COM(2026) 13 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2025/2026

Reçu à la Présidence de l'Assemblée nationale
le 18 mars 2026

Enregistré à la Présidence du Sénat
le 18 mars 2026

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2022/2555 en ce qui concerne l’introduction de mesures de simplification et l’alignement sur [la proposition de règlement sur la cybersécurité 2]

E 20472

COMMISSION
EUROPÉENNE

Strasbourg, le 20.1.2026
COM(2026) 13 final

2026/0012 (COD)

Proposition de

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2]

{SWD(2026) 11-12} - {SEC(2026) 11}

(Texte présentant de l'intérêt pour l'EEE)

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

La présente proposition fait partie d'un ensemble de mesures visant à aligner le cadre de l'Union en matière de cybersécurité sur les besoins des parties prenantes dans un panorama de cybermenaces toujours plus sophistiquées et une réalité géopolitique complexe. Les entités essentielles et importantes des secteurs critiques sont de plus en plus ciblées par des cyberattaques[1], tandis que les acteurs étatiques de la menace tirent parti des technologies émergentes, telles que l'intelligence artificielle (IA), pour étendre et optimiser davantage leurs attaques. Dans ce contexte, la résilience des infrastructures critiques face aux cybermenaces est reconnue comme un pilier stratégique de nos démocraties et de la sécurité économique de l'UE. Tant la stratégie européenne pour une union de la préparation[2] que la stratégie européenne de sécurité intérieure (ProtectEU)[3] ont placé la cybersécurité au cœur du programme de résilience de l'UE. De même, la communication intitulée «Renforcer la sécurité économique de l'UE»[4] fait de la prévention de l'accès à des informations et données sensibles susceptibles de compromettre la sécurité économique de l'UE et de la prévention et de l'atténuation des perturbations des infrastructures critiques de l'UE affectant l'économie de l'UE des objectifs prioritaires, pour lesquels des mesures de cybersécurité efficaces jouent un rôle crucial. En outre, le rapport Draghi a souligné l'impératif d'accroître la sécurité et de réduire les dépendances comme l'un des principaux domaines d'action nécessaires dans l'Union[5]. Dans sa communication intitulée «Une Europe plus simple et plus rapide»[6], la Commission annonçait son engagement en faveur d'un programme ambitieux visant à favoriser des politiques innovantes et tournées vers l'avenir qui renforcent la compétitivité de l'UE et allègent la charge réglementaire pesant sur les citoyens, les entreprises et les administrations, tout en maintenant les normes les plus élevées en matière de promotion de ses valeurs.

Face à cette situation, la présente proposition de directive modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur la [proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2)] vise à remédier au problème de la complexité et de la diversité des politiques liées à la cybersécurité ayant une incidence sur la posture de cybersécurité de l'UE, notamment en apportant des clarifications et en facilitant la mise en conformité des entités réglementées.

L'objectif de la présente directive devrait être considéré comme faisant partie des objectifs généraux du paquet de révision du règlement sur la cybersécurité, qui comprend la

---

1 ENISA, ENISA Threat Landscape 2025 (rapport 2025 de l'ENISA concernant le panorama des menaces).

2 JOIN/2025/130 final.

3 COM/2025/148 final.

4 JOIN(2025) 977 final.

5 Commission européenne, L'avenir de la compétitivité européenne, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_fr?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

6 COM(2025) 47 final.

proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881. Cette proposition de règlement vise à agir sur: i) le décalage entre le cadre d'action de l'UE en matière de cybersécurité et les besoins des parties prenantes dans un panorama de menaces de plus en plus hostile; ii) le blocage de la mise en œuvre du cadre européen de certification de cybersécurité (ci-après le «CECC»); iii) la complexité et la diversité des politiques liées à la cybersécurité ayant une incidence sur la posture de cybersécurité de l'UE; et iv) l'augmentation des risques pour la sécurité des chaînes d'approvisionnement des TIC. En ce qui concerne la complexité et la diversité des politiques liées à la cybersécurité ayant une incidence sur la posture de cybersécurité de l'UE, le paquet de révision du règlement sur la cybersécurité prévoit, dans le cadre d'une réforme du CECC, de promouvoir la certification en tant qu'outil de mise en conformité pour les entreprises et de permettre l'élaboration d'un système concernant la posture de cybersécurité des entités afin de réduire les coûts de mise en conformité pour les entités soumises à la directive (UE) 2022/2555 (ci-après la «directive SRI 2») et à d'autres dispositions législatives européennes applicables en matière de cybersécurité. Cette approche simplifiera considérablement les obligations réglementaires pour les entités soumises à de multiples exigences de conformité et garantira une utilisation plus efficace des ressources entre les autorités nationales.

L'exposé des motifs de la proposition de règlement sur la cybersécurité 2 présente les principales questions qui sous-tendent la proposition, ainsi que les objectifs spécifiques pour les traiter. La proposition de directive répondra à l'objectif spécifique nº 4 (OS4) de l'analyse d'impact de la révision du règlement sur la cybersécurité, à savoir celui visant à créer des mécanismes et des conditions pour contribuer à faciliter le respect des exigences en matière de cybersécurité et, ainsi, rendre leur application plus cohérente et plus efficace. Les modifications ciblées de la directive SRI 2 visent à simplifier la mise en conformité et à garantir la mise en œuvre rationalisée et cohérente d'aspects spécifiques du cadre de cybersécurité, y compris en ce qui concerne le champ d'application, les définitions, le signalement des attaques par rançongiciel et la supervision des entités fournissant des services transfrontières.

La proposition de directive modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur la [proposition de règlement sur la cybersécurité 2] relève du programme pour une réglementation affûtée et performante (REFIT). Combinée à la révision du règlement sur la cybersécurité, elle contribue fortement à améliorer la clarté, à éliminer les inefficacités et à harmoniser les procédures entre les cadres juridiques. Elle concourt au bon fonctionnement du marché intérieur tout en garantissant la sécurité et l'autonomie stratégique de l'UE.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

L'UE a étendu ses outils juridiques et politiques en adoptant un certain nombre d'instruments juridiques et de mesures politiques: i) la directive SRI 2 sert à renforcer la cybersécurité des infrastructures critiques; ii) les mesures de sécurité physique sont définies dans sa «directive sœur», la directive sur la résilience des entités critiques (CER); iii) le règlement sur la cyberrésilience accroît la cybersécurité des produits; iv) le règlement sur la cybersolidarité met en place des capacités de réaction à l'échelle de l'UE; v) le schéma directeur de l'UE en matière de cybersécurité[7] favorise la coopération dans le domaine de la gestion des crises au

[7] COM/2025/66 final.

niveau européen; vi) la boîte à outils de l'UE pour la cybersécurité de la 5G (boîte à outils de la 5G) soutient la cybersécurité dans les réseaux 5G; vii) le plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé[8] contribue à améliorer la cybersécurité de ces derniers; et viii) l'académie des compétences en matière de cybersécurité[9] répond au défi croissant que constitue la pénurie de talents dans le domaine de la cybersécurité.

Le cadre juridique susmentionné en matière de cybersécurité a été complété par des législations sectorielles, à savoir le règlement sur la résilience opérationnelle numérique du secteur financier (règlement DORA), le code de réseau pour les aspects de la cybersécurité des flux transfrontaliers d'électricité pour le sous-secteur de l'électricité et les règles en matière de sécurité de l'information (partie IS[10]) pour le sous-secteur du transport aérien.

La présente proposition de directive, à l'instar de la proposition de règlement qu'elle accompagne, fait partie d'un ensemble plus large d'initiatives juridiques et stratégiques adoptées par l'Union pour améliorer la résilience des entités face aux menaces pour la sécurité et aux cybermenaces. Elle est axée sur des modifications ciblées de la directive SRI 2 qui visent notamment à clarifier certains aspects concernant le champ d'application, les définitions et les règles de compétence, à réduire la charge liée à la supervision des entités essentielles et importantes, et à faciliter la surveillance des entités transfrontières en renforçant le rôle de l'ENISA dans le soutien à la coopération opérationnelle. En outre, conjointement à la proposition de règlement, la présente proposition permet de créer une forte synergie découlant de la mise au point d'une certification en matière de posture de cybersécurité pour la directive SRI 2 et, potentiellement, pour faciliter le respect d'autres actes juridiques pertinents de l'UE, tels que le règlement général sur la protection des données (RGPD), sans préjudice de leurs exigences spécifiques en matière de certification. Ces mesures de simplification devraient débloquer des ressources pour renforcer la préparation opérationnelle des entités en matière de cybersécurité dans les secteurs critiques de l'UE.

- **Cohérence avec les autres politiques de l'Union**

La présente proposition renforce les exigences de sécurité applicables aux entités fournissant des portefeuilles d'identité numérique pour les entreprises figurant dans la proposition de règlement du Parlement européen et du Conseil relatif à la création de portefeuilles européens d'identité numérique pour les entreprises[11]. Par ailleurs, la Commission veillera à la cohérence avec les initiatives à venir, telles que l'acte législatif sur les réseaux numériques. La présente proposition est alignée sur la proposition de règlement relative à la simplification de la législation numérique (règlement omnibus numérique), qui contient, entre autres, des modifications de la directive SRI 2, ainsi que d'autres actes juridiques de l'UE. Le règlement omnibus numérique prévoit de faciliter le respect des exigences en matière de signalement des incidents de cybersécurité, notamment au titre de la directive SRI 2, en proposant d'effectuer ces signalements par l'intermédiaire d'un guichet unique, qui sera mis au point et maintenu par l'ENISA. De plus, la présente proposition est alignée sur la proposition de règlement du

[8] COM(2025) 10 final.
[9] COM(2023) 207 final.
[10] Règlement d'exécution (UE) 2023/203 de la Commission et règlement délégué (UE) 2022/1645 de la Commission.
[11] COM/2025/838 final.

Parlement européen et du Conseil relatif à la sécurité, à la résilience et à la durabilité des activités spatiales dans l'Union[12].

En outre, la proposition est conforme au rapport sur l'avenir de la compétitivité européenne de Mario Draghi, comme souligné ci-dessus.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La base juridique de la présente directive est l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), dont l'objectif est l'établissement et le fonctionnement du marché intérieur par l'amélioration des mesures relatives au rapprochement des règles nationales. La présente proposition modifie la directive (UE) 2022/2555, qui a été adoptée en vertu de l'article 114 du TFUE.

• Subsidiarité (en cas de compétence non exclusive)

Le principe de subsidiarité suppose d'évaluer la nécessité et la valeur ajoutée de l'action de l'Union. Le respect du principe de subsidiarité dans ce domaine a déjà été reconnu lors de l'adoption de la directive (UE) 2022/2555, qui est modifiée par la présente proposition.

La présente proposition facilite le respect de la législation de l'UE relative à la cybersécurité, en réduisant les coûts de mise en conformité et l'insécurité juridique pour les entités concernées, ainsi qu'en facilitant et en améliorant le taux de conformité avec les exigences en matière de cybersécurité. Elle contribue également à garantir des conditions égales pour tous les États membres en ce qui concerne les approches en matière de supervision et de contrôles de conformité.

• Proportionnalité

Les règles proposées dans la présente directive ne vont pas au-delà de ce qui est nécessaire pour réaliser les objectifs spécifiques de manière satisfaisante. L'alignement et la rationalisation envisagés du champ d'application, des mesures de sécurité et des obligations de signalement sont liés aux demandes d'amélioration du cadre actuel formulées par les États membres et les entreprises.

• Choix de l'instrument

La proposition modifiera la directive SRI 2 existante et rationalisera davantage les obligations imposées aux entreprises, garantissant ainsi un niveau plus élevé d'harmonisation dans l'ensemble de l'Union. Le choix de l'instrument juridique pour la présente proposition est cohérent avec celui du texte juridique qu'elle modifie, à savoir la directive SRI 2. La présente proposition s'appuie sur l'objectif de la directive SRI 2 consistant à offrir aux États membres la flexibilité nécessaire pour tenir compte des spécificités nationales.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

• Évaluations ex post/bilans de qualité de la législation existante

Voir l'exposé des motifs de la [proposition de règlement sur la cybersécurité 2].

[12] COM/2025/335 final.

- **Consultation des parties intéressées**

Voir l'exposé des motifs de la [proposition de règlement sur la cybersécurité 2].

- **Obtention et utilisation d'expertise**

Voir l'exposé des motifs de la [proposition de règlement sur la cybersécurité 2].

- **Analyse d'impact**

Voir l'exposé des motifs ainsi que le rapport d'analyse d'impact accompagnant la [proposition de règlement sur la cybersécurité 2].

- **Réglementation affûtée et simplification**

Voir l'exposé des motifs de la [proposition de règlement sur la cybersécurité 2].

- **Droits fondamentaux**

Voir l'exposé des motifs de la [proposition de règlement sur la cybersécurité 2].

4. INCIDENCE BUDGÉTAIRE

Veuillez vous référer à la fiche législative et financière figurant dans [la proposition de règlement sur la cybersécurité 2].

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

Conformément à l'article 40 de la directive SRI 2, la Commission réexaminera le fonctionnement de la directive et en fera rapport au Parlement européen et au Conseil tous les 36 mois.

- **Explication détaillée de certaines dispositions de la proposition**

La proposition vise à faciliter le respect des obligations en matière de cybersécurité et à débloquer des ressources pour renforcer la préparation opérationnelle des entités en matière de cybersécurité dans les secteurs critiques de l'Union.

Elle apporte des modifications ciblées à la directive SRI 2 afin de simplifier des aspects spécifiques du cadre de cybersécurité, d'accroître la sécurité juridique et d'harmoniser la mise en œuvre.

Afin de permettre aux entités et aux fournisseurs de démontrer plus facilement la conformité avec la directive SRI 2, conformément à la proposition de règlement que la présente proposition accompagne, les entités régies par la directive SRI 2 pourront obtenir des certificats dans le cadre de schémas organisationnels de certification de cybersécurité élaborés au sein du CECC.

Pour faciliter davantage le respect des mesures de gestion des risques en matière de cybersécurité pour les entités multinationales soumises à la supervision des autorités compétentes de plusieurs États membres, l'ENISA se voit confier un nouveau rôle consistant à aider les États membres à superviser ces entités, à faciliter l'assistance mutuelle et à créer une meilleure vue d'ensemble des entités relevant du champ d'application de la directive SRI 2.

En outre, la proposition prévoit que la Commission adopte des lignes directrices portant sur l'application des exigences en matière de sécurité de la chaîne d'approvisionnement que les entités relevant du champ d'application de la directive SRI 2 transmettent à leurs fournisseurs, afin de garantir la sécurité juridique et d'éviter la répercussion injustifiée d'obligations sur les entités ne relevant pas du champ d'application de ladite directive.

Parmi les autres modifications ciblées de la directive SRI 2 figurent:

- des précisions dans le champ d'application et les définitions;
- le retrait des micro- et petits fournisseurs de services DNS du champ d'application;
- l'introduction d'une harmonisation maximale des actes d'exécution au titre de l'article 21, paragraphe 5 (précisant les mesures de gestion des risques en matière de cybersécurité) afin de faciliter la mise en conformité des entités et la supervision des autorités;
- l'ajout d'une nouvelle catégorie de petites entreprises à moyenne capitalisation, conformément à la recommandation de la Commission de 2025 concernant la définition des petites entreprises à moyenne capitalisation[18]; les entités qualifiées de petites entreprises à moyenne capitalisation doivent être désignées comme des entités importantes, ce qui réduira leur charge réglementaire et la charge de supervision pesant sur les autorités compétentes;
- l'obligation pour les États membres d'adopter des politiques de migration vers la cryptographie post-quantique (CPQ) dans le cadre de leur stratégie nationale en matière de cybersécurité; et
- l'introduction d'une collecte harmonisée de données sur les attaques par rançongiciel.

2026/0012 (COD)

Proposition de

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2]

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[1],

vu l'avis du Comité des régions[2],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) La directive (UE) 2022/2555 du Parlement européen et du Conseil[3] établit des mesures qui ont pour but d'obtenir un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, afin d'améliorer le fonctionnement du marché intérieur. Depuis l'entrée en vigueur de la directive (UE) 2022/2555, des progrès ont été réalisés dans l'amélioration du niveau de cyberrésilience de l'Union. Dans le même temps, certaines difficultés sont apparues au cours de son application par les États membres, notamment en ce qui concerne son champ d'application, la mise en œuvre des obligations en matière de gestion des risques de cybersécurité et de signalement des incidents de cybersécurité et la supervision des entités transfrontières. Sur la base de [la proposition de règlement sur la cybersécurité 2], il convient d'apporter des modifications ciblées à la directive (UE) 2022/2555 afin de relever ces défis, en simplifiant des aspects spécifiques afin d'accroître la sécurité juridique et de garantir une mise en œuvre uniforme de la directive (UE) 2022/2555.

(2) Afin de réduire la charge de la mise en conformité pour les entités et celle de la supervision pour les autorités compétentes, il convient d'ajouter une nouvelle catégorie de petites entreprises à moyenne capitalisation dans la directive (UE)

---

1 JO C [...], [...], p. [...].

2 JO C [...], [...], p. [...].

3 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) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

2022/2555, conformément à la recommandation (UE) 2025/1099 de la Commission[4]. Les entités d'un type visé à l'annexe I de la directive (UE) 2022/2555, qui sont considérées comme de petites entreprises à moyenne capitalisation aux termes de ladite recommandation, devraient, en règle générale, être désignées comme des entités importantes. En outre, afin de soutenir l'objectif de la Commission consistant à réduire les coûts administratifs de 25 % au total et de 35 % pour les petites et moyennes entreprises, il convient d'appliquer aux fournisseurs de services de système de noms de domaines la règle générale du plafond fixé dans la directive (UE) 2022/2555, selon laquelle toutes les entités qui constituent des entreprises moyennes en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission[5], ou qui dépassent les plafonds prévus au paragraphe 1 dudit article, relèvent du champ d'application de la directive (UE) 2022/2555.

(3) Au cours de la mise en œuvre de la directive (UE) 2022/2555, des difficultés ont surgi dans l'interprétation des dispositions relatives à son champ d'application. Par conséquent, il est nécessaire d'apporter des précisions sur certaines dispositions relatives au champ d'application concernant les prestataires de soins de santé, les producteurs d'électricité, les entreprises d'hydrogène et les entités du secteur chimique afin de garantir la sécurité juridique et de réduire la charge de mise en conformité tant pour les entités que pour les autorités nationales.

(4) Afin de garantir la proportionnalité en ce qui concerne les producteurs d'électricité au sens de l'article 2, point 38), de la directive (UE) 2019/944[6] du Parlement européen et du Conseil, seuls les producteurs d'électricité dont la capacité totale de production est supérieure à 1 MW devraient être considérés comme des entités essentielles ou importantes au titre de la directive (UE) 2022/2555, pour autant que ladite directive s'applique à eux en vertu de la règle relative au plafond. Cela devrait englober les producteurs d'électricité dont une seule installation de production d'électricité dépasse 1 MW, ainsi que ceux qui exploitent plusieurs installations de production dont la capacité de production cumulée est supérieure à 1 MW. Une telle approche permet de trouver un équilibre entre la nécessité d'inclure les entités pour lesquelles une interférence avec leur réseau et leur système d'information pourrait signifier une perte, une impossibilité d'exercer le contrôle ou une prise de contrôle externe de la capacité de production qui est, à elle seule, importante pour la sécurité et la stabilité du réseau électrique, et la nécessité de ne pas imposer de charge administrative disproportionnée aux entreprises au titre de la directive (UE) 2022/2555.

(5) Les portefeuilles européens d'identité numérique prévus par le règlement (UE) nº 910/2014[7] du Parlement européen et du Conseil sont une composante essentielle de

---

4 Recommandation (UE) 2025/1099 de la Commission du 21 mai 2025 concernant la définition des petites entreprises à moyenne capitalisation (JO L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

5 Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

6 Directive (UE) 2019/944 du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE (JO L 158 du 14.6.2019, p. 125), ELI: http://data.europa.eu/eli/dir/2019/944/oj).

7 Règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

l'infrastructure numérique de l'UE, permettant l'identification et l'authentification sécurisées ainsi que l'échange de documents électroniques, y compris les attestations électroniques d'attributs. Compte tenu du rôle indispensable de ces portefeuilles pour le public et pour la fourniture de services publics et privés, tout incident de cybersécurité les compromettant pourrait avoir d'importantes répercussions. Afin d'assurer la prestation de leurs services, les fournisseurs de portefeuilles européens d'identité numérique devraient être tenus de mettre en place des mesures techniques, opérationnelles et organisationnelles appropriées pour gérer les risques de cybersécurité, prévenir les incidents et y répondre, et coopérer avec les autorités compétentes conformément à la directive (UE) 2022/2555. Ils devraient donc figurer parmi les entités relevant de ladite directive, quelle que soit leur taille, et être classés en tant qu'entités essentielles. Les portefeuilles européens d'identité numérique pour les entreprises offrent des fonctionnalités et des services similaires adaptés aux besoins des opérateurs économiques et des organismes du secteur public, en s'appuyant sur le cadre européen relatif à une identité numérique, et sont tout aussi critiques pour la sécurité et l'intégrité de l'économie numérique. En conséquence, les fournisseurs de portefeuilles européens d'identité numérique pour les entreprises établis conformément à la [proposition de règlement relatif à la création de portefeuilles européens d'identité numérique pour les entreprises][8] devraient être soumis aux mêmes exigences et obligations en matière de cybersécurité que les fournisseurs de portefeuilles européens d'identité numérique, afin de garantir un niveau de sécurité identique et élevé dans l'ensemble de l'écosystème d'identité numérique.

(6) Les infrastructures de transmission de données sous-marines comprennent non seulement des câbles, mais aussi toute infrastructure liée à leur exploitation. Ces infrastructures incluent des stations d'atterrissement et les parties terrestres du câble sous-marin qui leur est relié, telles que les itinéraires terrestres entre la chambre-plage et la station d'atterrissement, le centre de données ou le point de présence. Les infrastructures de transmission de données sous-marines sont généralement exploitées par des entités auxquelles s'applique déjà la directive (UE) 2022/2555, notamment des fournisseurs de réseaux et de services de communications électroniques publics ou des fournisseurs de services d'informatique en nuage. Toutefois, les infrastructures de transmission de données sous-marines peuvent également être exploitées par d'autres types d'entités qui ne relèvent actuellement pas du champ d'application de la directive (UE) 2022/2555, telles que les infrastructures de transmission de données sous-marines exploitées par des fournisseurs de réseaux de communications électroniques qui ne sont pas publics, ou par des entités qui donnent en location l'exploitation d'infrastructures de transmission de données sous-marines, en tout ou en partie, à des fournisseurs de réseaux de communications électroniques publics. Compte tenu des risques croissants pesant sur les infrastructures de transmission de données sous-marines et de la grande criticité qui en résulte, il est nécessaire de veiller à ce que la directive (UE) 2022/2555 s'applique à tous les types d'exploitants d'infrastructures de transmission de données sous-marines. D'autres infrastructures maritimes critiques, telles que les câbles électriques sous-marins ainsi que les gazoducs, les conduites d'hydrogène et les oléoducs, entrent généralement déjà dans le champ d'application de la directive (UE) 2022/2555, étant donné qu'elles sont exploitées par des gestionnaires de réseau de transport dans les sous-secteurs de l'électricité, du gaz, de l'hydrogène et du pétrole.

[8] COM(2025) 838 final.

(7) Afin de permettre aux entités fournissant des services dans plusieurs États membres de bénéficier d'approches de supervision plus cohérentes et moins contraignantes dans l'ensemble du marché intérieur, il convient de les mettre en mesure de démontrer qu'elles respectent certaines ou toutes les obligations en matière de gestion des risques de cybersécurité énoncées dans la directive (UE) 2022/2555 en obtenant un certificat relatif à la posture de cybersécurité dans le cadre d'un schéma européen de certification de cybersécurité. L'élaboration d'un tel schéma sera favorisée par l'adoption d'actes d'exécution relatifs aux exigences techniques et méthodologiques ainsi qu'aux exigences sectorielles concernant les mesures de gestion des risques en matière de cybersécurité au titre de la directive (UE) 2022/2555, qui sont fondées sur une harmonisation maximale.

(8) Compte tenu de la dépendance croissante de notre société et de notre économie à l'égard des technologies numériques, il est nécessaire de prendre des mesures d'atténuation contre la menace quantique. L'éventualité d'attaques visant à «récolter maintenant, déchiffrer plus tard», qui se produisent probablement dès à présent, et les futurs risques engendrés par les attaques quantiques consistant à falsifier des signatures, ainsi que le projet de rendre obsolètes certaines utilisations d'algorithmes et d'abandonner totalement les algorithmes cryptographiques à clé publique actuels, accentuent l'urgence d'engager des actions en faveur de la migration vers la cryptographie post-quantique (CPQ). Par conséquent, il convient d'imposer aux États membres l'adoption de politiques de migration vers la CPQ dans le cadre de leur stratégie nationale en matière de cybersécurité. Ces politiques devraient faciliter l'accélération de la planification stratégique et la création de mesures et d'outils de soutien pour évaluer l'exposition des actifs cryptographiques aux risques posés par les ordinateurs quantiques. En outre, elles devraient contribuer à l'élaboration d'un plan de migration et à la mise à l'essai du déploiement de la CPQ dans les applications et réseaux numériques, tout en favorisant l'émergence et l'adoption de solutions de CPQ européennes officiellement vérifiées et évaluées respectant les cadres de conformité des produits et services. Ces politiques devraient s'aligner sur les étapes décrites dans les actes juridiques et les politiques de l'UE ainsi que dans les documents adoptés par le groupe de coopération SRI, en particulier la feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique, qu'il a adoptée en juin 2025, de manière à réaliser la migration vers la CPQ d'ici à 2030 pour les cas d'utilisation critique et d'ici à 2035 pour les cas d'utilisation de niveau moyen et faible.

(9) Conformément à l'article 21, paragraphe 2, point d), de la directive (UE) 2022/2555, les entités essentielles et importantes doivent assurer un niveau de sécurité approprié dans leur chaîne d'approvisionnement. Dans la pratique, cette obligation a conduit de nombreuses entités à demander des informations détaillées à leurs fournisseurs au moyen de questionnaires, de formats et de processus hétérogènes. Si ces demandes visent à soutenir le devoir de vigilance et la gestion des risques, elles peuvent également créer une charge administrative considérable pour les fournisseurs d'entités essentielles et importantes, en particulier lorsque des informations similaires doivent être fournies à plusieurs reprises sous des formes divergentes. Afin d'alléger cette charge et de promouvoir une approche cohérente, proportionnée et efficace des évaluations de la sécurité de la chaîne d'approvisionnement, la Commission devrait élaborer des lignes directrices pour recommander un niveau approprié de détail, de structure et de format pour ces demandes d'informations. Ces lignes directrices devraient faciliter l'harmonisation, réduire les redondances inutiles et aider tant les

entités que leurs fournisseurs à respecter efficacement les obligations qui leur incombent au titre de la directive (UE) 2022/2555.

(10) Les attaques par rançongiciel dans lesquelles des logiciels malveillants chiffrent les données et les systèmes et exigent un paiement de rançon pour les débloquer restent l'une des principales menaces pour les entités essentielles et importantes. L'harmonisation et l'amélioration de la collecte de données sur les attaques par rançongiciel effectuée par les entités essentielles et importantes touchées fourniraient aux centres de réponse aux incidents de sécurité informatique (CSIRT) et aux autorités nationales des informations leur permettant de veiller à ce que les futures interventions en cas d'attaque par rançongiciel soient appropriées et efficaces, d'aider les entités à accroître leur résilience et à prévenir de futures attaques, ainsi que de compiler les renseignements et les preuves dont les services répressifs ont besoin pour déstabiliser et démanteler les gangs de rançongiciel et sanctionner leurs agents. Compte tenu du caractère potentiellement sensible des informations à partager concernant les attaques par rançongiciel, en particulier celles se rapportant au paiement effectif d'une rançon et, le cas échéant, à son montant et à son destinataire, ces informations devraient être communiquées aux CSIRT ou, s'il y a lieu, aux autorités compétentes uniquement à leur demande. Aux fins de cet échange d'informations, les entités essentielles et importantes sont encouragées à désigner une personne qui sert de point de contact et assure la confidentialité et la fiabilité de l'échange d'informations. Dans le cadre de l'initiative internationale de lutte contre les rançongiciels, l'UE a approuvé une déclaration de politique générale internationale non contraignante selon laquelle les institutions compétentes placées sous l'autorité des gouvernements nationaux participants devraient s'opposer au paiement des rançons en cas de tentative d'extorsion par rançongiciel.

(11) Le respect des obligations de communication des informations pertinentes concernant les incidents liés à des rançongiciels ne devrait pas entraîner l'imposition d'obligations supplémentaires au titre de la directive (UE) 2022/2555 auxquelles l'entité n'aurait pas été soumise si elle n'avait pas communiqué ces informations. À cet effet, dans les limites de leur ordre juridique national, les États membres devraient traiter les risques éventuels découlant d'une responsabilité accrue liée à la communication d'informations pertinentes sur les incidents liés aux rançongiciels.

(12) Compte tenu de la dimension transfrontière de nombreuses entités essentielles et importantes dans l'ensemble du marché intérieur et de la nécessité d'assurer la cohérence et de promouvoir la convergence et l'efficacité en ce qui concerne les approches en matière de supervision, l'ENISA devrait aider les États membres à fournir une assistance mutuelle aux entités essentielles et importantes qui fournissent des services dans plusieurs États membres ou qui fournissent des services dans un ou plusieurs États membres et dont les réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres. Dans cette optique, les États membres devraient communiquer des informations supplémentaires au registre des entités tenu par l'ENISA. Sur la base des informations contenues dans le registre des entités essentielles et importantes, l'ENISA devrait procéder à une analyse complète des risques transfrontières en matière de cybersécurité liés à ces entités. Il convient de fonder cette analyse sur une méthode élaborée en collaboration avec la Commission et le groupe de coopération SRI. Cette méthode pourrait tenir compte de la mesure dans laquelle les entités essentielles et importantes déploient leurs services sur une large base transfrontière, dépendent de services transfrontières, sont exposées à un risque de concentration de la chaîne d'approvisionnement, peuvent être définies comme une

source de risque de concentration de la chaîne d'approvisionnement, sont exposées au risque de subir des incidents susceptibles d'avoir des effets perturbateurs importants sur les services transfrontières, ou sont tributaires de réseaux et de systèmes d'information pour la fourniture de leurs services qui sont situés dans différents États membres et en dehors de l'UE. Sur la base du rapport d'analyse des risques, l'ENISA devrait recommander aux autorités compétentes concernées de constituer des équipes d'examen conjointes afin de soutenir la supervision des entités présentant un degré de risque plus élevé pour le bon fonctionnement du marché intérieur en cas d'incident et d'assister les autorités compétentes dans l'exécution d'actions communes de supervision à leur demande.

(13) Étant donné que l'objectif de la présente directive, qui vise à simplifier la mise en œuvre des mesures visant à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(14) Le Contrôleur européen de la protection des données et le comité européen de la protection des données ont été consultés conformément à l'article 42, paragraphe 2, du règlement (UE) 2018/1725 du Parlement européen et du Conseil[9] et ont rendu un avis conjoint le [date],

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Modifications de la directive (UE) 2022/2555

La directive (EU) 2022/2555 est modifiée comme suit:

(1) l'article 2 est modifié comme suit:

(a) au paragraphe 2, le point a) est modifié comme suit:

i) le point iii) est remplacé par le texte suivant:

«iii) des registres des noms de domaine de premier niveau;»;

ii) les points iv) et v) suivants sont ajoutés:

«iv) des fournisseurs de portefeuilles européens d'identité numérique tels que prévus dans le règlement (UE) nº 910/2014;

v) des fournisseurs de portefeuilles européens d'identité numérique pour les entreprises établis conformément au règlement (UE) [...] *.

_____

[9] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE (JO L 295 du 21.11.2018, p. 39), ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

* Règlement (UE) [...] [proposition de règlement relatif à la création de portefeuilles européens d'identité numérique pour les entreprises].»;

(b) le paragraphe 3 *bis* suivant est inséré:

«3 *bis.* La présente directive s'applique aux entités, quelle que soit leur taille, recensées en tant que propriétaires, gestionnaires et exploitants d'infrastructures stratégiques à double usage au titre du règlement (UE) [...] **.

_____

** «Règlement (UE) [...] [Proposition de règlement du Parlement européen et du Conseil établissant un cadre de mesures visant à faciliter le transport d'équipements, de biens et de personnel militaires dans l'ensemble de l'Union.]»;

(2) l'article 3 est modifié comme suit:

(a) le paragraphe 1 est modifié comme suit:

i) les points a) et b) sont remplacés par le texte suivant:

«a) les entités d'un type visé à l'annexe I qui dépassent les plafonds fixés pour les petites entreprises à moyenne capitalisation;

b) les prestataires de services de confiance qualifiés, les fournisseurs de portefeuilles européens d'identité numérique, les fournisseurs de portefeuilles européens d'identité numérique pour les entreprises et les registres de noms de domaine de premier niveau, quelle que soit leur taille;»;

ii) le point h) suivant est ajouté:

«h) les entités recensées en tant que propriétaires, gestionnaires et exploitants d'infrastructures stratégiques à double usage au titre du règlement (UE) [...] [Proposition de règlement du Parlement européen et du Conseil établissant un cadre de mesures visant à faciliter le transport d'équipements, de biens et de personnel militaires dans l'ensemble de l'Union.]»;

(b) au paragraphe 4, le premier alinéa est remplacé par le texte suivant:

«Aux fins de l'établissement de la liste prévue au paragraphe 3, les États membres exigent des entités visées audit paragraphe qu'elles communiquent aux autorités compétentes au moins les informations suivantes:

a) le nom de l'entité;

b) les secteur, sous-secteur et type d'entité concernés mentionnés à l'annexe I ou II, le cas échéant;

c) l'adresse de l'entité ou, le cas échéant, celle de l'établissement principal de l'entité et de ses autres établissements légaux dans l'Union ou, si elle n'est pas établie dans l'Union, de son représentant désigné conformément à l'article 26, paragraphe 3;

d) les coordonnées actualisées, comprenant les adresses de courrier électronique, les numéros de téléphone, l'identifiant unique et les adresses numériques du portefeuille européen d'identité numérique pour les entreprises

de l'entité, le cas échéant, et du représentant désigné de l'entité en application de l'article 26, paragraphe 3, le cas échéant;

e) les États membres dans lesquels l'entité fournit des services;

f) les plages d'IP de l'entité.»;

(3) l'article 5 est remplacé par le texte suivant:

«*Article 5*

Harmonisation minimale

Sans préjudice de l'article 21, paragraphe 5, cinquième alinéa, la présente directive ne fait pas obstacle à l'adoption ou au maintien par les États membres de dispositions assurant un niveau plus élevé de cybersécurité, à condition que ces dispositions soient compatibles avec les obligations des États membres prévues par le droit de l'Union.»;

(4) à l'article 6,

les points 42) et 43) suivants sont ajoutés:

«42) "petite entreprise à moyenne capitalisation", une petite entreprise à moyenne capitalisation telle que définie à l'annexe de la recommandation (UE) 2025/1099 de la Commission***;

(43) "infrastructure sous-marine de transmission de données": les câbles sous-marins servant à transmettre des données, l'infrastructure connexe et d'autres installations ou éléments associés à la transmission de données.

_____

*** Recommandation (UE) 2025/1099 de la Commission du 21 mai 2025 concernant la définition des petites entreprises à moyenne capitalisation (JO L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).»;

(5) à l'article 7, paragraphe 2, le point k) suivant est ajouté:

«k) la transition vers la cryptographie post-quantique, en tenant compte des calendriers pour la transition et des exigences pertinentes énoncés dans les actes juridiques et les politiques applicables de l'Union.»;

(6) à l'article 15, paragraphe 2, la première phrase est remplacée par le texte suivant:

«Le réseau des CSIRT est composé de représentants des CSIRT désignés ou mis en place en application de l'article 10, de l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union (CERT-UE) et de l'ENISA.»;

(7) l'article 21, paragraphe 5, est modifié comme suit:

(a) le second alinéa est remplacé par le texte suivant:

«La Commission peut adopter des actes d'exécution établissant les exigences techniques et méthodologiques ainsi que les exigences sectorielles, si nécessaire, liées aux mesures prévues au paragraphe 2 concernant les entités essentielles et importantes autres que celles visées au premier alinéa du présent paragraphe. La Commission évalue régulièrement si des actes d'exécution mentionnés au présent alinéa doivent être adoptés pour des secteurs ou des types d'entités spécifiques afin d'améliorer le fonctionnement du marché

intérieur. Lorsqu'elle prépare ces évaluations, la Commission se concentre en particulier sur la nature transfrontière des secteurs ou des types d'entités et engage un processus de consultation ouvert, transparent et inclusif avec les parties prenantes concernées et les États membres.»;

(b) le cinquième alinéa suivant est ajouté:

«Lorsque la Commission adopte des actes d'exécution mentionnés aux premier et deuxième alinéas du présent paragraphe, les États membres n'imposent aucune exigence technique, méthodologique ou sectorielle supplémentaire liée aux mesures visées à l'article 21, paragraphe 2, de la directive (UE) 2022/2555 aux entités relevant du champ d'application desdits actes d'exécution.»;

(8) à l'article 23, les paragraphes 12 et 13 suivants sont ajoutés:

«12. Lorsqu'elle adopte un acte d'exécution en vertu du paragraphe 11, premier alinéa, la Commission inclut des exigences imposant que les informations suivantes concernant les attaques par rançongiciel soient notifiées en application du paragraphe 1:

(a) si l'entité a détecté une attaque par rançongiciel;

(b) le vecteur utilisé pour l'attaque par rançongiciel;

(c) si des mesures d'atténuation ont été mises en œuvre.

13. Les États membres veillent à ce qu'en cas d'incident important causé par une attaque par rançongiciel, les entités concernées fassent savoir, à la demande du CSIRT ou, le cas échéant, de l'autorité compétente par l'intermédiaire d'un canal de communication fourni par le CSIRT ou, le cas échéant, par l'autorité compétente:

(a) si l'entité a reçu une demande de rançon et, le cas échéant, de qui;

(b) si une rançon a été versée et, dans l'affirmative, quels en sont le montant, le moyen de paiement et le destinataire ou le récepteur, y compris le crypto-actif et le prestataire de services sur crypto-actifs, le cas échéant.»;

(9) à l'article 24, les paragraphes 4, 5 et 6 suivants sont ajoutés:

«4. Afin de démontrer la conformité avec l'article 21, les États membres peuvent exiger des entités essentielles et importantes qu'elles obtiennent un certificat de posture de cybersécurité dans le cadre d'un schéma européen de certification de cybersécurité adopté en application de l'article 75 du règlement (UE) XXX/XXX****[proposition CSA2].

5. Lorsque la posture de cybersécurité d'une entité essentielle ou importante est certifiée dans le cadre d'un schéma européen de certification de cybersécurité adopté en application de l'article 74 du règlement (UE) XXX/XXX**** [proposition CSA2] et que le certificat démontre la conformité avec les exigences énoncées dans un acte d'exécution adopté en application de l'article 21, paragraphe 5, de la présente directive ou énoncées dans la législation nationale transposant l'article 21, paragraphes 1 et 2 de la présente directive, les autorités compétentes ne soumettent pas l'entité à des mesures supplémentaires au titre de l'article 32, paragraphe 2, point b), ou de l'article 33, paragraphe 2, point b), selon le cas, en ce qui concerne les exigences couvertes par le certificat.

6. Une certification au titre du paragraphe 4 est sans effet sur la responsabilité de l'entité essentielle ou importante de se conformer à la présente directive.

_____

**** Règlement (UE) XXX/XXX [proposition CSA2]»;

(10) l'article 26 est modifié comme suit:

(a) au paragraphe 1, le point d) suivant est ajouté:

«d) les transporteurs aériens qui sont considérés comme relevant de la compétence de l'État membre dont l'autorité compétente pour l'octroi des licences a accordé la licence d'exploitation à l'entité en vertu du règlement (CE) n° 1008/2008 du Parlement européen et du Conseil***** ou qui, lorsque la licence d'exploitation ou l'équivalent n'a pas été délivré conformément audit règlement, sont considérés comme relevant de la juridiction de l'État membre dans lequel ils ont leur établissement principal dans l'Union en vertu du paragraphe 2.

_____

***** Règlement (CE) nº 1008/2008 du Parlement européen et du Conseil du 24 septembre 2008 établissant des règles communes pour l'exploitation de services aériens dans la Communauté (Refonte) (JO L 293 du 31.10.2008, p. 3, ELI: http://data.europa.eu/eli/reg/2008/1008/oj)»;

(b) le paragraphe 3 est remplacé par le texte suivant:

«3. Si une entité essentielle ou importante n'est pas établie dans l'Union mais offre des services dans l'Union, elle désigne un représentant dans l'Union. Celui-ci est établi dans l'un des États membres dans lesquels les services sont fournis. Une telle entité est considérée comme relevant de la compétence de l'État membre dans lequel le représentant est établi. Lorsqu'une telle entité est une entité visée au paragraphe 1, point a), elle est considérée comme relevant de la compétence de l'État membre dans lequel elle fournit ses services. En l'absence d'un représentant dans l'Union désigné en vertu du présent paragraphe, tout État membre dans lequel l'entité fournit des services peut intenter une action en justice contre l'entité pour violation de la présente directive.»;

(11) l'article 27 est modifié comme suit:

(a) le paragraphe 1 est remplacé par le texte suivant:

«1. L'ENISA crée et tient, sur la base des informations reçues des points de contact uniques conformément au paragraphe 4, un registre des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Sur demande, l'ENISA autorise les autorités compétentes à accéder aux informations concernant les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités qui fournissent des services d'enregistrement de noms de domaine, 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

transporteurs aériens enregistrés dans ledit registre, tout en veillant à la protection de la confidentialité des informations le cas échéant.»;

(b) le paragraphe 2 est supprimé;

(c) les paragraphes 3, 4 et 5 sont remplacés par le texte suivant:

«3. Les États membres veillent à ce que les entités essentielles et importantes notifient à l'autorité compétente toute modification des informations qu'elles ont communiquées au titre de l'article 3, paragraphe 4, sans tarder et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification.

4. À la réception des informations mentionnées à l'article 3, paragraphe 4, le point de contact unique de l'État membre concerné les transmet sans retard injustifié à l'ENISA.

5. S'il y a lieu, les informations mentionnées à l'article 3, paragraphe 4, premier alinéa, sont communiquées via le mécanisme national prévu à l'article 3, paragraphe 4, quatrième alinéa.»;

(12) l'article 37 *bis* suivant est inséré:

«Article 37 *bis*

Rôle de l'ENISA en matière d'assistance mutuelle

1. L'ENISA aide les États membres à se prêter mutuellement assistance au sens de l'article 37 et contribue à faciliter ce processus de coopération pour les entités essentielles et importantes qui fournissent des services dans plus d'un État membre ou qui fournissent des services dans un ou plusieurs États membres et dont les réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres.

2. Aux fins énoncées au paragraphe 1, au plus tard le ... [15 mois après l'entrée en vigueur du présent règlement], l'ENISA procède à une analyse complète des risques transfrontières en matière de cybersécurité liés aux entités essentielles et importantes qui fournissent des services dans plus d'un État membre ou qui fournissent des services dans un ou plusieurs États membres et dont les réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres. Cette analyse évalue les conséquences transfrontières et sur le marché intérieur que peuvent avoir des incidents qui touchent ces entités essentielles et ces entités importantes. Aux fins de cette analyse, l'ENISA élabore une méthodologie, en coopération avec la Commission et le groupe de coopération. Sur la base de l'analyse, l'ENISA établit un rapport complet d'évaluation des risques transfrontières en matière de cybersécurité, qui est mis à jour chaque année.

3. Sur la base du rapport complet d'évaluation des risques transfrontières en matière de cybersécurité, l'ENISA:

(a) recommande le cas échéant aux autorités compétentes concernées de mettre en place des équipes d'examen conjoint pour soutenir la supervision d'entités spécifiques;

(b) élabore des lignes directrices pour les actions communes de supervision;

(c) établit, à la demande des autorités compétentes des États membres concernés, les modalités pratiques de l'exécution des actions communes de supervision;

(d) participe à des actions communes de supervision à la demande des autorités compétentes des États membres concernés, sous réserve de la disponibilité de ressources propres et en proportion de celles-ci;

(e) contribue, à la demande des autorités compétentes des États membres concernés, à évaluer le niveau de mise en œuvre, par une entité essentielle ou importante, des mesures de gestion des risques en matière de cybersécurité prévues à l'article 21.

4. Aux fins du paragraphe 3, point e), du présent article, les autorités compétentes des États membres concernés fournissent à l'ENISA, lorsqu'elles en disposent, une liste des mesures de gestion des risques en matière de cybersécurité prises par l'entité essentielle ou importante conformément à l'article 21, une liste des mesures de supervision ou d'exécution prises, ainsi que la documentation pertinente, notamment les preuves de la mise en œuvre des politiques en matière de cybersécurité, telles que les résultats des audits de sécurité effectués par les autorités compétentes à l'égard de ladite entité au titre des articles 32 et 33.

5. Lorsqu'un État membre bénéficie de l'assistance mutuelle prévue à l'article 37, paragraphe 1, premier alinéa, point c), le point de contact unique informe l'ENISA qu'une assistance mutuelle a été obtenue. Le cas échéant, le point de contact unique indique à quel incident transfrontière visé à l'article 23, paragraphe 6, était liée l'assistance mutuelle obtenue.»

(13) Les annexes I et II sont modifiées conformément à l'annexe de la présente directive.

Article 2,

Transposition

1. Au plus tard le … [12 mois après l'entrée en vigueur de la présente directive], les États membres adoptent et publient les dispositions nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission.

Ils appliquent ces dispositions à partir du… [un jour après la date mentionnée au premier alinéa].

2. Lorsque les États membres adoptent les dispositions visées au paragraphe 1, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

Article 3,

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 4,

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Strasbourg, le

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président/La présidente*
[...]	*[...]*