de l'évaluation des risques, le degré d'exposition de l'entité, sa taille, et la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques, sont pris en compte.

Les entités sont conviées à adopter des mesures de gestion des risques en matière de cybersécurité conformes aux normes européennes sur la sécurité physique et la sécurité de l'environnement de leurs réseaux et de leurs systèmes d'information, de bout en bout. Dans le cas particulier des entités appartenant au secteur des infrastructures numériques, les obligations de la directive s'appliquent de manière globale sur la sécurité physique de leurs systèmes d'information.

Ces mesures doivent s'intégrer dans leurs mesures de gestion des risques et leurs obligations d'information. Les entités ont la responsabilité d'évaluer les vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits, y compris de leurs procédures de développement sécurisé. Elles sont également tenues de prendre en compte les résultats des évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement critiques et doivent prendre toutes les mesures nécessaires appropriées et proportionnées.

La plupart des acteurs du numérique ne sont pas soumis aux exigences relatives aux mesures de sécurité transposées à l'échelle nationale, mais à un acte d'exécution qui sera publié par la Commission au plus tard le 17 octobre 2024 qui précisera les mesures à appliquer.

II.C. Chaque État membre intègre et supervise la sécurité physique de ses entités

Chaque État membre est dans l'obligation élaborer une stratégie nationale avec l'aide de l'ENISA. La directive NIS 2 leur impose des axes stratégiques plus développés que NIS 1. Ils devront fournir leur plan stratégique à la Commission européenne dans les trois mois suivants leur adoption, comprenant notamment la liste des acteurs concernés par la stratégie nationale, un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident et un plan comprenant les mesures nécessaires pour améliorer le niveau général de sensibilisation des citoyens à la cybersécurité[9].

L'accent est mis sur la cybersécurité des chaînes d'approvisionnement, la gestion, la promotion, la facilitation et la divulgation des vulnérabilités et la promotion d'une cyber protection active à travers le développement de technologies et de formations.
Il incombe aux États membres d'intégrer la sécurité physique des entités dans leur propre stratégie nationale.

La directive n'impose pas de cadre particulier et harmonisé entre les États pour cela. La coordination et la coopération entre les acteurs nationaux concernés est cependant attendue. Les États membres sont invités à prévoir un cadre d'action adapté pour prévenir les risques, les menaces et les incidents sur les infrastructures physiques des entités. Ils jouent un rôle de supervision de la sécurité physique et non liée à la cybersécurité des entités au même titre que pour la gestion des risques et des incidents de cybersécurité.
Les États membres ont la charge de soutenir la recherche scientifique visant à développer et à améliorer le déploiement des outils de cybersécurité et à sécuriser les infrastructures de réseau.
Enfin, les États membres sont encouragés à renforcer les valeurs de cyber résilience et de cyber hygiène des petites et moyennes entreprises exclues du champ d'application de la directive en leur fournissant des orientations et un soutien répondant à leurs besoins spécifiques.

9 Les éléments sur lesquels les États membres doivent adopter des stratégies nationales sont détaillés à l'article 7.2 de la directive.

III - Renforcement de la coopération entre les Etats membres

III.A. Organisation d'un cadre commun de divulgation des incidents et de gestion des risques

Un mécanisme volontaire d'apprentissage par les pairs est mis en place afin de renforcer la confiance mutuelle et les enseignements à tirer des bonnes pratiques et des expériences au sein de l'Union européenne.
Les CSIRTs régionaux sont les premiers et les plus proches contacts des entités. Ils sont chargés de recevoir les notifications d'incidents et d'apporter réponses et conseils de gestion des incidents et des risques aux entités. Les réseaux de CSIRT nationaux sont chargés des échanges entre les États sur ces sujets. Ils sont réunis au sein du CSIRTs Network, le réseau des CSIRTs à périmètre national de l'Union européenne.

À travers le CSIRTs Network, les CSIRTs peuvent échanger des informations pertinentes avec des centres de réponse aux incidents de sécurité informatique nationaux de pays tiers, y compris des données à caractère personnel, dans le but de leur fournir une assistance en matière de cybersécurité. L'ENISA informe le groupe de coopération et le *CSIRTs Network* de ses conclusions tous les six mois. En France, le CERT-FR (ANSSI) est le représentant national du réseau CSIRT au *CSIRTs Network*.

Les États membres sont également invités à renforcer leur coopération en gestion de crise cyber en donnant un cadre plus formel et plus d'importance au réseau EU-CyCLONe (*European Cyber crisis liaison organisation network)* qui rassemble les autorités nationales en charge de la gestion des crises cyber (ANSSI en France). EU-CYCLONe est institué afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents de cybersécurité majeurs et des crises, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union.

L'ENISA et des représentants de la Commission européenne, sauf dans le cas d'un incident majeur relevant du champ d'application de la Commission, y assistent en qualité d'observateurs. Les plans nationaux d'intervention en cas d'incident de cybersécurité majeurs et de crise doivent être soumis à EU-CyCLONe et à la Commission dans les trois mois suivant l'incident.
De cette façon, les autorités compétentes des États membres continuent leurs travaux de régulation et d'accompagnement des entités et leur action est renforcée.

Les États membres sont encouragés à effectuer régulièrement des autoévaluations et à présenter et examiner les résultats au sein du Groupe de coopération. En France, l'ANSSI serait l'autorité en charge de ces évaluations. Le Groupe de coopération rédige ensuite les lignes directrices à l'intention des autorités nationales et coordonne leurs actions en matière de gestion de risques cyber.

La directive NIS 2 prévoit la remontée des incidents notifiés aux CSIRTs jusqu'aux instances décisionnelles de l'Union européenne sous la forme de rapports d'incidents et de vulnérabilités. A partir de ces données, l'ENISA élabore une base des données des vulnérabilités qui a pour objectif d'adapter les instructions de gestion des risques pour les groupes de travail européens, qui sont ensuite transposées à l'échelle nationale.

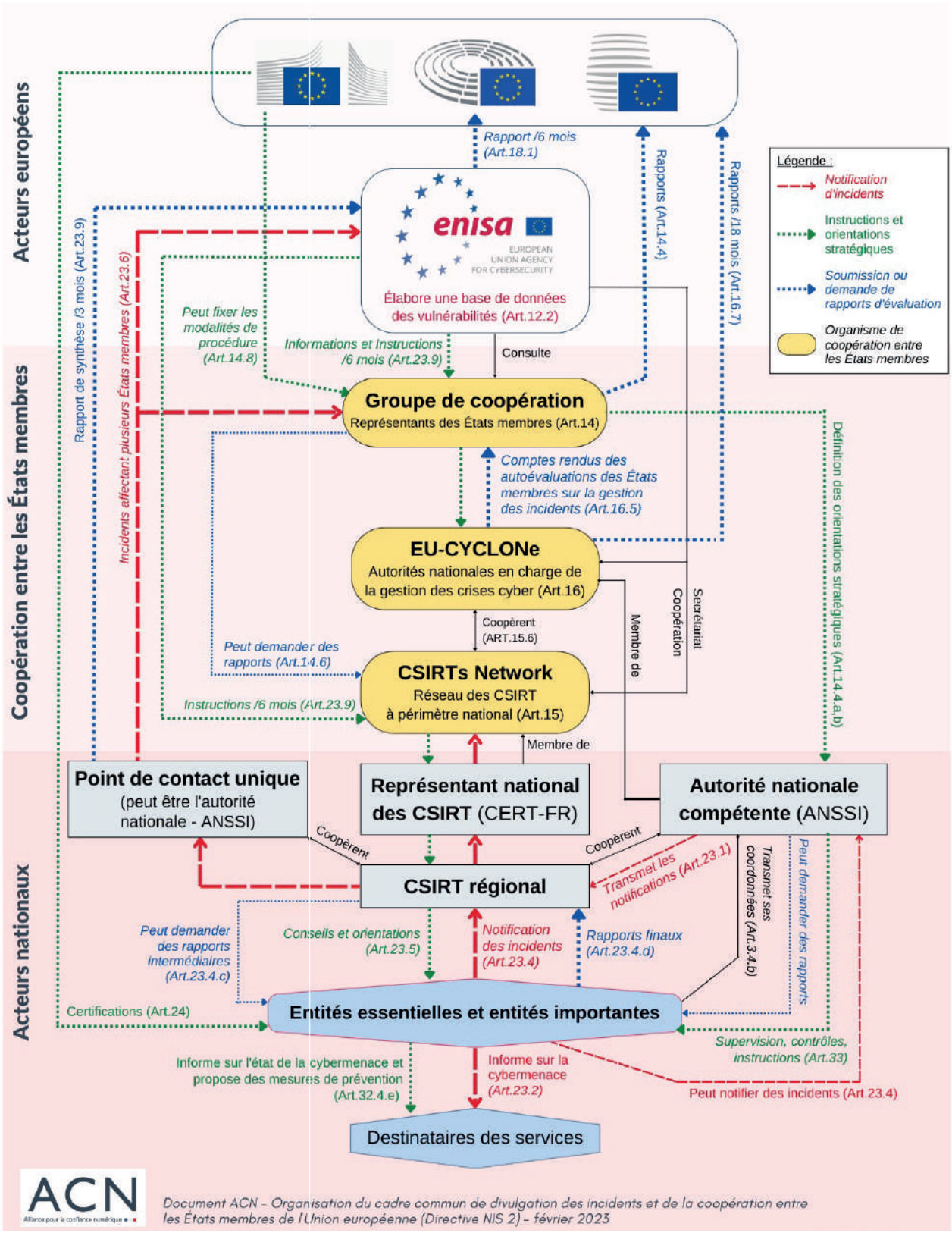
III.B. Recours aux schémas européens de certification obligatoires

Après avoir effectué des consultations et des analyses d'impacts, la Commission européenne est habilitée à préciser les catégories d'entités soumises à des obligations de certification par le biais d'actes délégués. Ces actes délégués sont adoptés lorsque des niveaux insuffisants de cybersécurité ont été constatés et ils prévoient une période de mise en œuvre.

Lorsqu'il n'existe pas de schéma européen de certification approprié, la Commission peut, après consultation du Groupe de coopération et du groupe européen de certification de cybersécurité, demander à l'ENISA de préparer un schéma adéquat.

En outre, afin de démontrer la conformité des exigences en gestion des risques, les États membres peuvent prescrire aux entités d'utiliser des produits TIC, services TIC et processus TIC particuliers, mis au point par l'entité ou acquis auprès de tiers, qui sont certifiés dans le cadre de schémas européens de certification de cybersécurité, telle que la loi sur la cybersécurité de l'UE (Cybersecurity Act (CSA)).

Cadre commun de notification des incidents et coopération entre les États membres de l'UE (Directive NIS 2)



IV- Renforcement des sanctions pénales et pécuniaires

IV.A. Harmonisation et imposition de mesures plus coercitives à l'échelle européenne

Les sanctions mises en place par la directive NIS 2 (Article 31) sont harmonisées au sein de l'Union afin d'assurer à la fois le bon respect des mesures prévues et un niveau d'application plus uniforme entre les Etats membres. Elles sont définies et obligatoires pour toutes les entités entrant dans son champ d'application tandis que NIS 1 déléguait l'imposition de sanctions aux États membres.
À travers NIS 2, les États membres conservent la faculté de fixer leurs propres sanctions, mais ils sont chargés d'appliquer les sanctions définies par la directive en plus des leurs. Ils doivent notamment veiller à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques prises en matière de cybersécurité, supervisent leur mise en œuvre et puissent être tenus responsables en cas de la violation des articles 21 (mesures de gestion des risques) et 23 (obligations d'information) par ces entités.

Les États membres doivent renforcer le contrôle des opérateurs de services essentiels et importants quant aux obligations de gestion des risques cyber et aux efforts que les organisations doivent fournir en sécurité numérique. Les autorités compétentes (l'ANSSI en France) supervisent l'exécution de la directive par les entités.
Leur pouvoir de sanction administrative et leur rôle de régulateur sont renforcés. Elles sont en mesure de soumettre les entités à des inspections, des contrôles, des audits ou encore de demander les informations, les accès et les données nécessaires à l'évaluation des mesures de gestion des risques.

Les exigences sont affermies par rapport à la directive NIS 1. Les entités importantes et les entités essentielles sont soumises aux mêmes sanctions, proportionnées selon la taille de l'entité. Elles doivent prendre les dispositions techniques, opérationnelles et organisationnelles nécessaires pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent et en réduire les conséquences.

IV.B. Nouveauté : engagement de la responsabilité des organes de gestion et des dirigeants

La directive NIS 2 implique la responsabilité des organes de gestion, des décideurs et des cadres supérieurs au sein des entités, en particulier la responsabilité pénale pour les dirigeants qui tentent de dissimuler un problème de sécurité critique.
Les autorités compétentes nationales peuvent engager la responsabilité des gestionnaires dans le cas où une négligence grave est prouvée à la suite d'un incident de sécurité. Lorsque l'infraction concerne un individu d'une entité essentielle, les autorités compétentes ont le droit d'interdire temporairement le responsable d'occuper ses fonctions de direction lorsqu'il s'agit d'une négligence répétée et en cas d'échec de toutes les mesures préventives prévues par la directive. Toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans une entité essentielle peut également être interdit d'exercer ses responsabilités dirigeantes dans le cas où les autorités compétentes estiment qu'il n'a pas mis en place les mesures ordonnées par la directive et n'a pas fait preuve de collaboration pour le faire, excepté dans le cas d'une administration publique.

IV.C. Des amendes proportionnelles et plus dissuasives

Des sanctions financières pour les entités sont prévues, harmonisées et renforcées au sein de chaque État membre en cas de non-respect de la règlementation et de refus de collaborer avec les autorités. La directive de 2016 ne prévoyait pas de sanctions harmonisées au niveau européen. La loi française a fixé des amendes d'un montant maximum de 125 000 € pour les opérateurs de services essentiels et de 100 000 € pour les fournisseurs de services numériques.Désormais, la directive NIS 2 demande aux États membres de renforcer les sanctions pécuniaires des entités en cas de violations de leurs obligations en imposant des amendes administratives.
Le montant maximum ne peut pas être inférieur à un certain seuil fixé en fonction de la taille de l'entité.

Le pourcentage de la somme imposée lors d'une sanction varie selon une échelle calculée à partir de la situation donnée et de l'entité impliquée. Les amendes sont comprises entre 1,4% et 2% du chiffre d'affaires annuel de l'entité, réalisé au niveau national et dans le monde. Dans le cas d'une amende visant une filiale, le pourcentage est calculé sur la base du chiffre d'affaires annuel total du groupe. Pour une violation des articles 21 et 23 de la directive, la somme peut atteindre jusqu'à 10 millions d'euros et 2% du chiffre d'affaires annuel mondial consolidé pour les entités essentielles et jusqu'à 7 millions d'euros ou 1,4% du chiffre annuel mondial pour les entités importantes. Les États membres ont la possibilité d'ajouter leurs propres sanctions pécuniaires nationales aux amendes administratives de l'Union européenne.

Entre
1,4% et 2%
du
Chiffre d'affaires

CONCLUSION

La directive NIS 2 s'inscrit dans le prolongement de NIS 1. L'objectif est d'homogénéiser la protection des systèmes d'information et du quotidien des citoyens de l'Union européenne en mettant les Etats membres au même niveau de sécurité. Elle vise à éliminer les divergences entre les États membres en ce qui concerne la cybersécurité et les obligations de déclaration à l'autorité publique. Les exigences de la directive NIS 1 de 2016 restent en vigueur lors de l'application de NIS 2.
À cette fin, elle fixe des normes minimales, des plans d'orientations stratégiques et elle renforce les mécanismes de coopération en donnant davantage d'importance aux groupes de coopérations des États membres. L'ENISA devient un acteur décisif de la coopération entre les États membres grâce à ses compétences d'harmonisation des mesures et de centralisation des rapports de vulnérabilités.

Le champ d'application de la directive NIS est élargi. Alors qu'il incombait aux États membres de déterminer quelles entités remplissaient les critères pour être qualifiées d'opérateurs de services essentiels, NIS 2 introduit comme règle générale l'identification d'entités essentielles et importantes selon leur taille et leur domaine d'activité.

Par ailleurs, la coordination entre les États membres est renforcée afin d'améliorer la gestion des risques, des menaces et des incidents liés ou non à la cybersécurité.
Enfin, les exigences et la mise en œuvre des mesures de cybersécurité sont harmonisées en fixant les règles d'un cadre réglementaire et en augmentant les sanctions encourues en cas de non-respect de la directive.

Le renforcement de ces mesures attend de tous les États membres qu'ils instituent la cybersécurité de leurs entités afin que les vulnérabilités et les incidents soient traités plus rapidement, en synergies et avec l'aide de l'Union européenne à travers des directives communes.
Les obligations de notifications des incidents sont rationnalisées et de nouvelles mesures de surveillance sont introduites. Les exigences d'exécution deviennent globalement plus strictes.

La directive NIS 2 impose des obligations de renforcement des exigences en matière de cybersécurité. Les entités rentrant dans son champ d'application devront notifier leurs incidents et préparer leurs systèmes d'information au respect des normes exigées de gestion de risques.
Enfin, les certifications européennes sont désormais les seules pouvant attester de la bonne mise en place des mesures de cybersécurité et de gestion des risques au sein de l'Union européenne.
Certaines entités peuvent se voir obligées de certifier leurs solutions. La Commission est également en mesure de préciser les critères et les procédures de notifications des incidents.

La directive NIS 2 fait partie intégrante de la stratégie de sécurité et de cybersécurité de l'Union européenne aux côtés des règlementations actuelles et en cours d'élaboration *(CyberSecurity Act, Cyber Resilience Act, Cybersolidarity Act, Digital Markets Act, Digital Services Act, IA Act, Data Governance Act…).*
L'interdépendance, l'interconnexion et la cohérence des périmètres, des champs d'application et de la mise en œuvre de ces différents textes conditionneront l'effectivité de la protection que l'Union européenne entend apporter dans l'espace numérique.
Il appartient désormais à chaque Etat membre de transposer la directive NIS 2 dans un délai relativement court – avant octobre 2024. Ces transpositions joueront un rôle crucial dans la nécessaire cohérence de l'édifice juridique européen relatif à la cybersécurité. L'enjeu est majeur : afin que ces nouvelles règles puissent produire leurs pleins effets, leur application doit demeurer lisible et compréhensible pour l'ensemble des entités visées.
Cybersécuriser l'espace numérique européen est un défi immense : la directive NIS 2 et sa transposition apportent ainsi une pierre supplémentaire à cet édifice vital pour nos sociétés.

Calendrier d'application de NIS 2

17 janvier 2023 :

la directive NIS 2 entre en application et remplace l'actuelle directive NIS.

17 juillet 2023 :

au plus tard, la Commission fournit les lignes directrices clarifiant l'application des actes juridiques sectoriels de l'Union, notamment en ce qui concerne les entités concernées par la directive mais non couvertes par ces actes juridiques, en tenant compte des observations du groupe de coopération et de l'ENISA.

17 juillet 2024 :

EU-CyCLONe soumet au Parlement européen et au Conseil son premier rapport d'évaluation des travaux.

Octobre 2024 :

les États membres doivent avoir transposé la directive NIS 2 en loi nationale (21 mois après sa sortie sur le journal officiel de l'Union européenne).

17 janvier 2025 :

au plus tard, les entités essentielles et importantes doivent soumettre les informations requises les concernant aux autorités compétentes.

17 janvier 2025 :

au plus tard, les États membres informent la Commission des règles et des mesures de sanctions nationales adoptées.

17 avril 2025 :

au plus tard, les États membres peuvent notifier à la Commission européenne le nom des entités essentielles et importantes.

Détail des entités des secteurs hautement critiques désignés par NIS 2 (Annexe I)

Secteur	Sous - Secteur	Type d'entité
1. Énergie	a) Électricité	Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil qui remplissent la fonction de « fourniture » au sens de l'article 2, point 12), de ladite directive
		Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944

Secteur	Sous - Secteur	Type d'entité
1. Énergie	a) Électricité	Exploitants 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
	b) Réseaux de chaleur et de froid	Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil
	c) Pétrole	Exploitants d'oléoducs
		Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil
	d) Gaz	Entreprises de fourniture au sens de l'article 2, point 8, de la directive 2009/73/CE du Parlement européen et du Conseil
		Gestionnaires de réseau de distribution au sens de l'article 2, point 6, de la directive 2009/73/CE
		Gestionnaires de réseau de transport au sens de l'article 2, point 4, de la directive 2009/73/CE

Secteur	Sous - Secteur	Type d'entité
1. Énergie	d) Gaz	Gestionnaires d'installation de stockage au sens de l'article 2, point 10, de la directive 2009/73/CE
		Gestionnaires d'installation de GNL au sens de l'article 2, point 12, de la directive 2009/73/CE
		Entreprises de gaz naturel au sens de l'article 2, point 1, de la directive 2009/73/CE
		Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) no 300/2008 utilisés à des fins commerciales
		Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil, aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) no 1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports

Secteur	Sous - Secteur	Type d'entité
2. Transports	a) Transports aériens	Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) no 549/2004 du Parlement européen et du Conseil
	b) Transports ferroviaires	Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil
		Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, y compris les exploitants d'installation de service au sens de l'article 3, point 12), de ladite directive
	c) Transports par eau	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) no 725/2004 du Parlement européen et du Conseil, à l'exclusion des navires exploités à titre individuel par ces sociétés
		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) no 725/2004, ainsi que les entités exploitant des infrastructures et des équipements à l'intérieur des ports

Secteur	Sous - Secteur	Type d'entité
2. Transports	c) Transports par eau	Exploitants de services de trafic maritime (STM) au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil
	d) Transports routiers	Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale
3. Secteur bancaire		Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) no 575/2013 du Parlement européen et du Conseil
4. Infrastructures des marchés financiers		Exploitants de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE du Parlement européen et du Conseil
		Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) no 648/2012 du Parlement européen et du Conseil
5. Santé		Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil

Secteur	Sous - Secteur	Type d'entité
5. Santé		Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil
		Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2, section C, division 21 Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil
6. Eau potable		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 du Parlement européen et du Conseil, 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

Secteur	Sous - Secteur	Type d'entité
7. Eaux usées		Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées au sens de l'article 2, points 1), 2) et 3), de la directive 91/271/CEE du Conseil, à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale
8. Infrastructure numérique		Fournisseurs de points d'échange internet
		Fournisseurs de services DNS, à l'exclusion des opérateurs de serveurs racines de noms de domaine
		Registres de noms de domaine de premier niveau
		Fournisseurs de services d'informatique en nuage
		Fournisseurs de services de centres de données
		Fournisseurs de réseaux de diffusion de contenu
		Prestataires de services de confiance
		Fournisseurs de réseaux de communications électroniques publics

Secteur	Sous - Secteur	Type d'entité
8. Infrastructure numérique		Fournisseurs de services de communications électroniques accessibles au public
9. Gestion des services TIC (interentreprises)		Fournisseurs de services gérés Fournisseurs de services de sécurité gérés
10. Administration publique		Entités de l'administration publique des pouvoirs publics centraux définies comme telles par un État membre conformément au droit national Entités de l'administration publique au niveau régional définies comme telles par un État membre conformément au droit national
11. Espace		Entités de l'administration publique au niveau régional définies comme telles par un État membre conformément au droit national

Détails des secteurs critiques définis par NIS 2 (Annexe II)

Secteur	Sous - Secteur	Type d'entité
1. Services postaux et d'expédition		Prestataires de services postaux au sens de l'article 2, point 1 bis), de la directive 97/67/CE, y compris les prestataires de services d'expédition
2. Gestion des déchets		Entreprises 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 (1), à l'exclusion des entreprises pour lesquelles la gestion des déchets n'est pas la principale activité économique
3. Fabrication, production et distribution de produits chimiques		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) no 1907/2006 du Parlement européen et du Conseil (2) 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
4. Production, transformation et distribution des denrées alimentaires		Entreprises du secteur alimentaire au sens de l'article 3, point 2), du règlement (CE) no 178/2002 du Parlement européen et du Conseil (3) qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles

Secteur	Sous - Secteur	Type d'entité
5. Fabrication	a) Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro	Entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1), du règlement (UE) 2017/745 du Parlement européen et du Conseil (4) et entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2), du règlement (UE) 2017/746 du Parlement européen et du Conseil (5), à l'exception des entités fabriquant des dispositifs médicaux mentionnés à l'annexe I, point 5, cinquième tiret, de la présente directive
	b) Fabrication de produits informatiques, électroniques et optiques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 26
	c) Fabrication d'équipements électriques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 27
	d) Fabrication de machines et équipements n.c.a.	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 28
	e) Construction de véhicules automobiles, remorques et semi-remorques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 29
	f) Fabrication d'autres matériels de transport	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 30

Secteur	Sous - Secteur	Type d'entité
6. Fournisseurs numériques		Fournisseurs de places de marché en ligne
		Fournisseurs de moteurs de recherche en ligne
		Fournisseurs de plateformes de services de réseaux sociaux
7. Recherche		Organismes de recherche

Définitions

Entité :
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.

Entité de l'administration publique :
une entité reconnue comme telle dans un État membre conformément au droit national, à l'exclusion de la justice, des parlements et des banques centrales, qui satisfait aux critères suivants :

- elle a été créée pour satisfaire des besoins d'intérêt général et n'a pas de caractère industriel ou commercial,
elle est dotée de la personnalité juridique ou est juridiquement habilitée à agir pour le compte d'une autre entité dotée de la personnalité juridique,

- elle est financée majoritairement par l'État, les autorités régionales ou d'autres organismes de droit public, sa gestion est soumise à un contrôle de la part de ces autorités ou organismes, ou son organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou d'autres organismes de droit public,

- elle a le pouvoir d'adresser à des personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs droits en matière de mouvements transfrontières des personnes, des biens, des services ou des capitaux.

Incident :
Evénement 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.

Incident de cybersécurité majeur :
Incident qui provoque des perturbations dépassant les capacités de réaction du seul État membre concerné ou qui a un impact important sur au moins deux États membres.

Incident important :
Un incident est considéré comme important lorsqu'il cause une perturbation opérationnelle grave ou des pertes financières qui affectent des personnes tierces physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

Définitions

Fournisseur de services DNS :
Entité qui fournit des services de résolution de noms de domaine récursifs accessibles au public et destinés aux utilisateurs finaux de l'internet ou 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.

Stratégie nationale en matière de cybersécurité :
Cadre cohérent d'un État membre fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser dans cet État membre.

Vulnérabilité :
Faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace.

Sources

- Journal Officiel de l'Union européenne, « 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 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE) », Lex Europa, 27 décembre 2022.
  URL:https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC

- Journal officiel de l'Union européenne, « 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 », Lex Europa, 19 juillet 2016.
  URL : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148

- « Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique », Légifrance, 23 mai 2018. URL : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036939971

- « NIS : un dispositif de cybersécurité pour les Opérateurs de services essentiels », ANSSI,
  URL:https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/nis-un-dispositif-de-cybersecurite-pour-les-operateurs-de-service-essentiel/

- Bordone Francesco, Directive (EU) 2022/2555 on measures for High Common Level of Cybersecurity across the Union (NIS2), European Cybersecurity Organisation (ECSO), 27 janvier 2023.
  Bordone Francesco, Overview of the main EU policies on cybersecurity, ECSO, 27 janvier 2023. P.4

- Commission européenne, « Lignes directrices de la Commission relatives à l'application de l'article 3, paragraphe 4, de la directive (UE) 2022/2555 (Directive SRI 2) », 13 septembre 2023.
  URL:https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-34-directive-eu-20222555-nis-2-directive

- Commission européenne, « Lignes directrices de la Commission relatives à l'application de l'article 4, paragraphes 1 et 2, de la directive (UE) 2022/2555 (Directive SRI 2) », 13 septembre 2023
  URL:https://digital-strategy.ec.europa.eu/fr/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive

- Yves VERHOEVEN (Sous-Directeur Stratégie de l'ANSSI), « Directive NIS 2 : ce qui va changer pour les entreprises et l'administration françaises », ANSSI, janvier 2023.
  URL : https://www.ssi.gouv.fr/directive-nis-2-ce-qui-va-changer-pour-les-entreprises-et-ladministration-francaises/

ACN

Alliance pour la confiance numérique

SITE :

https://www.confiance-numerique.fr/

@ACN_SecNum

ACN - Alliance pour la Confiance Numérique