COM(2026) 11 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 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)

E 20470

COMMISSION
EUROPÉENNE

Strasbourg, le 20.1.2026
COM(2026) 11 final

2026/0011 (COD)

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)

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

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Depuis l'adoption du règlement sur la cybersécurité en 2019, le panorama des menaces de cybersécurité a considérablement évolué[1], dans une réalité géopolitique de plus en plus complexe. Les cyberattaques se sont multipliées et sont devenues plus sophistiquées, en ciblant les infrastructures critiques, les entreprises et le grand public et en tournant spécifiquement autour de l'activité des rançongiciels[2]. Les technologies émergentes telles que l'intelligence artificielle (IA) et l'informatique quantique remodèlent les outils de défense et les tactiques des adversaires. Dans son **rapport de 2024 intitulé «L'avenir de la compétitivité européenne»**, Mario Draghi a souligné la nécessité d'accroître la sécurité et de réduire les dépendances, en la définissant comme étant l'un des principaux domaines dans lesquels une action est requise dans l'Union européenne[3]. Tant la stratégie européenne pour une union de la préparation[4] que la stratégie européenne de sécurité intérieure (ProtectEU)[5] ont placé la cybersécurité au cœur du programme de résilience de l'Union. Ces stratégies reconnaissent que les menaces persistantes en matière de cybersécurité ne sont pas seulement des défis techniques, mais aussi des risques stratégiques pour notre démocratie, notre économie et notre mode de vie. De même, la communication intitulée «Renforcer la sécurité économique de l'UE»[6] fait de la prévention de l'accès à des informations et données sensibles susceptibles de compromettre la sécurité économique de l'Union et de la prévention et de l'atténuation des perturbations des infrastructures critiques de l'Union affectant l'économie de l'Union des objectifs prioritaires, dans lesquels des mesures de cybersécurité efficaces jouent un rôle crucial.

Dans ce contexte, la présente proposition de révision du règlement sur la cybersécurité vise à résoudre **quatre problèmes principaux**: i) le décalage entre le cadre d'action de l'Union 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 (ECCF); iii) la complexité et la diversité des politiques liées à la cybersécurité ayant une incidence sur la posture de cybersécurité de l'Union; et iv) l'accroissement des risques pour la sécurité des chaînes d'approvisionnement des TIC.

Sur la base des principaux problèmes recensés, les **deux objectifs généraux** de l'intervention sont d'accroître les capacités et la résilience en matière de cybersécurité et d'éviter la fragmentation au sein du marché unique:

- en contribuant à renforcer la gouvernance de l'Union en matière de cybersécurité et à faire en sorte que les institutions, autorités et autres parties prenantes concernées

---

1 ENISA, *Rapport de l'ENISA concernant le panorama des menaces 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

2 ENISA, *Rapport de l'ENISA concernant le panorama des menaces 2025.*

3 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.

4 JOIN/2025/130 final.

5 COM/2025/148 final.

6 JOIN(2025) 977 final.

soient mieux préparées à prévenir et à détecter les menaces en matière de cybersécurité et à y réagir de manière coordonnée et efficace; et

- en soutenant l'élaboration, la mise en œuvre et l'adoption d'instruments communs de l'Union en matière de cybersécurité, tels que les schémas de certification, et en fournissant des cadres harmonisés qui renforcent la confiance et l'interopérabilité entre les États membres.

Ces objectifs généraux répondent aux principaux défis recensés dans la définition du problème. Ils reflètent l'objectif stratégique global consistant à renforcer la gouvernance de la cybersécurité dans l'Union et à soutenir le développement d'un marché unique numérique sûr, résilient et compétitif.

Afin de contribuer à la réalisation des objectifs généraux énumérés ci-dessus, cette intervention poursuit les **objectifs spécifiques (OS)** suivants:

- pour remédier au décalage entre le cadre d'action de l'Union en matière de cybersécurité et les besoins des parties prenantes:
  - OS 1: créer les capacités nécessaires pour mettre en œuvre efficacement les politiques de cybersécurité de l'Union et une coopération opérationnelle continue qui permettra une coopération plus structurée entre les États membres;
  - OS 2: élaborer et mettre en œuvre des moyens et des mécanismes permettant de soutenir et de répondre efficacement aux besoins des États membres, de l'industrie et des autres parties prenantes;
- pour remédier à l'adoption et à l'efficacité limitées de l'ECCF:
  - OS 3: créer les conditions préalables à une mise en œuvre plus rapide des schémas de certification de cybersécurité en fonction des besoins du marché, en élargissant le champ d'application de l'ECCF, en garantissant une maintenance efficace et des procédures souples et en renforçant la transparence;
- pour remédier à la fragmentation du paysage de la conformité et à la complexité des cadres horizontaux et sectoriels:
  - OS 4: créer des mécanismes et des conditions pour faciliter le respect des exigences en matière de cybersécurité, en rendant ainsi leur mise en œuvre plus cohérente et plus efficace.
- pour faire face aux risques de cybersécurité dans la chaîne d'approvisionnement:
  - OS 5: réduire les risques pour les chaînes d'approvisionnement critiques des TIC posés par des entités établies dans des pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlées par des entités de tels pays (fournisseurs à haut risque) et réduire les dépendances critiques en élaborant un cadre cohérent et efficace au niveau de l'Union pour faire face aux risques liés à la sécurité des chaînes d'approvisionnement des TIC.

La révision du règlement sur la cybersécurité relève du **programme pour une réglementation affûtée et performante (REFIT).** Elle contribue fortement à améliorer la clarté, à supprimer les inefficacités et à harmoniser les procédures entre les cadres juridiques.

La révision du règlement sur la cybersécurité contribue au bon fonctionnement du marché intérieur tout en garantissant la sécurité et l'autonomie stratégique de l'Union.

Plus concrètement, elle propose une réforme complète du mandat de l'Agence de l'Union européenne pour la cybersécurité (ENISA) qui apporte un soutien efficace à la mise en œuvre des politiques et apporte une valeur ajoutée en ce qui concerne le soutien à la coopération opérationnelle entre les États membres.

Compte tenu de l'augmentation des risques et des défis en matière de cybersécurité auxquels l'Union est confrontée, la proposition vise à accroître les ressources financières et humaines de l'ENISA afin de tenir compte du renforcement de son rôle et de ses tâches, ainsi que de sa position critique dans la défense de l'écosystème numérique de l'Union, ce qui permettra à l'ENISA d'exécuter efficacement les tâches qui lui sont confiées en vertu de la présente proposition.

La révision contribuera également à éliminer les pratiques fragmentées, en améliorant la coordination tout en réduisant les coûts de mise en conformité et les coûts opérationnels à long terme. En abrogeant l'actuel règlement sur la cybersécurité et en introduisant un ECCF réformé, la proposition fournit un outil plus efficace et efficient qui stimule la confiance des entreprises, du grand public et des pouvoirs publics et facilite le respect de la législation pertinente de l'Union. Elle accroît l'efficacité en révisant le modèle de gouvernance et en soutenant des procédures de certification plus prévisibles, cohérentes et souples afin de permettre une élaboration et une mise en œuvre plus rapides des schémas.

Le renforcement des synergies avec les cadres juridiques pertinents existants de l'Union encouragera la certification en tant qu'outil de conformité pour les entreprises et réduira la charge administrative pesant sur les organismes d'évaluation de la conformité qui sont actifs au titre de plusieurs actes législatifs en matière de cybersécurité. En outre, en élargissant le champ d'application de l'ECCF et en permettant l'élaboration d'un schéma sur la posture de cybersécurité des entités, la proposition réduit les coûts de mise en conformité pour les entités soumises à la législation pertinente de l'Union en matière de cybersécurité, en commençant par les entités relevant du champ d'application de la directive SRI 2. 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. Outre cette révision, une proposition de directive introduisant des modifications ciblées de la directive SRI 2 vise à simplifier le respect et à garantir une 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 rançongiciels et la surveillance des entités fournissant des services transfrontières.

Le nouveau règlement crée également un cadre harmonisé pour faire face aux risques non techniques pesant sur les chaînes d'approvisionnement des TIC, en réduisant ainsi la fragmentation actuelle des approches entre les États membres. Ensemble, ces aspects représentent une simplification et une modernisation substantielles du cadre juridique de l'Union en matière de cybersécurité, qui alignent pleinement celui-ci sur les principes du programme REFIT de clarté, d'efficacité et de préparation au numérique.

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

L'Union a élargi son portefeuille d'outils juridiques et stratégiques en adoptant plusieurs instruments juridiques et mesures stratégiques: 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», à savoir la directive sur la résilience des entités critiques (directive CER); iii) le règlement sur la cyberrésilience renforce la cybersécurité des produits; iv) le règlement sur la cybersolidarité met en place des capacités de réaction à l'échelle de l'Union; v) le schéma directeur de l'UE en matière de cybersécurité[7] soutient la coopération au niveau de l'Union en matière de gestion des crises, dans le cadre de laquelle la Commission et le haut représentant jouent des rôles clés dans la préparation et la réaction aux incidents de cybersécurité majeurs; vi) la boîte à outils sur la cybersécurité des réseaux 5G (boîte à outils 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 leur cybersécurité; et viii) l'académie des compétences en matière de cybersécurité[9] répond au défi croissant que constitue la pénurie de talents dans le secteur de la cybersécurité.

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

La révision du règlement sur la cybersécurité est alignée sur les dispositions de la directive SRI 2 et les renforce en ce qui concerne le rôle de l'ENISA dans le soutien à la mise en œuvre de la directive SRI 2, y compris en ce qui concerne le soutien à la coopération opérationnelle; elle est également alignée sur le règlement sur la cyberrésilience, y compris en ce qui concerne la vue d'ensemble et la gestion des vulnérabilités dans l'ensemble du marché intérieur, et accroît la valeur ajoutée de la conscience situationnelle commune. En ce qui concerne l'ECCF, la révision du règlement sur la cybersécurité est alignée sur le règlement sur la cyberrésilience en ce qui concerne les objectifs de sécurité des produits et la gestion des vulnérabilités, ainsi que sur le nouveau cadre législatif (NCL) en matière d'accréditation. En outre, il existe une forte synergie découlant de l'élaboration de la certification de posture de cybersécurité pour la directive SRI 2 ainsi que, potentiellement, pour faciliter le respect d'autres actes juridiques pertinents de l'Union, tels que le règlement général sur la protection des données (RGPD), sans préjudice de leurs exigences spécifiques en matière de certification. En outre, le cadre horizontal qui traite des risques de cybersécurité des chaînes d'approvisionnement des TIC soutient l'objectif général de la directive SRI 2 consistant à créer un niveau commun élevé de cybersécurité dans l'ensemble de l'Union et s'appuie sur l'approche fondée sur les risques de la directive SRI 2.

En outre, la révision du règlement sur la cybersécurité, combinée à la proposition de directive introduisant des modifications ciblées de la directive SRI 2 dans un but de simplification, fournit les outils nécessaires pour rendre ce cadre global plus efficace et efficient dans

[7] COM/2025/66 final.
[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.

l'obtention des résultats escomptés, renforcer la dimension européenne et combler les lacunes réglementaires qui subsistent.

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

La révision du règlement sur la cybersécurité compléterait la directive CER, qui inclut des considérations relatives à la chaîne d'approvisionnement dans le cadre des mesures de résilience des entités critiques. En outre, elle compléterait les initiatives à venir, telles que: i) le règlement sur le développement de l'informatique en nuage et de l'IA (CAIDA), qui vise, entre autres, à remédier à l'absence d'offre concurrentielle de services d'informatique en nuage dans l'Union à une échelle suffisante pour répondre aux besoins des cas d'usage ou des secteurs d'utilisation hautement critiques, ii) la proposition de règlement sur les réseaux numériques; iii) la prochaine révision du règlement (UE) 2023/1781[11]; iv) le cadre applicable aux marchés publics[12] qui est actuellement en cours d'évaluation[13] et la proposition de règlement relatif à la simplification de la législation numérique (règlement omnibus sur le numérique)[14], qui prévoit l'obligation pour l'ENISA de mettre en place un guichet unique pour la notification des incidents, par l'intermédiaire duquel les entités peuvent remplir simultanément leurs obligations de notification des incidents découlant de plusieurs actes juridiques. En outre, elle renforcerait la position des autorités et des opérateurs de l'Union lorsqu'ils dialoguent avec les partenaires du sud de la Méditerranée, notamment en favorisant l'interconnexion au moyen d'infrastructures numériques sûres et fiables dans toute la Méditerranée, ce qui est un objectif fondamental du pacte pour la Méditerranée.

La révision du règlement sur la cybersécurité est également conforme aux documents stratégiques de l'Union, en particulier en ce qui concerne le cadre de sécurité de la chaîne d'approvisionnement des TIC. Dans la stratégie ProtectEU, la Commission a en outre déclaré qu'une approche harmonisée de la sécurisation de la chaîne d'approvisionnement des technologies de l'information et de la communication (TIC) pourrait remédier à la fragmentation actuelle du marché intérieur due aux différences d'approche entre pays, éviter les dépendances critiques et réduire les risques que les fournisseurs à haut risque font peser sur les chaînes d'approvisionnement, ce qui permettra de sécuriser les infrastructures critiques. La stratégie de sécurité économique a également souligné la nécessité de rendre l'économie et la chaîne d'approvisionnement de l'Union plus résilientes afin de promouvoir la propre compétitivité de l'Union[15]. La nécessité de s'attaquer aux perturbations des chaînes d'approvisionnement et aux cyberattaques a également été soulignée dans la stratégie pour une union de la préparation et dans le livre blanc sur l'avenir de la défense européenne[16]. Elle est également alignée sur le rapport sur l'avenir de la compétitivité européenne de Mario Draghi, comme souligné ci-dessus. Qui plus est, la révision du règlement sur la cybersécurité dans le domaine de la sécurité de la chaîne d'approvisionnement des TIC avec la

---

11 Règlement (UE) 2023/1781 du Parlement européen et du Conseil du 13 septembre 2023 établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs et modifiant le règlement (UE) 2021/694 (règlement sur les puces) *(JO L 229 du 18.9.2023, p. 1)*.

12 En particulier les directives 2014/23/UE, 2014/24/UE et 2014/25/UE.

13 Commission européenne, Commission launches call for evidence and public consultation on the evaluation of the Public Procurement Directives (la Commission lance un appel à contributions et une consultation publique sur l'évaluation des directives sur les marchés publics), https://single-market-economy.ec.europa.eu/news/commission-launches-call-evidence-and-public-consultation-evaluation-public-procurement-directives-2024-12-13_en.

14 COM/2025/837 final

15 JOIN/2023/20 final.

16 JOIN/2025/120 final.

communication conjointe récemment adoptée au Parlement européen et au Conseil sur le renforcement de la sécurité économique de l'UE[17].

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La base juridique de la présente proposition est l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE). L'article 114 TFUE prévoit l'adoption de mesures visant à assurer l'établissement et le fonctionnement du marché intérieur. Le règlement (UE) 2019/881 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications, communément appelé «règlement sur la cybersécurité»[18], a initialement été adopté au titre de cette disposition.

Dans le domaine de la cybersécurité de la chaîne d'approvisionnement des TIC, la fragmentation des cadres nationaux traitant des facteurs de risque non techniques a des effets négatifs sur le fonctionnement du marché intérieur, étant donné que les divergences entre les approches nationales pourraient, en fin de compte, accroître la vulnérabilité de certains États membres, avec des retombées potentielles dans l'ensemble de l'Union, ce qui aurait une incidence sur la résilience globale ainsi que sur la fiabilité.

Compte tenu de la nature évolutive des menaces pour la cybersécurité et de l'interdépendance croissante des systèmes numériques des États membres, l'article 114 TFUE reste la base juridique justifiée pour la révision du règlement sur la cybersécurité. Le règlement proposé reflète les évolutions les plus récentes du paysage législatif en matière de cybersécurité, en particulier compte tenu des responsabilités croissantes de l'ENISA et de l'élargissement du champ d'application des certifications et de la gestion des risques.

• 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 l'actuel règlement sur la cybersécurité.

Comme cela a déjà été analysé dans le cadre du règlement sur la cybersécurité, l'intervention de l'Union est essentielle étant donné que les menaces en matière de cybersécurité et les défis qui y sont liés s'étendent au-delà des différents États membres. Les solutions nationales fragmentées se sont révélées insuffisantes pour assurer la confiance et la coordination à l'échelle du marché. Un cadre juridique révisé de l'Union est nécessaire pour supprimer les obstacles, assurer une mise en œuvre cohérente et soutenir les États membres dans un environnement réglementaire et de menaces de plus en plus complexe. La cybersécurité est un sujet présentant un intérêt commun pour l'Union.

Les actions couvertes par le règlement proposé apportent une valeur ajoutée manifeste en soutenant l'harmonisation, la clarté juridique et les réponses coordonnées aux défis en matière de cybersécurité.

Les tâches actuelles de l'ENISA ont été élargies par des actes législatifs ultérieurs sans que ses responsabilités essentielles et ses ressources ne soient réexaminées en profondeur, ce qui a

[17] JOIN/2025/977 final

[18] Règlement (UE) 2019/881 - FR - EUR-Lex

créé des inefficacités et une priorisation insuffisante des tâches essentielles destinées à soutenir les États membres. Par conséquent, la proposition d'intervention vise à affiner et à hiérarchiser les tâches actuelles afin de renforcer le mandat de l'ENISA, en lui permettant de faire office de centre d'expertise unique en matière de cybersécurité au niveau de l'Union. Sur ce point, il n'y a pas de différence substantielle en termes de subsidiarité par rapport au règlement sur la cybersécurité. En outre, la diversité des schémas nationaux de certification et des approches réglementaires des États membres crée une fragmentation du marché et des charges supplémentaires en matière de conformité, ce qui nuit à la compétitivité.

La nouvelle proposition prévoit également de nouvelles actions en ce qui concerne les politiques relatives à la chaîne d'approvisionnement et les efforts de simplification au niveau de l'Union. Elle renforce encore la sécurité de la chaîne d'approvisionnement et le secteur de la cybersécurité au sein de l'Union et améliore la préparation et la résilience des États membres et de l'industrie.

Les dépendances à l'égard d'entités établies dans des pays tiers posant des risques de cybersécurité ou contrôlées par de tels pays tiers, par des entités établies dans ces pays tiers ou par des ressortissants de ces pays tiers (fournisseurs à haut risque) affectent des entités de toute l'Union, tandis que les incidents de cybersécurité importants dans la chaîne d'approvisionnement se propagent souvent au-delà des frontières nationales. En outre, compte tenu de la nature transfrontière des chaînes d'approvisionnement des TIC, la fragmentation des exigences de conformité au sein du marché intérieur compromettrait la sécurité juridique pour les entités. En outre, les propositions relatives au cadre financier pluriannuel (CFP) imposent l'exclusion des fournisseurs à haut risque afin de protéger l'intégrité du budget de l'Union et les intérêts en matière de sécurité. Le cadre pour le fonctionnement de la chaîne d'approvisionnement inclus dans le présent règlement prévoit le mécanisme permettant de recenser les pays qui suscitent des préoccupations en matière de cybersécurité, une activité qui ne peut être menée efficacement qu'au niveau de l'Union. En ce qui concerne la sécurité de la chaîne d'approvisionnement des TIC, seule une intervention au niveau de l'Union garantira le même niveau minimal de sécurité dans l'ensemble de l'Union et l'harmonisation nécessaire des approches.

L'objectif du règlement sur la cybersécurité est maintenu et renforcé dans le cadre de cette révision. Cet objectif ne peut pas être atteint de manière suffisante par les États membres, mais peut l'être mieux au niveau de l'Union, conformément à l'article 5 du traité sur l'Union européenne.

- **Proportionnalité**

Les mesures proposées n'excèdent pas ce qui est nécessaire pour atteindre les objectifs stratégiques de la proposition. De plus, la portée de l'intervention de l'Union n'interdit aucune mesure nationale relative à des questions touchant à la sûreté de l'État. L'action de l'Union se justifie pour des raisons de subsidiarité et de proportionnalité.

La proposition vise à mieux refléter, sur le plan juridique, le mandat de l'ENISA et le processus d'élaboration, d'adoption et de maintenance des certificats de cybersécurité européens. Bien que la proposition prévoie certaines nouvelles tâches pour l'ENISA, son objectif est de soutenir les États membres dans les domaines où des lacunes importantes ont été recensées. L'ENISA ne remplacera pas les CSIRT des États membres. En ce qui concerne l'ECCF, la certification reste volontaire et peut aider les entités à démontrer qu'elles respectent les exigences de l'Union en matière de cybersécurité. Cette approche garantit le respect du principe de proportionnalité.

En ce qui concerne les solutions proposées en matière de sécurité de la chaîne d'approvisionnement des TIC, le cadre prévoit la collecte de preuves de ce qui constitue des actifs essentiels et des mesures qui seraient proportionnées et nécessaires pour garantir la réduction des risques liés aux chaînes d'approvisionnement critiques. Avant de définir ces mesures, il sera procédé à une évaluation des incidences économiques qui examinera, entre autres, la faisabilité économique, les autres solutions disponibles sur le marché et le cycle de vie des produits concernés. Cette évaluation éclairera la détermination des mesures fondées sur les risques qui sont nécessaires et les plus appropriées.

- **Choix de l'instrument**

La présente proposition prévoit le réexamen du règlement (UE) 2019/881, qui définit le mandat actuel et les missions de l'ENISA et de l'ECCF. Par conséquent, mieux vaut établir le mandat révisé de l'ENISA et les modifications de l'ECCF en vertu du même instrument juridique, en l'occurrence un règlement La législation proposée prévoit également un cadre efficace au niveau de l'Union pour faire face aux risques liés à la sécurité de la chaîne d'approvisionnement des TIC, pour lesquels un règlement permettrait de gérer les problèmes recensés et d'atteindre les objectifs formulés plus efficacement, étant donné que seule une intervention au niveau de l'Union garantira le même niveau de sécurité dans l'ensemble de l'Union et l'harmonisation nécessaire des approches. Dans le cas d'une directive, le processus de transposition pourrait laisser trop de marge de manœuvre au niveau national, ce qui pourrait conduire à un manque d'uniformité de certaines exigences essentielles en matière de cybersécurité, à une insécurité juridique, à une fragmentation accrue ou même à des situations transfrontières discriminatoires.

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**

Conformément à l'article 67 du règlement (UE) 2019/881, la Commission européenne a apprécié la pertinence, l'incidence, l'efficacité, l'efficience, la cohérence et la valeur ajoutée de l'ENISA et de l'ECCF, eu égard à l'évolution du paysage technologique et réglementaire. Cette évaluation, achevée en décembre 2024, couvrait la période 2017-2023 et visait à réexaminer le mandat et les activités de l'ENISA ainsi qu'à évaluer le rôle de l'ECCF dans la promotion d'un cyberespace sûr dans l'ensemble de l'Union. Les principales constatations peuvent être résumées comme suit.

- **Pertinence:** la pertinence de l'ENISA dans le domaine de la cybersécurité est soulignée par sa réactivité à l'évolution des besoins des parties prenantes et son adaptabilité à un paysage en mutation. Bien que la satisfaction des parties prenantes soit généralement positive, il existe des possibilités d'accroître l'impact de l'ENISA. Cet objectif peut être atteint en améliorant le soutien qu'elle apporte et sa visibilité pour divers secteurs, en particulier les petites et moyennes entreprises (PME), qui ont souvent du mal à se conformer aux exigences en matière de cybersécurité. Une meilleure organisation des ressources et une coordination plus claire avec les autorités nationales sont essentielles. La redéfinition des activités prioritaires et l'optimisation des ressources existantes permettront de mieux aligner l'ENISA sur les besoins dynamiques du paysage européen de la cybersécurité.

  En ce qui concerne l'ECCF, malgré son postulat prometteur, ce cadre est toujours considéré comme ayant plus de potentiel que d'impact concret: en effet, un seul schéma de certification est récemment devenu opérationnel. Ce cadre est conçu pour

s'intégrer harmonieusement à d'autres actes juridiques de l'Union afin de rationaliser les procédures et de faciliter les échanges transfrontières. Son importance est soulignée dans des domaines à niveau élevé de garantie tels que les services en nuage et les infrastructures 5G.

- **Efficacité:** l'ENISA a rempli avec succès son mandat en livrant la quasi-totalité des réalisations prévues, en mettant en évidence sa flexibilité et sa résilience lors de crises telles que la pandémie de COVID-19 et la guerre d'agression menée par la Russie contre l'Ukraine. Toutefois, une meilleure hiérarchisation des priorités, une orientation claire et une allocation stratégique des ressources sont nécessaires pour accroître son efficacité. Une approche plus souple de la gouvernance interne est essentielle pour s'adapter à l'évolution des besoins de cybersécurité et réduire au minimum les retards.

  Si l'ECCF avait pour but d'harmoniser la certification de cybersécurité dans l'ensemble de l'Union, elle a toutefois rencontré des difficultés importantes, notamment des limitations procédurales et une fragmentation, qui ont entraîné des retards et des inefficacités, tels que le retard dans l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC). Des facteurs externes, tels que les tensions géopolitiques et la pandémie de COVID-19, ont encore compliqué la réalisation des objectifs de l'ECCF, ce qui souligne la nécessité de mesures adaptables et d'une allocation cohérente des ressources entre les parties prenantes afin de permettre une certification de cybersécurité uniforme et efficace. Malgré ces obstacles, des résultats positifs ont été obtenus, notamment en ce qui concerne la sensibilisation des États membres à l'importance et aux complexités de la certification de cybersécurité.

- **Efficience:** l'ENISA a fonctionné efficacement dans son cadre organisationnel matriciel, qui favorise la coopération et la hiérarchisation des tâches. Toutefois, l'ENISA a été confrontée à des difficultés pour répondre à des demandes croissantes et pourvoir des postes spécialisés, qui ont été exacerbées par une pénurie mondiale de spécialistes des technologies de l'information, ce qui a entraîné des retards et une lourde charge de travail. Pour remédier à ces problèmes, l'ENISA pourrait optimiser ses effectifs internes et réaffecter efficacement les ressources, comme l'ont démontré des ajustements stratégiques tels que le transfert de ressources vers l'action de soutien à la cybersécurité en 2022. En outre, l'amélioration de la gestion budgétaire et la réduction des dépenses administratives amélioreraient encore l'efficacité opérationnelle de l'Agence.

  L'efficacité de l'ECCF a été critiquée en raison de la prolongation des délais d'adoption des schémas de certification de cybersécurité et des complexités associées, le premier schéma n'ayant été adopté qu'au début de l'année 2024, près de cinq ans après l'adoption du règlement sur la cybersécurité. Les défis politiques et techniques, tels que les débats sur la souveraineté des données et les difficultés rencontrées pour traduire les projets en actes juridiques, ont contribué à des retards. Les défis politiques et les exigences techniques ont entravé les progrès, comme nous l'avons vu avec le schéma européen de certification pour les services d'informatique en nuage (EUCS) et le schéma EU5G. Malgré ces inefficacités, le cadre a donné lieu à plusieurs aspects positifs. Toutefois, il reste nécessaire d'améliorer la participation des parties prenantes et la gouvernance interne afin de garantir un fonctionnement optimal et une contribution stratégique.

- **Cohérence:** la cohérence de l'ENISA est soutenue par un engagement important des parties prenantes et par son alignement sur les cadres législatifs récents. Toutefois, afin de renforcer la cohérence et l'allocation des ressources, il est essentiel d'améliorer les synergies avec d'autres organes de l'Union, tels que le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité (CECC), et les autorités nationales. En outre, la communication interne et la gestion des ressources au sein de l'ENISA, ainsi que la transparence des interactions avec les parties prenantes privées, doivent être affinées. Une délimitation claire des tâches de l'ENISA, conforme au règlement sur la cyberrésilience et à la directive SRI 2, améliorera à la fois leur efficacité et leur cohérence réglementaire.

  En ce qui concerne l'ECCF, une cohérence totale avec les autres instruments législatifs de l'Union, y compris la directive SRI 2 et le règlement sur la cyberrésilience, est essentielle pour garantir une approche unifiée en matière de cybersécurité. Bien que l'ECCF soit théoriquement alignée sur ces mesures législatives, son intégration réelle reste complexe et nécessite un contrôle diligent. La mise en œuvre du schéma EUCC adopté dans le cadre du règlement sur la cyberrésilience constituera un test important à cet égard.

- **Valeur ajoutée de l'UE:** l'ENISA a contribué de manière substantielle à l'écosystème de cybersécurité de l'Union en promouvant la coopération et en harmonisant les pratiques. Le rôle qu'elle a joué dans la facilitation des efforts nationaux et la fourniture d'informations sur les menaces émergentes a été essentiel. Toutefois, les critiques des parties prenantes du secteur privé quant à la nécessité d'un soutien plus adapté indiquent qu'il est nécessaire d'améliorer l'engagement des parties prenantes et la collaboration de l'industrie. Une réévaluation stratégique de la gestion des ressources permettrait à l'ENISA de mieux s'adapter à l'évolution des défis en matière de cybersécurité et de servir plus efficacement diverses parties prenantes. L'ECCF visait à introduire des processus de certification harmonisés, mais a été confronté à des difficultés de mise en œuvre en raison de délais prolongés et de la fragmentation. La valeur ajoutée de l'ECCF a été limitée en raison de ses lacunes dans la réalisation de ses objectifs et de son manque d'efficacité. Malgré ces difficultés, l'ECCF a amélioré l'harmonisation entre les États membres et établi de meilleures possibilités de coopération, notamment en créant des forums de coopération des parties prenantes tels que le groupe européen de certification de cybersécurité (GECC).

- **Consultation des parties intéressées**

Entre 2023 et 2025, plusieurs consultations des parties prenantes ont été menées dans le cadre de l'évaluation du règlement sur la cybersécurité et dans le cade de sa révision, comme expliqué ci-après.

– **En 2023**, 65 entretiens ont été menés (dont 52 étaient davantage axés sur l'ENISA et 13 ciblaient principalement l'ECCF), un programme d'enquête a été mené et a reçu 209 réponses (dont 70 sur l'ECCF), une consultation publique s'est achevée et deux ateliers ont été organisés sur l'analyse SWOT (forces, faiblesses, opportunités et menaces) et sur les recommandations à son sujet, auxquels ont participé respectivement 26 et 70 personnes. Ces activités visaient spécifiquement à recueillir les points de vue des parties prenantes afin d'évaluer l'impact, l'efficacité et l'efficience de l'ENISA. Le rapport final de l'*étude à l'appui de l'évaluation de l'Agence de l'Union européenne pour la cybersécurité (ENISA) et du cadre européen de certification de cybersécurité élaboré pour*

la Commission par PwC, Intellera Consulting et PPMI (2024) a été achevé en décembre 2024.

– **En 2025,** la Commission a lancé un appel à contributions. Les parties prenantes ont notamment été invitées à soumettre des contributions écrites, y compris des documents de prise de position, des rapports techniques ou des commentaires sur des propositions de réforme spécifiques. Au total, 184 contributions individuelles ont été reçues d'un large éventail de catégories de parties prenantes, dont des associations sectorielles, des entreprises de cybersécurité, des PME, des établissements universitaires et des organisations d'intérêt public.

– **Entre avril et juin 2025**, la Commission a organisé une consultation publique dans le cadre de la révision du règlement sur la cybersécurité et a reçu 193 réponses. Cette consultation a consisté en 38 questions, à la fois fermées et ouvertes, qui portaient sur le mandat de l'ENISA, sur l'ECCF, sur la sécurité de la chaîne d'approvisionnement des TIC et sur la simplification.

– **Consultation ciblée (entretiens):** une série d'entretiens semi-structurés ont été menés avec certaines parties prenantes. Parmi celles-ci figuraient des représentants de l'ENISA ainsi que des autorités publiques nationales qui ont mis en place ou qui gèrent des plateformes nationales de signalement. Les entretiens ont porté sur le rôle et les capacités de l'ENISA, sur le fonctionnement opérationnel de l'ECCF, sur les difficultés pratiques liées à l'alignement des processus de certification au niveau national et au niveau de l'Union, sur les charges liées au signalement et sur les obstacles à la mise en œuvre. Ces discussions ont fourni des informations qualitatives qui ont enrichi l'interprétation des résultats de la consultation publique et ont permis d'affiner les options stratégiques.

– **Consultation des représentants des États membres dans le cadre du groupe du Conseil[19] et lors de discussions bilatérales**, au cours desquelles les États membres ont eu la possibilité d'exprimer leur point de vue sur le réexamen du règlement sur la cybersécurité.

– **Consultation ciblée [groupes de l'ECCF – GECC, groupe des parties prenantes pour la certification de cybersécurité (SCCG)]:** la Commission, en sa qualité de présidente des deux groupes, a présenté l'état d'avancement de la révision du règlement sur la cybersécurité lors des réunions du GECC des 12 mars et 3 juillet 2025, ainsi que lors de la réunion du SCCG du 17 mars 2025. En outre, des avis d'experts supplémentaires ont été recueillis auprès des membres du GECC au moyen de questionnaires.

La consultation s'est concentrée sur cinq grands aspects jugés essentiels au fonctionnement et à la cohérence futurs du cadre de cybersécurité de l'Union:

- **Le mandat et le rôle opérationnel de l'ENISA**, y compris le soutien aux États membres et l'expertise dans le domaine des technologies émergentes;
- **l'efficacité du cadre européen de certification de cybersécurité**, y compris les processus de gouvernance et de développement;
- **la complexité et la fragmentation des obligations en matière de cybersécurité**, avec une attention particulière accordée aux charges liées au signalement et aux possibilités de simplification;

[19] Groupe horizontal «Questions liées au cyberespace».

- **la proportionnalité des exigences applicables aux PME** et la possibilité de trajectoires de mise en conformité différenciées; et
- **les incidences sociétales et économiques** des règles harmonisées en matière de cybersécurité, y compris les effets sur les consommateurs, les droits, l'innovation et la compétitivité.

- **Analyse d'impact**

La révision du règlement sur la cybersécurité, ainsi que la proposition de directive introduisant des modifications ciblées de la directive SRI 2, ont été étayées par une analyse d'impact (voir le résumé ci-dessous). Le comité d'examen de la réglementation (CER) a émis un «avis favorable assorti de réserves» sur le projet de rapport d'analyse d'impact relatif à la révision du règlement sur la cybersécurité qui a été soumis une nouvelle fois[20]. L'analyse d'impact a été adaptée afin de tenir compte des recommandations et des observations du CER.

La proposition stratégique finale ne s'écarte pas des options évaluées dans l'analyse d'impact.

La Commission a examiné des options dans quatre domaines d'intervention, compte tenu des objectifs spécifiques à atteindre: 1) le mandat de l'ENISA (qui fait également partie de l'actuel règlement sur la cybersécurité); 2) l'ECCF (qui fait également partie de l'actuel règlement sur la cybersécurité); 3) des modifications ciblées de la directive SRI 2, dans le but de la simplifier, mais aussi de la relier au mandat de l'ENISA et à l'ECCF; et 4) la sécurité de la chaîne d'approvisionnement des TIC, qui est également pertinente tant pour l'écosystème de la directive SRI 2 que pour l'ECCF. Chaque ensemble d'options représente un domaine d'intervention à part entière. Tous les groupes d'options sont néanmoins interconnectés et pertinents les uns pour les autres.

Options pour remédier au décalage entre le cadre d'action de l'Union en matière de cybersécurité et les besoins des parties prenantes dans un environnement de plus en plus hostile

Option A.1: *clarification du mandat de l'ENISA et établissement de priorités* - Cette option fournirait un cadre clair et stable pour les tâches de l'ENISA en intégrant les tâches définies par d'autres actes législatifs.

Option A.2: *réforme du mandat de l'ENISA* – Cette option abrogerait et remplacerait le règlement sur la cybersécurité, en révisant le mandat de l'Agence.

Option A.3: réforme du mandat de l'ENISA avec une priorité résolument accordée au soutien opérationnel – Cette option s'appuierait sur l'option A.2. En outre, l'ENISA développerait des capacités pour aider directement les entités relevant de la directive SRI 2, à la demande d'un État membre, à réagir aux incidents de cybersécurité et à s'en remettre.

Options pour l'ECCF

Option B.1: *clarification du champ d'application, des éléments et des objectifs de l'ECCF et introduction d'un mécanisme de maintenance* – Cette option prévoirait un nouveau mécanisme de maintenance pour les schémas, après leur adoption, à mettre en œuvre par l'ENISA.

[20] Règlement (UE) 2019/881 (http://data.europa.eu/eli/reg/2019/881/oj).

Option B.2: *réforme de l'ECCF au moyen d'une révision de ses procédures et d'un élargissement de son champ d'application afin de simplifier le respect des obligations réglementaires* – Cette option abrogerait le règlement sur la cybersécurité et le remplacerait par un nouveau règlement. Outre l'option B.1, les procédures relatives à la demande, à l'élaboration et à l'adoption de schémas seraient révisées afin d'améliorer la responsabilité et l'efficacité.

Option B.3: *réforme de l'ECCF telle qu'envisagée dans l'option B.2 et introduction d'une certification obligatoire pour la posture de cybersécurité* – Cette option s'appuierait sur l'option B.2, mais vise à accroître encore l'incidence du cadre en introduisant une certification obligatoire des entités essentielles en tenant compte de scénarios de risque spécifiques, au lieu de s'appuyer uniquement sur la certification volontaire des entités.

Options de simplification

Option C.1: *adoption d'une approche fondée sur des instruments non contraignants et non législatifs, y compris en ayant recours aux habilitations existantes (adoption d'actes d'exécution au titre de l'article 21, paragraphe 5, et de l'article 23, paragraphe 11, de la directive SRI 2)* – Cette option envisage l'adoption d'actes d'exécution en utilisant les habilitations existantes au titre de la directive SRI 2 afin de garantir un degré plus élevé d'harmonisation des mesures de gestion des risques de cybersécurité, des seuils de notification des incidents ainsi que des types d'informations, des formats et de la procédure de notification. Elle prévoit également l'adoption d'un ensemble de lignes directrices visant à renforcer la sécurité juridique et à assurer une mise en œuvre harmonisée.

Option C.2: *Intervention ciblée – mesures visant à simplifier davantage le respect du cadre législatif pertinent de l'Union en matière de cybersécurité* – Cette option implique une intervention limitée au moyen de modifications apportées au règlement sur la cybersécurité et à la directive SRI 2 dans le but de simplifier certains aspects du cadre de cybersécurité, y compris des adaptations du champ d'application, une harmonisation maximale des actes d'exécution, la démonstration de la conformité au moyen d'une certification et l'adoption de l'ensemble de lignes directrices envisagé dans le cadre de l'option C.1.

Option C.3: *harmonisation des mesures liées à la cybersécurité énoncées dans la législation de l'Union* – Cette option s'appuierait sur l'option C.2 et supprimerait toutes les mesures de gestion des risques de cybersécurité incluses dans la législation sectorielle et les habilitations relatives à ces mesures. En lieu et place, l'écosystème de la directive SRI 2 serait modifié afin de prévoir des exigences rationalisées pour tous les types d'entités, dans le but de promouvoir l'harmonisation.

Options pour la sécurité de la chaîne d'approvisionnement des TIC

Option D.1: adoption d'une approche non contraignante pour faire face aux risques de cybersécurité dans les chaînes d'approvisionnement des TIC – Cette option ne prévoirait pas d'intervention réglementaire au niveau de l'Union. En lieu et place, la Commission augmenterait le nombre d'évaluations coordonnées des risques et de boîtes à outils volontaires.

Option D.2: *intervention réglementaire ad hoc codifiant la boîte à outils 5G* – Cette option codifierait les mesures de la boîte à outils 5G. Elle introduirait l'obligation pour les États membres de veiller à ce que les composants provenant de fournisseurs à haut risque ne soient pas utilisés dans les actifs essentiels du réseau.

Option D.3: *cadre global et horizontal pour faire face aux risques de cybersécurité dans les chaînes d'approvisionnement des TIC* – Cette option établirait un cadre réglementaire horizontal et neutre sur le plan technologique et sectoriel afin de faire face aux risques de cybersécurité non techniques dans les chaînes d'approvisionnement des TIC.

Après une analyse approfondie, la combinaison d'options suivante est apparue comme le train de mesures privilégié: option A.2 (réforme du mandat de l'ENISA); option B.2 (réforme de l'ECCF au moyen d'une révision de ses procédures et d'un élargissement de son champ d'application afin de faciliter la simplification du respect des obligations réglementaires); option C.2 (intervention ciblée – mesures visant à faciliter le respect du cadre législatif pertinent de l'Union en matière de cybersécurité) et option D.3 (cadre global et horizontal pour faire face aux risques de cybersécurité dans les chaînes d'approvisionnement des TIC).

Cette combinaison offre une réponse équilibrée aux défis stratégiques recensés, en renforçant considérablement l'efficacité, l'efficience et la cohérence dans l'ensemble de l'Union.

La transition vers l'option privilégiée proposée pour le cadre réglementaire entraînera des coûts, tant pour l'ENISA, qui devra s'acquitter de ses nouvelles tâches (estimées à un maximum de 161,3 millions d'euros sur cinq ans), que pour les autorités publiques de l'Union chargées de la surveillance (estimées à un maximum de 80 millions d'euros sur cinq ans, compte tenu des économies de coûts pertinentes). En ce qui concerne les entreprises, sur cinq ans, la suppression progressive d'équipements spécifiques à haut risque pourrait entraîner des coûts annuels de 3,4 à 4,3 milliards d'euros pour les opérateurs de réseaux mobiles, tandis que les investissements dans des fournisseurs de confiance pourraient atteindre 2 milliards d'euros par an.

Dans le même temps, des obligations de mise en conformité rationalisées et réduites devraient permettre aux entreprises de réaliser des économies allant jusqu'à 15,3 milliards d'euros sur cinq ans. En outre, l'amélioration de la posture de cybersécurité globale et de la souveraineté technologique de l'Union et la stimulation de l'innovation et de la compétitivité apporteraient des avantages considérables au grand public, aux pouvoirs publics et aux entreprises, ce qui devrait largement compenser les dépenses initiales sur le long terme.

En réduisant la fragmentation du marché et en harmonisant les exigences réglementaires, les options privilégiées renforcent l'égalité concurrentielle dans l'ensemble de l'Union, en offrant aux entreprises des trajectoires plus claires en matière de conformité et d'innovation.

Les options privilégiées contribueraient également à la simplification grâce à des orientations claires et à des systèmes intégrés, en réduisant ainsi les charges administratives. Les options respectent le principe «un ajout, un retrait» en veillant à ce que les nouvelles obligations soient contrebalancées par des réductions dans d'autres domaines.

- **Réglementation affûtée et simplification**

La révision du règlement sur la cybersécurité, au moyen des options stratégiques A.2, B.2, C.2 et D.3 retenues, contribue fortement à améliorer la clarté, à supprimer les inefficacités et à harmoniser les procédures des différents cadres juridiques. Plus concrètement, l'option A.2 propose une réforme complète du mandat de l'ENISA, soutenant efficacement la mise en œuvre des politiques et la coopération opérationnelle entre les États membres. Cette consolidation contribuera également à éliminer les pratiques fragmentées, en améliorant la coordination tout en réduisant les coûts de mise en conformité et les coûts opérationnels à long terme. L'option B.2, qui consiste à abroger l'actuel règlement sur la cybersécurité et à

introduire un ECCF réformé, accroît l'efficacité en révisant le modèle de gouvernance et en favorisant des procédures de certification plus prévisibles, plus cohérentes et plus souples. Cela permettra d'adopter plus rapidement les schémas et d'assurer un meilleur alignement sur la législation transversale, ce qui réduira la fragmentation réglementaire et allégera la charge pesant sur les parties prenantes tant publiques que privées. L'option C.2 réduit les coûts de mise en conformité pour les entités soumises à la législation pertinente de l'Union en matière de cybersécurité en modifiant le champ d'application et en permettant la mise en place de schémas de certification de cybersécurité organisationnels pour les entités relevant du champ d'application de la directive SRI 2 et d'autres actes juridiques. Cette approche simplifiera considérablement les obligations réglementaires pour les entités soumises à de multiples exigences et garantira une utilisation plus efficace des ressources entre les autorités nationales. L'option D.3 crée un cadre harmonisé pour faire face aux risques non techniques pesant sur les chaînes d'approvisionnement des TIC, en réduisant ainsi la fragmentation actuelle des approches entre les États membres. Ensemble, ces options représentent une simplification et une modernisation substantielles du cadre juridique de l'Union en matière de cybersécurité, qui alignent pleinement celui-ci sur les principes du programme REFIT de clarté, d'efficacité et de préparation au numérique.

La proposition satisfait à l'évaluation sous l'angle numérique («digital check»), étant donné que l'accent mis sur des processus numériques rationalisés témoigne de l'engagement de l'Union en faveur d'une approche consistant à donner la priorité au numérique, garantissant un échange de données et une prise de décision plus rapides et plus fiables. L'option D.3 pourrait également avoir une forte incidence sur la numérisation, car elle impliquerait le remplacement de composants provenant d'entités établies dans des pays tiers ou contrôlées par des entités de pays tiers suscitant des préoccupations en matière de cybersécurité (fournisseurs à haut risque).

- **Droits fondamentaux**

La proposition législative a été évaluée au regard de son potentiel à renforcer ou à mettre en péril les droits fondamentaux et à promouvoir l'égalité et la confiance, en accordant une attention particulière aux incidences sociétales et aux droits, y compris la protection de la vie privée, la protection des données et la capacité des personnes à comprendre, à exercer et à faire respecter leurs droits.

L'extension du mandat de l'ENISA contribuera à accroître la cyberrésilience dans l'ensemble de l'économie et dans la société en général, ce qui conduira à une meilleure protection de la vie privée et des données à caractère personnel des individus. La proposition soutiendra également l'éducation et la formation en matière de cybersécurité, en clarifiant le rôle de l'ENISA dans le développement des compétences au sein de la main-d'œuvre dans le domaine de la cybersécurité.

En outre, l'ECCF renforcera la confiance du grand public et des entreprises de l'Union dans les solutions TIC certifiées qui facilitent la vie quotidienne. La mise en place de schémas supplémentaires accroîtrait cet effet.

La proposition contribue à renforcer la confiance des citoyens en incitant les entités des secteurs critiques à obtenir une certification de cybersécurité et à démontrer ainsi publiquement leur niveau élevé de cybersécurité. En outre, en garantissant un signalement harmonisé des incidents liés aux rançongiciels et en prenant des mesures pour la transition vers la cryptographie post-quantique, elle renforcerait la confiance du public dans la protection des données sensibles dans les secteurs critiques.

Les dispositions relatives à la sécurité de la chaîne d'approvisionnement auront une certaine incidence sur la protection des droits fondamentaux en limitant les ingérences étrangères. Des activités telles que l'espionnage et la surveillance portent gravement atteinte aux droits fondamentaux des citoyens. Ce cadre horizontal pourrait améliorer la confiance, la sécurité et le respect de la vie privée dans diverses technologies et solutions numériques.

4. INCIDENCE BUDGÉTAIRE

Le budget estimé de l'Agence de l'Union européenne pour la cybersécurité (ENISA), qui contribuera à un renforcement significatif de la sécurité de l'Union, a été estimé à 341 millions d'euros pour sept ans, soit un budget annuel moyen de 49 millions d'euros (projection pour la période 2028-2034). Cela représente une augmentation de 81,5 % du budget de l'Agence en 2025. Les bénéfices générés par l'initiative proposée, tels qu'analysés dans l'analyse d'impact, seront considérables, avec jusqu'à 14,6 milliards d'euros d'économies pour les entreprises. En outre, si l'ampleur des économies de coûts potentielles liées à l'amélioration globale de la préparation de l'Union aux incidents de cybersécurité est par nature difficile à quantifier, on estime que les économies de coûts liées à une réaction plus rapide et au ralentissement de la prolifération des incidents de cybersécurité pourraient se chiffrer entre 3,7 et 4,4 milliards d'euros sur cinq ans. Dans le contexte des initiatives stratégiques à venir, la Commission examinera la répartition globale des ressources pour et au sein des institutions, organes et organismes européens dans le domaine de la cybersécurité afin de tirer parti des connaissances et de l'expertise, ainsi que de recenser et de développer des synergies.
Les ressources supplémentaires proposées pour renforcer l'Agence se traduisent par 118 ETP et par des coûts opérationnels supplémentaires qui couvriront les conventions de contribution actuelles entre l'ENISA et la Commission, telles que la maintenance de la plateforme unique de signalement; les ETP travaillant sur le fonctionnement et l'administration de la réserve de cybersécurité de l'Union, ainsi que d'importantes initiatives de la Commission telles que la création du point d'entrée unique dans le cadre de la proposition «omnibus numérique». D'autres coûts opérationnels sont liés au programme coordonné de divulgation des vulnérabilités, à la collecte et à l'analyse de renseignements sur les menaces de cybersécurité, aux communications sécurisées et au renforcement de la maturité de l'ENISA en matière de cybersécurité. Les coûts opérationnels liés à la maintenance des schémas européens de certifications de cybersécurité, des autorisations de compétences en matière de cybersécurité et du service d'outils de test sont également ajoutés à ce budget, mais ces coûts comprennent également des mécanismes qui s'autofinanceront au moyen de redevances.

Un aspect important de la proposition est l'introduction de mécanismes de redevances qui, entre autres objectifs stratégiques, contribueront également à un circuit financier durable au sein de l'Agence. Le règlement sur la cybersécurité révisé présente trois types de redevances qui contribueront au budget de l'ENISA, à savoir des redevances provenant de la délivrance d'agréments pour les attestations de compétences, des redevances provenant du service d'outils de test et des redevances provenant du soutien de la maintenance des schémas européens de certification de cybersécurité. Le bénéfice escompté pour le budget de l'Union est estimé à environ 18,5 millions d'euros sur une période de sept ans, de 2028 à 2034.

La demande budgétaire de la Commission se traduit par 50 postes ETP supplémentaires, qui mettront en œuvre le cadre pour le fonctionnement de la chaîne d'approvisionnement, ainsi que les tâches liées à l'élaboration d'actes d'exécution pour les mécanismes de redevances, à la maintenance des schémas de certification, à la normalisation et au soutien à la coopération opérationnelle, entre autres. Le coût pour la Commission de la mise en œuvre du cadre pour le

fonctionnement de la chaîne d'approvisionnement devrait être spécifiquement influencé par le nombre d'évaluations du contrôle de la propriété (ECP) que la Commission réalisera. Les résultats de cette tâche contribueront toutefois grandement à permettre aux États membres de réaliser des économies lorsqu'ils superviseront la mise en œuvre des mesures et obligations d'atténuation imposées par le cadre aux entités relevant de la directive SRI 2. Les États membres seront en mesure de tirer directement parti des résultats des ECP, plutôt que de dépenser chacun individuellement des ressources pour répondre aux mêmes besoins d'évaluation.

Voir la fiche financière accompagnant le paquet législatif sur la cybersécurité pour de plus amples informations.

5. AUTRES ÉLÉMENTS

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

La Commission surveillera l'application du règlement proposé et soumettra tous les cinq ans au Parlement européen et au Conseil un rapport sur son évaluation. Ces rapports seront publiés et décriront en détail comment le règlement proposé est appliqué et exécuté dans les faits.

- **Documents explicatifs (pour les directives)**

Sans objet car la proposition est un règlement.

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

La proposition clarifie le rôle de l'ENISA et lui confie des tâches concrètes pour soutenir ses parties prenantes, au premier rang desquelles figurent les États membres, en particulier en ce qui concerne le soutien à la mise en œuvre de la politique et de la législation de l'Union, la coopération opérationnelle, le renforcement des capacités, la certification de cybersécurité et la normalisation et l'amélioration de la main-d'œuvre dans le domaine de la cybersécurité et de sa mobilité dans l'ensemble de l'Union. La proposition vise en outre à rendre le cadre européen de certification de cybersécurité (ECCF) plus efficace et efficient afin d'améliorer le niveau de cybersécurité au sein de l'Union et de donner aux clients les moyens de faire des choix éclairés lors de l'acquisition de produits TIC, de services TIC, de processus TIC et de services de sécurité gérés dans l'ensemble du marché intérieur. En outre, en combinaison avec la proposition de directive introduisant des modifications ciblées de la directive SRI 2, la présente proposition vise à faciliter le respect des obligations en matière de cybersécurité et à débloquer des ressources pour renforcer la préparation opérationnelle des entités dans les secteurs critiques de l'Union en matière de cybersécurité. Enfin, la proposition répond à la nécessité de rendre l'économie et la chaîne d'approvisionnement des TIC de l'Union plus résilientes afin de promouvoir la sécurité et la compétitivité de l'Union. Les détails sont fournis ci-dessous.

TITRE I: DISPOSITIONS GENERALES

Le titre I du règlement proposé contient les dispositions générales: l'objet (article 1er) et les définitions (article 2), y compris les références aux définitions applicables tirées d'autres

instruments de l'Union, comme la directive (UE) 2022/2555[21] (directive SRI 2), le règlement (CE) nº 765/2008[22] et le règlement (UE) nº 1025/2012[23].

TITRE II: ENISA (L'AGENCE DE L'UNION EUROPÉENNE POUR LA CYBERSÉCURITÉ)

Le titre II de la proposition de règlement contient les principales dispositions relatives à l'ENISA.

Le chapitre I décrit la mission (article 3) et les objectifs de l'ENISA (article 4).

Le chapitre II décrit les tâches de l'Agence en trois sections.

La section 1 comprend des dispositions concernant les tâches liées au soutien à la mise en œuvre de la politique et du droit de l'Union. Elle précise quelles entités et organisations doivent recevoir un soutien et la manière dont ce soutien devrait leur être fourni (article 5). L'article 6 définit les responsabilités de l'Agence en matière de renforcement des capacités, qui consistent notamment à offrir aux États membres des connaissances et une expertise en matière de prévention et de lutte contre les cybermenaces, à actualiser les stratégies de cybersécurité et à accroître la main-d'œuvre dans le domaine de la cybersécurité. L'ENISA assistera également les États membres dans leurs activités de sensibilisation (article 7), analysera les principales tendances du marché en matière de cybersécurité et diffusera des conseils et des analyses techniques (article 8). L'ENISA contribuera également à la coopération internationale sur les questions de cybersécurité décrite à l'article 9 et l'encouragera.

La section 2 définit les tâches de l'ENISA en ce qui concerne la coopération opérationnelle avec les États membres, les entités de l'Union et le CERT-UE, le réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT), EU-CyCLONe et d'autres parties prenantes, y compris la publication de lignes directrices et la mise en œuvre d'outils de communication sécurisés (article 10). L'ENISA contribuera également à améliorer la conscience situationnelle concernant les cybermenaces et les incidents en créant (entre autres) un ou plusieurs répertoires de renseignements sur les cybermenaces, en procédant à des analyses et en émettant des alertes précoces (article 11). Les règles relatives à ces alertes précoces (contenu, délais, service) sont énoncées à l'article 12. Afin d'aider les entités essentielles et importantes à se préparer aux incidents liés aux rançongiciels, à y réagir et à s'en remettre, l'ENISA gère la réserve de cybersécurité de l'Union comme expliqué à l'article 13 et en coopération avec Europol et les CSIRT ou d'autres autorités compétentes, selon le cas. L'article 14 comprend des dispositions sur le rôle de l'ENISA dans les exercices de cybersécurité au niveau de l'Union, y compris l'élaboration d'un programme annuel continu d'exercices de cybersécurité au niveau de l'Union. Outre ces tâches, l'ENISA devrait fournir des outils et des plateformes, en particulier la plateforme unique de signalement établie en vertu de l'article 16, paragraphe 1, du règlement (UE) 2024/2847 (article 15). Enfin, l'Agence doit développer une capacité commune de services de gestion des vulnérabilités au niveau de l'Union et fournir des services de gestion des vulnérabilités (article 16).

[21] http://data.europa.eu/eli/dir/2022/2555/oj
[22] http://data.europa.eu/eli/reg/2008/765/oj
[23] http://data.europa.eu/eli/reg/2012/1025/oj

La section 3 sur la certification de cybersécurité et la normalisation définit les tâches de l'Agence à cet égard. L'article 17 décrit le rôle de l'ENISA dans l'élaboration et la mise en œuvre de l'ECCF, y compris son rôle de premier plan dans la préparation des schémas et dans la garantie de leur maintenance et du renforcement de leurs capacités, tandis que l'article 18 définit la manière dont l'ENISA devrait participer à l'élaboration de spécifications techniques et contribuer aux activités de normalisation aux niveaux européen et international, y compris dans le domaine des algorithmes cryptographiques.

La section 4 détaille les tâches de l'Agence en ce qui concerne la mise en œuvre de l'académie des compétences en matière de cybersécurité. L'article 19 comprend des dispositions relatives au rôle joué par l'ENISA en ce qui concerne le cadre européen de compétences en matière de cybersécurité (ECSF), tandis que ses tâches relatives à l'élaboration et à la maintenance de programmes d'attestation individuelle européenne des compétences en matière de cybersécurité sont énoncées à l'article 20. Les exigences à satisfaire pour devenir un fournisseur d'attestations agréé sont énoncées à l'article 21 et celles relatives au traitement des demandes à l'article 22. L'ENISA doit fournir au public des informations sur l'ECSF et les attestations individuelles de compétences en matière de cybersécurité (article 23).

Le chapitre III concerne l'organisation de l'ENISA. La structure administrative et de gestion de l'Agence comprend également un directeur exécutif adjoint (article 24). Les dispositions relatives au conseil d'administration, à sa composition, à son président, à ses réunions, à ses fonctions et à ses règles de vote figurent à la section 1 (article 25 à 29). Le conseil exécutif doit assister le conseil d'administration conformément à l'article 30, dans la section 2. La section 3 comprend des règles relatives à la nomination, à la révocation et à la prolongation du mandat du directeur exécutif (article 31) et des règles relatives aux tâches et responsabilités du directeur exécutif (article 32). Le conseil d'administration peut décider de créer un poste de directeur exécutif adjoint chargé d'assister le directeur exécutif (section 4, articles 33 et 34). Le conseil d'administration doit mettre en place le groupe consultatif de l'ENISA, qui doit conseiller l'ENISA conformément aux règles énoncées à l'article 35. La section 6 énonce les règles relatives à la création et à la composition de la commission de recours (article 36) et à ses membres (article 37). L'article 38 précise les circonstances dans lesquelles les membres de la commission de recours doivent s'abstenir de participer à une procédure de recours et expose les motifs de récusation d'un membre de la chambre. Des recours peuvent être formés devant la commission de recours contre des décisions prises par l'ENISA ou lorsque cette dernière s'abstient d'agir (article 39). L'article 40 contient des dispositions relatives aux personnes habilitées à former un recours, aux délais et à la forme du recours. Les articles 41 à 43 énoncent les règles relatives à la révision préjudicielle, à l'examen des décisions relatives aux recours et aux recours devant la Cour de justice. Enfin, l'article 44 établit le processus relatif au document unique de programmation.

Le chapitre IV concerne l'établissement et la structure du budget de l'Agence ainsi que les règles régissant sa présentation et sa mise en œuvre (articles 45 à 55). Il comprend aussi les dispositions visant à faciliter la lutte contre la fraude, la corruption et les autres activités illicites (article 51).

Le chapitre V porte sur la dotation en personnel de l'Agence. Il comprend des dispositions générales sur le statut et le régime applicable au personnel, et des règles régissant les privilèges et immunités (articles 56 et 57). Il introduit des dispositions imposant aux États membres de désigner des officiers de liaison en tant qu'experts nationaux détachés auprès de l'ENISA et définissant leur rôle au sein de l'Agence (article 58). Il contient également des

dispositions orientant le recours à des experts nationaux détachés et à d'autres personnes non employées par l'Agence (article 59).

En dernier lieu, le chapitre VI contient les dispositions générales relatives à l'Agence. Il décrit son statut juridique (article 60), fixe son siège (article 61) et contient des dispositions relatives à son accord de siège et à ses conditions de fonctionnement, ainsi qu'au contrôle administratif exercé par le médiateur (articles 62 et 63). Il comprend des dispositions régissant les questions de responsabilité, de régime linguistique et de protection des données à caractère personnel (article 64 à 66), ainsi que des règles de sécurité en matière de protection des informations sensibles non classifiées et des informations classifiées (article 67). Il prévoit des règles pour la coopération avec les entités de l'Union et les autorités nationales (article 68) et d'autres parties prenantes (article 69). Il décrit les règles régissant la coopération de l'Agence avec des pays tiers et les organisations internationales (article 70).

TITRE III: CADRE EUROPÉEN DE CERTIFICATION DE CYBERSÉCURITÉ

Le titre III du règlement proposé établit l'ECCF.

Le chapitre I présente les objectifs, le champ d'application et les procédures du cadre. Les objectifs (article 71) consistent notamment à renforcer la cybersécurité dans l'ensemble de l'Union et à faciliter une approche harmonisée de la certification des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou de la posture de cybersécurité des entités. Le cadre devrait également tirer parti de la certification pour simplifier le respect de la législation applicable de l'Union grâce à la présomption de conformité, en réduisant ainsi la charge pesant sur les entreprises (article 78). Le chapitre I détaille ensuite les aspects procéduraux, en commençant par les consultations sur les priorités stratégiques européennes en matière de certification de cybersécurité et les informations publiques relatives à l'élaboration de schémas par la Commission et sur la création d'une nouvelle assemblée européenne de certification de cybersécurité (article 72). À la suite d'une demande détaillée de la Commission (article 73), l'ENISA devrait fournir un schéma candidat dans un délai de 12 mois. L'article 74 prévoit des délais supplémentaires en ce qui concerne la présentation de l'avis du GECC et la soumission du schéma en vue de son adoption par la Commission. L'article 75 introduit un mécanisme de maintenance clair pour les schémas existants, qui pourrait conduire à la révision de ces schémas (article 76). Le réexamen d'un schéma pourrait également s'appuyer sur une évaluation périodique de son efficacité et de son incidence sur le marché unique. L'article 77 fournit à l'ENISA une base pour l'élaboration de spécifications techniques à l'appui du développement et de la maintenance des schémas européens de certification de cybersécurité. Lors de l'adoption ou de la révision d'un schéma, la Commission peut inclure des références à ces spécifications techniques (article 74). Les différentes procédures garantissent la transparence et la qualité de la mise en œuvre en associant des experts et des parties prenantes générales à différents stades de la planification, de l'élaboration, de l'adoption et de la maintenance des schémas de certification. L'article 79 prévoit un site web spécifique de l'ENISA sur les schémas européens de certification de cybersécurité, qui devrait fournir des informations sur les schémas adoptés ainsi que sur les certificats de cybersécurité européens et les déclarations de conformité de l'Union délivrés au titre de ces schémas.

Le chapitre II prévoit des règles générales pour le contenu des schémas européens de certification de cybersécurité.

L'article 80 établit une liste d'objectifs de sécurité que l'ENISA doit prendre en considération lors de la conception d'un schéma et garantit l'alignement sur la législation pertinente en matière de cybersécurité. Chaque schéma européen de certification de cybersécurité peut prévoir des éléments précisés à l'article 81. Ces éléments doivent être compatibles avec la législation de l'Union et peuvent être harmonisés entre les schémas au moyen de dispositions types. Ces deux dispositions offrent la souplesse nécessaire pour s'adapter aux différents types de schémas. Des dispositions supplémentaires précisent les règles relatives aux niveaux d'assurance (article 82) et à l'autoévaluation de la conformité (article 83). Le chapitre établit en outre une liste d'informations supplémentaires (article 84) que le fabricant ou le fournisseur de produits TIC, de services TIC ou de processus TIC doit mettre à disposition.

Enfin, le chapitre III établit les règles de gouvernance de l'ECCF, réparties en trois sections.

La section 1 concerne les règles relatives à la délivrance de certificats de cybersécurité européens, y compris ceux correspondant au niveau d'assurance «élevé» (article 85). Elle établit également des règles visant à harmoniser les schémas européens de certification de cybersécurité avec les schémas nationaux de certification de cybersécurité et les certificats de cybersécurité (article 86) et prévoit la possibilité d'une reconnaissance internationale des certificats de cybersécurité européens, sur la base du principe d'équivalence (article 87). Cette section décrit également le rôle des autorités nationales de certification de cybersécurité et les règles applicables à celles-ci (article 88) et établit des règles pour un mécanisme d'examen par les pairs entre ces autorités, garantissant des normes équivalentes dans l'ensemble de l'Union (article 89), et pour la coopération entre ces autorités au sein du GECC (article 90).

La section 2 prévoit: i) des règles harmonisées concernant l'accréditation et l'autorisation des organismes d'évaluation de la conformité (articles 91 et 92); ii) des règles de notification, y compris une habilitation visant à poursuivre l'alignement sur le droit pertinent de l'Union et le nouveau cadre législatif (NCL) (article 93); et iii) une procédure de contestation (article 94) garantissant le respect des exigences applicables aux organismes d'évaluation de la conformité.

Enfin, la section 3 prévoit des droits et des recours juridictionnels contre les décisions relatives à la certification (article 96) et impose aux États membres de prévoir et d'appliquer des sanctions proportionnées en cas d'infractions réglementaires.

TITRE IV

Le chapitre I, article 98, définit le champ d'application du cadre de confiance pour la chaîne d'approvisionnement des TIC. Ce cadre abordera les risques non techniques dans les secteurs hautement critiques et dans d'autres secteurs critiques visés dans la directive (UE) 2022/2555. Le mécanisme identifie les actifs de TIC essentiels dans les chaînes d'approvisionnement critiques des TIC et définit des mesures d'atténuation appropriées et proportionnées pour les types d'entités visés aux annexes I et II de la directive (UE) 2022/2555. Le cadre sera fondé sur des évaluations coordonnées au niveau de l'Union des risques pour la sécurité, demandées par la Commission ou par au moins trois États membres. L'article 99 expose en détail la manière dont ces évaluations des risques seront réalisées et précise qu'elles devraient également établir des mesures d'atténuation. Ces évaluations des risques devraient être finalisées dans un délai de six mois à compter de la demande. À la demande de la Commission, le groupe de coopération SRI peut convenir d'un délai plus court. Le cadre prévoit la possibilité d'une procédure d'urgence si une intervention immédiate est justifiée pour préserver le bon fonctionnement du marché intérieur et lorsque la Commission a des

raisons suffisantes de considérer qu'il existe une cybermenace importante pour la sécurité de l'Union en ce qui concerne les chaînes d'approvisionnement critiques des TIC. Dans ce cas, la Commission consulte les États membres sur la nécessité de prendre une ou plusieurs mesures d'atténuation et procède à une évaluation des risques. L'article 100 prévoit que lorsque, à la suite de l'évaluation des risques visée à l'article 99, ou sur la base d'autres sources, telles qu'une déclaration publique au nom de l'Union ou d'un État membre, il apparaît qu'un pays tiers présente des risques non techniques graves et structurels pour les chaînes d'approvisionnement des TIC, la Commission vérifie la menace posée par ce pays, en tenant compte des éléments énumérés à l'article 100. Lorsque la Commission conclut qu'un pays tiers présente des risques non techniques graves et structurels pour les chaînes d'approvisionnement des TIC, l'article 100 prévoit une procédure qui lui permet de désigner ce pays tiers comme un pays suscitant des préoccupations en matière de cybersécurité pour les chaînes d'approvisionnement des TIC. Les entités établies dans un pays tiers suscitant des préoccupations de cybersécurité et désigné comme tel conformément à cet article, ou qui sont contrôlées par un tel pays tiers, par une entité établie dans un tel pays tiers ou par un ressortissant d'un tel pays tiers ne seront pas autorisées à exercer un certain nombre d'activités spécifiées dans cet article. L'article 101 prévoit un mécanisme général pour les chaînes d'approvisionnement des TIC dans le cadre duquel, à l'issue de l'évaluation des risques pour la sécurité effectuée par le groupe de coopération SRI ou par la Commission conformément à l'article 99, la Commission peut prendre les mesures prévues aux articles 102 et 103.

La Commission peut identifier, au moyen d'actes d'exécution, les actifs de TIC essentiels utilisés pour la fabrication de produits et la fourniture de services par les types d'entités visés aux annexes I et II de la directive (UE) 2022/2555. L'article 102 décrit plus en détail les éléments à prendre en considération pour l'identification des actifs de TIC essentiels. L'article 103 établit des mesures d'atténuation potentielles dans les chaînes d'approvisionnement des TIC. La Commission peut, au moyen d'actes d'exécution, décider que les entités opérant dans des secteurs hautement critiques et d'autres secteurs critiques doivent faire l'objet de mesures d'atténuation spécifiques, décrites plus en détail dans cet article.

La Commission établit, par voie d'actes d'exécution, des listes des fournisseurs à haut risque concernés par les interdictions énoncées dans les actes d'exécution adoptés conformément à l'article 103, paragraphe 1 ou à l'article 103, paragraphe 7, ou par l'interdiction visée à l'article 110, paragraphe 1, après avoir procédé à une évaluation de l'établissement et de la propriété et du contrôle. Elle devrait consulter les fournisseurs concernés et les autorités compétentes (article 104).

Une entité qui est établie dans un pays tiers suscitant des préoccupations en matière de cybersécurité désigné en tant que tel conformément à l'article 100 ou qui est contrôlée par une entité provenant d'un tel pays tiers peut demander à être autorisée à fournir des composants TIC dans des actifs de TIC essentiels d'entités du type visé aux annexes I et II de la directive (UE) 2022/2555 et à participer à des marchés publics concernant la fourniture de ces composants TIC. L'article 105 précise ce que cette demande doit contenir et quelle est la procédure à suivre pour obtenir une telle exemption. L'article 106 précise les droits de la défense d'une entité se trouvant dans une telle situation. La Commission tient un registre accessible au public reprenant les décisions relatives aux dérogations (article 107). Les articles 108 et 109 précisent les règles de confidentialité et les redevances applicables à la procédure d'exemption.

Le chapitre II prévoit l'application du cadre de confiance pour la chaîne d'approvisionnement des TIC aux réseaux de communications électroniques mobiles, fixes et par satellite, en garantissant ainsi l'alignement sur la proposition de règlement sur les réseaux numériques.

Les actifs de TIC essentiels pour les réseaux de communications électroniques mobiles, fixes et par satellite sont définis à l'annexe II. La période de transition pour l'élimination progressive des composants TIC des fournisseurs à haut risque pour les actifs de TIC essentiels du réseau de communications électroniques mobiles ne dépasse pas 36 mois à compter de l'entrée en vigueur du présent règlement. Les périodes de transition prévues pour les réseaux de communications électroniques fixes et par satellite sont précisées par la Commission par voie d'actes d'exécution. La Commission est habilitée à adopter des actes délégués afin de modifier les actifs de TIC essentiels désignés et les périodes de transition, y compris pour les futures générations mobiles (article 110). L'article 111 dispose que les fournisseurs de réseaux de communications électroniques mobiles, fixes et par satellite ne peuvent pas utiliser, installer ou intégrer, sous quelque forme que ce soit, des composants TIC provenant de fournisseurs à haut risque et ne peuvent pas obtenir d'autorisation générale ou individuelle.

Autorités compétentes, surveillance et exécution, compétence, droits de la défense (chapitre III)

Le chapitre III établit en outre les règles relatives aux autorités compétentes, à la surveillance, à l'exécution et à la compétence.

Les articles 112 à 114 précisent les pouvoirs, moyens et responsabilités des États membres pour assurer la mise en œuvre et l'application des dispositions du titre IV. Les États membres doivent désigner une ou plusieurs autorités compétentes, qui doivent être notifiées à la Commission. L'article 113 prévoit que la Commission met en place un réseau de coopération entre les autorités compétentes des États membres et la Commission afin de faciliter le respect des règles, tandis que l'article 114 précise les mesures de supervision et d'exécution que les autorités compétentes sont habilitées à prendre. Les sanctions en cas de violation des dispositions du titre IV sont précisées à l'article 115. L'article 116 expose en détail la possibilité pour les États membres de se prêter mutuellement assistance lorsque des entités exercent des activités transfrontières ou lorsque leurs actifs de TIC essentiels sont situés dans plusieurs États membres. L'article 117 établit les règles de compétence et de territorialité.

TITRE VI: DISPOSITIONS FINALES

Le titre VI de la proposition de règlement comprend les dispositions finales, qui définissent les règles applicables concernant l'adoption des actes d'exécution et des actes délégués, le processus d'évaluation du règlement proposé ainsi que l'abrogation et la succession du règlement (UE) 2019/881. Il fixe également la date d'entrée en vigueur du règlement proposé.

2026/0011 (COD)

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)

(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[24],

vu l'avis du Comité des régions[25],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Depuis l'adoption du règlement (UE) 2019/881 du Parlement européen et du Conseil[26], les paysages géopolitique, technologique et politique ont subi d'importantes transformations. Les incidents de cybersécurité, qu'ils soient causés par des défaillances du système, des erreurs humaines, des actes malveillants ou des phénomènes naturels, se sont multipliés et les cyberattaques sont devenues plus sophistiquées, touchant des entités essentielles, des entreprises et le grand public. L'écosystème de la cybercriminalité s'est développé, centré sur l'activité des rançongiciels. Les incidents touchant les chaînes d'approvisionnement, qu'ils soient causés par des criminels mus par la recherche d'un gain financier ou par des acteurs étatiques à des fins de perturbation, d'espionnage, de désinformation ou de guerre, se sont intensifiés. Dans le cadre d'une stratégie hybride plus large, les incidents résultant d'actes de cybermalveillance et de défaillances de systèmes ont des répercussions qui se propagent, en perturbant les services essentiels, en sapant la confiance dans les institutions et en affectant la préparation de la société et de la défense de l'Union. Ces incidents ont, en ce qui concerne les conséquences sur l'activité économique, la stabilité financière et la vie des citoyens, un potentiel qui n'est plus à démontrer. Dans

[24] JO C , , p. .

[25] JO C , , p. .

[26] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

le même temps, la vulnérabilité des infrastructures et systèmes civils critiques engendre des risques pour les capacités de défense lorsque celles-ci dépendent de tels infrastructures et systèmes.

(2) Parallèlement, les technologies émergentes telles que l'intelligence artificielle et l'informatique quantique ont un effet perturbateur sur la cybersécurité et la cyberdéfense. Elles remodèlent les outils de défense et les tactiques des adversaires, en compromettant ainsi la cybersécurité et la cyberdéfense, mais offrent en même temps des possibilités de progrès technologiques. Bien qu'elles puissent contribuer à la cybersécurité en renforçant la détection des menaces ou la réaction automatisée aux incidents, elles augmentent également la surface d'attaque globale pour les organisations, sont des cibles potentielles de manipulation et peuvent compromettre la viabilité à long terme des mesures de sécurité telles que le chiffrement.

(3) Pour faire face à ces évolutions, l'Union a renforcé ses outils juridiques et stratégiques. La directive (UE) 2022/2555 du Parlement européen et du Conseil[27] renforce la cybersécurité des infrastructures critiques; elle est complétée, pour la sécurité physique, par la directive (UE) 2022/2557 du Parlement européen et du Conseil[28]. Le règlement (UE) 2024/2847 du Parlement européen et du Conseil[29] renforce la cybersécurité des produits comportant des éléments numériques. Le règlement (UE) 2025/38 du Parlement européen et du Conseil[30] renforce les capacités de réaction à l'échelle de l'Union et la recommandation du Conseil du 6 juin 2025 sur un schéma directeur de l'UE pour la gestion des crises de cybersécurité[31] (ci-après la «recommandation relative au schéma directeur de l'UE en matière de cybersécurité») soutient la coopération au niveau de l'Union en matière de gestion des crises. La boîte à outils sur la cybersécurité des réseaux 5G[32] constitue une première étape vers une approche coordonnée au niveau de l'Union pour sécuriser les réseaux 5G. La communication de la Commission sur l'académie des compétences en matière de cybersécurité[33] répond au défi croissant que constitue la pénurie de talents dans le

---

27 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).

28 Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

29 Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) no 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

30 Règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (règlement sur la cybersolidarité) (JO L, 2025/38, 15.01.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

31 JO C, C/2025/3445, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj.

32 Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures, NIS Cooperation Group, 1/2020, disponible à l'adresse suivante: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

33 Communication de la Commission au Parlement européen et au Conseil, Remédier à la pénurie de talents dans le secteur de la cybersécurité pour renforcer la compétitivité, la croissance et la résilience

secteur de la cybersécurité. Le cadre en matière de cybersécurité a également été renforcé par la législation sectorielle, en particulier par le règlement (UE) 2022/2554 du Parlement européen et du Conseil[34] pour le secteur financier, le règlement délégué (UE) 2024/1366 de la Commission[35] pour le sous-secteur de l'électricité, le règlement délégué (UE) 2022/1645 de la Commission[36] et le règlement d'exécution (UE) 2023/203 de la Commission (PARTIE-IS)[37] ainsi que par les règles de sûreté de l'aviation pertinentes énoncées dans le règlement (UE) 2019/1583 de la Commission[38] pour le sous-secteur du transport aérien et d'autres documents stratégiques tels que la communication de la Commission relative à un plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé[39]. Les entités de l'Union sont également renforcées par le règlement (UE, Euratom) 2023/2841 du Parlement européen et du Conseil[40], qui établit des mesures visant à atteindre un niveau commun élevé de cybersécurité au sein des institutions, organes et organismes de l'Union. Ce cadre juridique renforcé en matière de cybersécurité a précisé davantage les tâches de l'ENISA.

---

de l'UE («L'académie des compétences en matière de cybersécurité»), COM(2023) 207 final, 18 avril 2023.

34 Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

35 Règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil en établissant un code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité (JO L, 2024/1366, 24.05.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

36 Règlement délégué (UE) 2022/1645 de la Commission du 14 juillet 2022 portant modalités d'application du règlement (UE) 2018/1139 du Parlement européen et du Conseil en ce qui concerne les exigences relatives à la gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne imposées aux organismes relevant des règlements (UE) nº 748/2012 et (UE) nº 139/2014 de la Commission et modifiant les règlements (UE) nº 748/2012 et (UE) nº 139/2014 de la Commission (JO L 248 du 26.9.2022, p. 18, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj).

37 Règlement d'exécution (UE) 2023/203 de la Commission du 27 octobre 2022 portant modalités d'application du règlement (UE) 2018/1139 du Parlement européen et du Conseil en ce qui concerne les exigences en matière de gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne pour les organismes relevant des règlements (UE) nº 1321/2014, (UE) nº 965/2012, (UE) nº 1178/2011 et (UE) 2015/340 de la Commission, des règlements d'exécution (UE) 2017/373 et (UE) 2021/664 de la Commission, et pour les autorités compétentes relevant des règlements (UE) nº 748/2012, (UE) nº 1321/2014, (UE) nº 965/2012, (UE) nº 1178/2011, (UE) 2015/340 et (UE) nº 139/2014 de la Commission, des règlements d'exécution (UE) 2017/373 et (UE) 2021/664 de la Commission, et modifiant les règlements (UE) nº 1178/2011, (UE) nº 748/2012, (UE) nº 965/2012, (UE) nº 139/2014, (UE) nº 1321/2014 et (UE) 2015/340 de la Commission, et les règlements d'exécution (UE) 2017/373 et (UE) 2021/664 de la Commission (JO L 31 du 2.2.2023, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj).

38 Règlement d'exécution (UE) 2019/1583 de la Commission du 25 septembre 2019 modifiant le règlement d'exécution (UE) 2015/1998 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, en ce qui concerne les mesures de cybersécurité (JO L 246 du 26.9.2019, p. 15, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj).

39 Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions, Plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé, COM(2025) 10 final du 15 janvier 2025.

40 Règlement (UE/Euratom) 2023/2841 du Parlement européen et du Conseil du 13 décembre 2023 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union (JO L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

(4) Dans ce contexte, et comme indiqué dans la stratégie européenne de sécurité intérieure ProtectEU[41] et dans la stratégie européenne pour une union de la préparation[42], assurer la préparation, la sécurité et la résilience de la société et de l'économie de l'Union, nécessite une coordination, une confiance et un partage d'informations solides entre les parties prenantes européennes, des cadres robustes afin de garantir la sécurité des produits TIC, des services TIC, des processus TIC et des services de sécurité gérés, ainsi qu'un développement et un renforcement de la main-d'œuvre dans le domaine de la cybersécurité. Cela nécessite aussi un renforcement des chaînes d'approvisionnement des TIC en garantissant la souveraineté technologique européenne sur les actifs essentiels, ce qui accroîtrait la résilience de l'Union et pourrait être bénéfique pour les efforts de cyberdéfense. En outre, la communication intitulée «Renforcer la sécurité économique de l'UE»[43] définit comme objectifs prioritaires la nécessité d'empêcher tout accès à des informations et données sensibles susceptible de compromettre la sécurité économique de l'Union et de prévenir et d'atténuer les perturbations des infrastructures critiques de l'Union affectant l'économie de l'Union. Cette communication reconnaît le rôle essentiel que jouent à cet égard des mesures efficaces en matière de cybersécurité.

(5) Les incidents de cybersécurité majeurs qui touchent des infrastructures critiques, des services numériques ou des fonctions essentielles de la société peuvent avoir des répercussions sur la population nécessitant une action coordonnée de protection civile et de gestion de crise au niveau de l'Union. Conformément à l'approche «tous risques» de la stratégie européenne pour une union de la préparation et de la décision nº 1313/2013/UE relative au mécanisme de protection civile de l'Union, les dispositions relatives à la conscience situationnelle, à la réponse aux incidents et aux exercices au titre du présent règlement devraient alimenter la gestion des crises de l'Union, notamment par l'intermédiaire du centre de coordination de la réaction d'urgence (ERCC).

(6) La présente proposition est également cohérente et complémentaire par rapport à la [proposition de directive complétant [la révision du règlement (UE) 2019/881] et modifiant la directive (UE) 2022/2555 en ce qui concerne la simplification de la mise en œuvre des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union], ainsi que par rapport à la [proposition de règlement relatif à la simplification de la législation numérique (règlement omnibus sur le numérique)][44], qui prévoit l'obligation pour l'ENISA de mettre en place un guichet unique pour la notification des incidents par l'intermédiaire duquel les entités peuvent remplir simultanément leurs obligations de notification des incidents découlant de plusieurs actes juridiques.

---

41 Communication de la Commission au Parlement Européen, au Conseil, au Comité économique et Social Européen et au Comité des Régions, «ProtectEU: une stratégie européenne de sécurité intérieure», COM(2025) 148 final, 1er avril 2025.

42 Communication conjointe de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la stratégie européenne pour une union de la préparation, JOIN(2025) 130 final.

43 Communication conjointe de la Commission au Parlement européen et au Conseil, «Renforcer la sécurité économique de l'UE», JOIN(2025) 977 final.

44 COM/2025/837 final

(7) Le règlement (CE) nº 460/2004 du Parlement européen et du Conseil[45] a institué l'ENISA aux fins de contribuer à assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de l'Union et à favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des administrations publiques. Le mandat de l'ENISA a été prorogé à trois reprises avant de devenir permanent en vertu du règlement (UE) 2019/881. Afin de mieux répondre aux besoins créés par l'évolution du paysage des menaces et de la technologie, en particulier en ce qui concerne la coopération opérationnelle et le besoin accru de professionnels de la cybersécurité, il convient de renforcer encore le mandat de l'ENISA. Par souci de sécurité juridique, il convient de remplacer le règlement (UE) 2019/881.

(8) Dans un paysage de menaces en pleine évolution, où les incidents de cybersécurité prennent de plus en plus d'ampleur, il est plus important que jamais de susciter la confiance des particuliers, des pouvoirs publics et des entreprises dans leur utilisation quotidienne des technologies. Une certification renforcée de l'ECCF mise en œuvre à l'échelle de l'Union prévoyant des exigences et des critères d'évaluation communs en matière de cybersécurité dans l'ensemble des marchés nationaux et des secteurs peut faciliter le renforcement de la confiance. Le nouveau cadre devrait définir les principales exigences horizontales applicables aux schémas européens de certification de cybersécurité et permettre la reconnaissance et l'utilisation des certificats de cybersécurité européens et des déclarations de conformité de l'Union dans tous les États membres. Ce faisant, il devrait établir une procédure et un cadre de gouvernance permettant le développement et la maintenance en temps utile et prévisible des schémas européens de certification de cybersécurité. Les schémas européens de certification de cybersécurité devraient être appliqués de manière uniforme dans tous les États membres afin de garantir une mise en œuvre harmonisée des exigences en matière de cybersécurité, d'assurer des conditions de concurrence équitables et d'empêcher la pratique du «tourisme de la certification» en fonction des différents niveaux de rigueur appliqués dans les différents États membres. L'ENISA devrait jouer un rôle essentiel en prévoyant le développement des schémas au moyen de spécifications techniques et en veillant à ce que ces schémas restent techniquement à jour. En outre, afin de répondre efficacement aux besoins du marché, le cadre devrait prévoir la possibilité de certifier les mesures de gestion des risques de cybersécurité destinées aux entités et faciliter le respect d'autres actes législatifs applicables de l'Union dans le domaine de la cybersécurité. L'alignement sur le droit existant de l'Union, tel que le règlement (UE) 2024/2847 et la directive (UE) 2022/2555, est essentiel pour que les schémas européens de certification de cybersécurité contribuent à réduire la charge que représente la conformité pour les entreprises, à gagner en attractivité et à renforcer la cyberrésilience de l'Union.

(9) La mission de l'ENISA devrait être d'aider les États membres et les entités de l'Union à atteindre un niveau élevé de cybersécurité, de résilience et de confiance dans l'Union. À cette fin, l'ENISA devrait servir de point de référence pour obtenir des conseils et une expertise en matière de cybersécurité et ses travaux devraient principalement s'articuler autour de quatre domaines clés de la cybersécurité au niveau de l'Union. Premièrement, l'ENISA devrait aider les États membres à mettre en œuvre

[45] Règlement (CE) nº 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JO L 77 du 13.3.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/460/oj).

de manière cohérente la politique et la législation de l'Union en matière de cybersécurité et les aider, au moyen d'activités de renforcement des capacités, à améliorer en permanence leurs capacités en matière de préparation, de résilience et de réaction. Deuxièmement, l'ENISA devrait contribuer à la coopération opérationnelle au niveau de l'Union, entre les États membres, et à une meilleure conscience situationnelle commune en matière de cybermenaces et d'incidents entre les États membres et les entités de l'Union. Le troisième domaine essentiel devrait être la certification de cybersécurité et la normalisation, tandis que le quatrième devrait être la mise en œuvre de l'académie des compétences en matière de cybersécurité, qui devrait contribuer au développement d'une main-d'œuvre européenne abondante dans le domaine de la cybersécurité, dotée de compétences qui devraient être transférables dans tous les États membres.

(10) Le règlement (UE, Euratom) 2023/2841 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union prévoit le mandat du CERT-UE, en faisant de ce dernier le service de cybersécurité pour les institutions, organes et organismes de l'Union chargé de contribuer à la sécurité de l'environnement TIC non classifié des entités de l'Union en leur fournissant des conseils concernant la cybersécurité, en les aidant à prévenir, à détecter et à traiter les incidents, ainsi qu'à en atténuer les effets, à y répondre et à s'en remettre, et en faisant office de pôle d'échange d'informations sur la cybersécurité et de coordination des réponses aux incidents. En outre, le CERT-UE est chargé de proposer des services de cybersécurité pertinents aux entités de l'Union. Dans le cadre de sa mission, l'ENISA devrait également soutenir les entités de l'Union. Pour ce faire, elle devrait notamment mener une coopération structurée avec le CERT-UE en ce qui concerne le renforcement des capacités, la coopération opérationnelle et les analyses stratégiques à long terme des cybermenaces. Le cas échéant, l'ENISA peut tirer parti de sa coopération structurée avec le CERT-UE pour offrir des services de cybersécurité ou un soutien susceptible d'apporter une valeur ajoutée aux entités de l'Union, de manière coordonnée afin de garantir des synergies avec les efforts du CERT-UE.

(11) L'une des tâches essentielles de l'ENISA devrait être d'aider les États membres à mettre en œuvre de manière cohérente la politique et le droit de l'Union en matière de cybersécurité, notamment en ce qui concerne la directive (UE) 2022/2555, le règlement (UE) 2024/2847 et le règlement (UE) 2025/38. Afin de contribuer à la mise en œuvre cohérente et efficace de l'acquis de l'Union en matière de cybersécurité, l'ENISA devrait publier des rapports et des orientations techniques, fournir des conseils et des bonnes pratiques et faciliter l'échange de bonnes pratiques entre les autorités compétentes à cette fin. En outre, l'ENISA évalue l'état de la cybersécurité dans l'Union et adopte un rapport à cette fin conformément à l'article 18 de la directive (UE) 2022/2555. L'ENISA devrait également être en mesure de répondre aux demandes de conseil et d'assistance des États membres et, le cas échéant, des entités de l'Union sur des questions qui relèvent de son mandat.

(12) Afin de stimuler la coopération entre le secteur public et le secteur privé et au sein de ce dernier, notamment pour soutenir la protection des infrastructures critiques, l'ENISA devrait soutenir le partage d'informations au sein des secteurs et entre ceux-ci, en particulier les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555, et d'informations concernant les produits comportant des éléments numériques relevant du champ d'application du règlement (UE) 2024/2847. Elle peut apporter un tel soutien en proposant des bonnes pratiques et des orientations sur les

outils disponibles et sur les procédures, ainsi qu'en proposant des orientations sur la manière de traiter les questions de réglementation liées au partage d'informations, par exemple en facilitant la mise en place de centres de partage et d'analyse d'informations sectoriels (ISAC).

(13) En vue de soutenir et de faciliter la coopération stratégique et l'échange d'informations, l'ENISA devrait contribuer aux travaux du groupe de coopération institué par la directive (UE) 2022/2555 (ci-après le «groupe de coopération SRI»), notamment en le faisant bénéficier de ses conseils et de ses compétences et en facilitant l'échange de bonnes pratiques en matière de risques et d'incidents, entre autres en ce qui concerne les dépendances transfrontières. L'ENISA devrait également contribuer aux travaux du groupe de coopération européen en matière d'identité numérique institué par le règlement (UE) nº 910/2014 du Parlement européen et du Conseil[46], du groupe européen de certification de cybersécurité et du groupe de coopération administrative (ADCO) institué par le règlement (UE) 2024/2847.

(14) Le noyau public de l'internet ouvert, à savoir ses principaux protocoles et ses principales infrastructures, qui constituent un bien public mondial, joue un rôle essentiel dans la fonction de l'internet en général et soutient son fonctionnement normal. Dans le cadre de son mandat, l'ENISA devrait soutenir la sécurité et la résilience du noyau public de l'internet ouvert et la stabilité de son fonctionnement, y compris, sans s'y limiter, le déploiement et l'exploitation sécurisés de ses protocoles clés (notamment le système de noms de domaine, le protocole BGP et l'IPv6) et le fonctionnement du système des noms de domaines (tel que le fonctionnement de tous les domaines de premier niveau), en promouvant les meilleures pratiques, les orientations et la coopération, conformément aux dispositifs mondiaux de gouvernance multipartite de l'internet et aux rôles et responsabilités respectifs des organismes techniques et opérationnels internationaux concernés.

(15) L'ENISA sert de point de référence pour les conseils et compétences en matière de cybersécurité. Par conséquent, à la demande de la Commission, l'ENISA devrait l'assister au moyen d'une expertise, de conseils techniques, d'informations, d'analyses, y compris d'études de faisabilité, d'avis et de travaux préparatoires concernant toute question spécifique dans le domaine de la cybersécurité, en vue d'éclairer l'élaboration des politiques de la Commission et de faciliter le suivi par la Commission de la mise en œuvre de la législation de l'Union en matière de cybersécurité.

(16) De même, compte tenu de son expertise, l'ENISA devrait assister les États membres dans leurs efforts pour mettre en place et développer les capacités et la préparation requises aux fins de prévenir et de détecter les cybermenaces et incidents et d'y réagir, et en ce qui concerne la sécurité des réseaux et des systèmes d'information. L'ENISA devrait notamment soutenir le développement et l'amélioration des centres de réponse aux incidents de sécurité informatique (CSIRT) prévus par la directive (UE) 2022/2555, afin d'atteindre un niveau de maturité commun élevé des CSIRT dans l'Union.

---

[46] 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).

(17) L'ENISA a soutenu et devrait continuer à aider les États membres à élaborer et à mettre en œuvre des lignes directrices pour leurs stratégies nationales de cybersécurité et à contribuer à l'adoption et à la mise en œuvre de stratégies de cybersécurité par tous les États membres. L'ENISA devrait promouvoir la diffusion de telles stratégies au moyen de la carte interactive des stratégies nationales en matière de cybersécurité (SNCS) et continuer de suivre les progrès de leur mise en œuvre, y compris en soutenant la mise au point d'indicateurs de performance clés dans ce contexte.

(18) Le règlement (UE, Euratom) 2023/2841 a chargé le conseil interinstitutionnel de cybersécurité d'aider les entités de l'Union à améliorer leur posture de cybersécurité respective et le CERT-UE de contribuer à la sécurité de l'environnement TIC non classifié de toutes les entités de l'Union. L'ENISA, sur la base de son expérience en matière de cybersécurité, devrait soutenir le conseil interinstitutionnel de cybersécurité et le CERT-UE dans leurs tâches conformément au règlement (UE, Euratom) 2023/2841, y compris en contribuant à l'analyse des cybermenaces, à la conscience situationnelle, aux exercices de cybersécurité, à la coordination de la réaction aux incidents et à l'échange de savoir-faire et de meilleures pratiques.

(19) Sur la base de l'expertise de l'ENISA et afin de compléter les capacités des autorités publiques nationales et de l'Union, l'ENISA devrait dispenser des formations en s'appuyant sur le cadre européen des compétences en matière de cybersécurité (ECSF), en particulier pour favoriser une mise en œuvre efficace des politiques, la coopération opérationnelle et la sensibilisation.

(20) Afin de garantir des synergies avec le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité (CECC) et le Réseau de centres nationaux de coordination établi en vertu du règlement (UE) 2021/887 du Parlement européen et du Conseil[47], l'ENISA devrait les soutenir en partageant des informations sur les risques et cybermenaces actuels et émergents, y compris les risques et les menaces concernant les technologies de l'information et de la communication.

(21) La stratégie de préparation souligne que l'habileté numérique, qui repose sur l'acquisition de compétences numériques de base, est essentielle pour donner aux citoyens les moyens d'agir de manière plus résiliente face à d'éventuelles crises. Toutefois, comme souligné dans la communication de la Commission sur l'union des compétences[48], près de la moitié de la population adulte ne possède pas de compétences numériques de base, lesquelles sont néanmoins nécessaires dans plus de 90 % des emplois. Afin de faire en sorte que la main-d'œuvre actuelle et potentielle future possède les compétences requises dans un environnement numérique en évolution rapide et de contribuer au développement du réservoir européen de talents en matière de cybersécurité, l'ENISA devrait soutenir les activités de sensibilisation à la cybersécurité qui visent à attirer les talents et contribuer à informer sur l'éducation et les compétences nécessaires dans le domaine de la cybersécurité, telles que le défi européen en matière de cybersécurité. À cet égard, l'ENISA devrait coordonner les

---

47 Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination (JO L 202 du 8.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

48 Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «L'union des compétences» [COM(2025) 90 final], 5 mars 2025.

concours dans le domaine de la cybersécurité, les jeux de «capture du drapeau» et les exercices pratiques similaires, afin de développer les compétences en matière de cybersécurité et de favoriser le renforcement des capacités dans l'ensemble de l'Union. Lorsqu'elle mène des activités de sensibilisation, l'ENISA devrait veiller à ce que celles-ci répondent aux besoins des autorités publiques nationales et des entités de l'Union, ainsi qu'aux besoins des entreprises, en particulier des PME, et des établissements d'enseignement et de formation, en maintenant des cadres et des formations pratiques tels que la boîte à outils «Awareness Raising in a Box». L'ENISA devrait continuer à élaborer des orientations pratiques et exploitables pour soutenir la mise en œuvre de la politique et de la législation de l'Union en matière de cybersécurité. L'ENISA devrait également s'efforcer de fournir des informations pertinentes concernant les schémas de certification en vigueur, par exemple en fournissant des lignes directrices et des recommandations.

(22) Afin de soutenir les entreprises actives dans le secteur de la cybersécurité et les utilisateurs qui recourent aux solutions de cybersécurité, ainsi que de garantir la mise en œuvre effective du titre III du présent règlement, l'ENISA devrait mettre sur pied et gérer un «observatoire du marché» en procédant à des analyses régulières et en diffusant des informations sur les principales tendances observées sur le marché de la cybersécurité, tant du côté de la demande que du côté de l'offre. En outre, afin de soutenir les utilisateurs de la réserve de cybersécurité de l'Union établie en vertu du règlement (UE) 2025/38, l'ENISA devrait préparer la cartographie des services nécessaires à ces utilisateurs et de leur disponibilité, conformément audit règlement.

(23) Les cybermenaces constituent un problème mondial. L'amélioration de la cybersécurité nécessite un renforcement de la coopération internationale, y compris pour définir des normes de comportement et des approches communes. À cette fin, l'ENISA devrait soutenir la coopération de l'Union avec les pays tiers, en mettant l'accent sur les pays candidats à l'adhésion à l'Union et les organisations internationales, telles que l'OTAN, en mettant les compétences et l'analyse nécessaires au service de la Commission et des entités compétentes de l'Union, le cas échéant. Les activités de l'ENISA au niveau international devraient toujours répondre aux priorités de l'Union.

(24) Afin de contribuer à atteindre un niveau élevé de cybersécurité dans l'Union, l'ENISA devrait soutenir la coopération opérationnelle entre les États membres, en coopération avec le CERT-UE, entre les entités de l'Union et entre les parties prenantes. À cette fin, le rôle de l'ENISA devrait être renforcé. L'ENISA devrait devenir membre du réseau des CSIRT, en contribuant ainsi à l'échange et à l'analyse d'informations sur le réseau. L'ENISA devrait continuer à promouvoir et soutenir la coopération entre les CSIRT concernés en cas d'incidents, d'attaques ou de perturbations sur les réseaux ou infrastructures dont les CSIRT assurent la gestion ou la protection. Le soutien actif de l'ENISA aux travaux du réseau des CSIRT et du réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) devrait permettre à ces réseaux de continuer à gagner en maturité Le rôle joué par l'ENISA dans le soutien à cette coopération consiste notamment à lutter contre les menaces qui pèsent sur la sécurité et l'intégrité des institutions démocratiques, des élections et d'autres processus, ainsi que des infrastructures critiques dont ils dépendent, conformément au bouclier européen de la démocratie: renforcer la position de démocraties fortes et résilientes[49].

[49] JOIN(2025) 791 final.

(25) Afin de soutenir le renforcement des capacités, la coopération opérationnelle et les analyses stratégiques à long terme des cybermenaces, l'ENISA devrait recourir aux compétences techniques et opérationnelles disponibles du CERT-UE grâce à une coopération structurée, par exemple au moyen d'arrangements spécifiques.

(26) Afin de renforcer la cybersécurité dans l'ensemble de l'Union et d'assurer une réaction rapide et efficace aux cybermenaces, l'ENISA devrait soutenir les États membres à leur demande, notamment en fournissant des conseils sur la manière d'améliorer leurs capacités de prévention et de détection des incidents, de réaction aux incidents et de rétablissement après ceux-ci, en facilitant la gestion technique des incidents importants au sens de la directive (UE) 2022/2555, en particulier en favorisant le partage volontaire de solutions techniques entre les États membres, ou en assurant l'analyse des cybermenaces et des incidents. L'ENISA devrait également aider EU-CyCLONe à élaborer des rapports au niveau politique de l'Union et des États membres.

(27) Afin de réduire l'exposition à l'ingérence étrangère, à la manipulation des chaînes d'approvisionnement et à l'exfiltration stratégique de données, l'ENISA devrait utiliser les outils de communication sécurisés du réseau des CSIRT et EU-CyCLONe. Sur la base de la recommandation relative au schéma directeur de l'UE en matière de cybersécurité, ces outils devraient être fournis par des entités juridiques établies ou réputées établies dans l'Union et contrôlées par des États membres ou par des ressortissants d'États membres.

(28) Afin de contribuer à la préparation et à la réaction au niveau de l'Union en cas de crises et d'incidents de cybersécurité majeurs, l'ENISA devrait mener des activités de conscience situationnelle en matière de cybersécurité.

(29) L'accès à des renseignements vérifiés et fiables en temps réel sur les cybermenaces est essentiel pour établir une conscience situationnelle commune dans l'Union. L'ENISA, la Commission, le CERT-UE et le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol ont déjà mis au point des répertoires de renseignements sur les cybermenaces qui sont adaptés à leurs besoins spécifiques. L'ENISA et d'autres entités concernées de l'Union devraient coopérer, sur une base volontaire, pour mettre au point des répertoires de renseignements fiables, vérifiés et en temps réel sur les cybermenaces et rechercher des synergies afin de réaliser des économies d'échelle et de renforcer la bonne gestion financière. Ces travaux devraient également inclure des entités sectorielles de l'Union telles que l'agence de l'Union européenne pour le programme spatial. Dans le cadre de ces travaux, seules des analyses dérivées, des tendances et des tactiques, techniques et procédures devraient être partagées et non les sources brutes, et il y a lieu de respecter l'indépendance des entités en ce qui concerne leur gestion du cycle de vie des renseignements sur les cybermenaces conformément à leur mandat et à leurs règles relatives au besoin d'en connaître.

(30) Afin de contribuer à une réaction rapide et coordonnée, l'ENISA devrait être en mesure d'envoyer des alertes précoces concernant un incident important ou majeur potentiel ou en cours, ou une cybermenace de nature transfrontière potentielle, au(x) CSIRT concerné(s) et, le cas échéant, au réseau des CSIRT et à EU-CyCLONe, en particulier en ce qui concerne les entités énumérées aux annexes I et II de la directive (UE) 2022/2555. Les informations contenues dans ces alertes précoces peuvent porter sur des vulnérabilités connues du public et indiquer si ces vulnérabilités affectent des produits comportant des éléments numériques couverts par le règlement (UE) 2024/2847 et peuvent également concerner des techniques et procédures, des

indicateurs de compromission, des tactiques adverses, ainsi que des informations spécifiques sur les acteurs de la menace et des recommandations de mesures d'atténuation.

(31) Afin de maintenir la confiance et de ne pas compromettre le partage d'informations, il est important que l'ENISA applique des marquages visibles indiquant dans quelle mesure un document ou des informations qu'elle a produits ou reçus peuvent être ultérieurement partagés. De même, l'ENISA devrait utiliser les documents ou informations qu'elle reçoit aux fins de l'exercice de ses activités, sous réserve d'éventuelles limitations de la diffusion ultérieure de ces informations, indiquées au moyen d'un marquage visible.

(32) Afin de contribuer à mieux faire connaître les indicateurs de cybermenace et les recommandations sur les mesures d'atténuation, l'ENISA devrait mettre un service d'alerte précoce à la disposition des entités opérant dans les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555. Ces alertes précoces génériques et volontaires devraient bénéficier en particulier aux PME et être fournies dans un format lisible par machine accessible au public. En tout état de cause, ce service volontaire est distinct d'éventuels partenariats public-privé que l'ENISA pourrait établir ou a déjà établis et n'a pas de lien avec ceux-ci.

(33) Afin de faciliter une conscience situationnelle commune en matière de cybersécurité au niveau de l'Union, l'ENISA devrait préparer à intervalles réguliers, en coopération étroite avec les États membres, un rapport approfondi de situation technique en matière de cybersécurité de l'Union européenne sur les incidents et cybermenaces dans l'Union, sur la base d'informations du domaine public, de sa propre analyse et de rapports que lui communiquent les CSIRT des États membres ou les points de contact nationaux uniques en matière de sécurité des réseaux et des systèmes d'information (ci-après dénommés «points de contact uniques») prévus par la directive (UE) 2022/2555, sur une base volontaire dans les deux cas, Europol et la CERT-UE. Ce rapport devrait être mis à la disposition du Conseil, du Service européen pour l'action extérieure, d'EU-CyCLONe, du réseau des CSIRT, de la Commission et d'Europol.

(34) Afin d'améliorer la conscience situationnelle commune du panorama des cybermenaces et des incidents par les parties prenantes, l'ENISA devrait analyser les tendances en matière de cybermenaces et d'incidents. Cela devrait inclure une analyse régulière portant sur les secteurs hautement critiques et d'autres secteurs critiques énumérés aux annexes I et II de la directive (UE) 2022/2555, y compris les secteurs des soins de santé, de l'énergie et des transports. Cette analyse devrait inclure le niveau de maturité des secteurs et recenser, entre autres, les éventuelles difficultés propres à un secteur donné. Le cas échéant, et afin de recenser les effets sur les chaînes d'approvisionnement, l'analyse devrait mettre en évidence les cybermenaces et les tendances liées aux catégories de produits couvertes par le règlement (UE) 2024/2847. L'ENISA devrait développer des compétences dans le domaine de la cybersécurité des infrastructures et de leurs dépendances critiques à l'égard de la chaîne d'approvisionnement, en particulier pour soutenir les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555 et la mise en œuvre du règlement (UE) 2024/2847. À cette fin, l'ENISA devrait également coopérer, le cas échéant, avec d'autres entités de l'Union concernées.

(35) En outre, pour mieux comprendre les défis dans le domaine de la cybersécurité, l'ENISA doit analyser les technologies actuelles et émergentes et fournir des évaluations thématiques sur les incidences escomptées des innovations technologiques

en matière de cybersécurité, du point de vue sociétal, juridique, économique et réglementaire. En vue de faciliter l'accès du public à des informations sur les risques liés à la cybersécurité et les solutions possibles, l'ENISA peut fournir des informations pertinentes sur son site web, d'une manière conviviale et bien structurée.

(36) Le rôle renforcé de l'ENISA dans la promotion de la conscience situationnelle, dans l'analyse des menaces et dans la fourniture de conseils techniques contribuera à renforcer les efforts collectifs en matière de cybersécurité concernant les produits comportant des éléments numériques et soutiendra la mise en œuvre du règlement (UE) 2024/2847. Conformément au règlement (UE) 2024/2847, l'ENISA peut proposer des activités conjointes aux autorités de surveillance du marché pour vérifier la conformité des produits comportant des éléments numériques et recenser les catégories de produits comportant des éléments numériques pour lesquelles des opérations «coup de balai» pourraient être organisées. Les informations provenant de l'analyse des cybermenaces et des alertes précoces devraient renforcer le soutien apporté par l'ENISA à ces autorités et contribuer à une application effective du règlement (UE) 2024/2847 en vue de prévenir les effets des cyberattaques sur les chaînes d'approvisionnement dans l'ensemble du marché intérieur et d'améliorer la préparation globale de l'Union.

(37) Les attaques par rançongiciel constituent une menace majeure pour la cybersécurité de l'Union. Afin de renforcer la cybersécurité de l'Union et de lutter contre les rançongiciels, l'ENISA devrait développer des capacités de conscience situationnelle et de soutien aux efforts de réaction et de rétablissement après un incident. Lorsqu'elle aide certaines entités essentielles et importantes à réagir à une attaque par rançongiciel et à s'en rétablir, l'ENISA devrait coopérer étroitement avec Europol et avec les CSIRT ou les autorités compétentes, selon le cas, en s'appuyant ainsi sur l'expérience acquise par Europol dans la lutte contre la criminalité par rançongiciel. Cette assistance devrait compléter les activités menées par les CSIRT pour soutenir la réaction aux incidents. Afin de créer des synergies dans ses travaux contre les rançongiciels, l'ENISA devrait mettre en place un service d'assistance et, à cette fin, elle pourrait rassembler les capacités pertinentes et les services de lutte contre les rançongiciels et rendre aisément accessibles des informations, des orientations et des outils susceptibles d'aider les entités essentielles et importantes à réagir à un incident lié à un rançongiciel et à s'en rétablir.

(38) L'ENISA devrait fournir une expertise technique et un soutien à la Commission dans l'élaboration d'un programme annuel continu d'exercices de cybersécurité au niveau de l'Union, conformément à la recommandation relative au schéma directeur de l'UE en matière de cybersécurité, afin de se préparer aux crises de cybersécurité, de tester le niveau de cybersécurité des entités participant à ces exercices et de réduire au minimum les doubles emplois. L'ENISA devrait, par exemple, fournir des conseils sur les types d'exercices appropriés, tels que les exercices théoriques, hybrides ou en direct, ainsi que sur les objectifs, les scénarios et la participation.

(39) L'accès à des informations correctes et en temps utile sur les vulnérabilités et une gestion solide des vulnérabilités sont indispensables pour garantir un niveau élevé de cybersécurité dans le marché intérieur. C'est pourquoi l'ENISA devrait tenir à jour une base de données européenne des vulnérabilités conformément à la directive (UE) 2022/2555 et créer une capacité commune de l'Union en matière de services de gestion des vulnérabilités, en garantissant un niveau de service résilient et durable et en réduisant le risque de perturbations. À cette fin, l'ENISA devrait étudier les possibilités d'approfondir sa coopération structurée avec des programmes, des

registres ou des bases de données similaires à la base de données européenne des vulnérabilités, afin d'éviter une duplication des efforts et de rechercher des complémentarités au niveau international, le cas échéant. En outre, l'ENISA devrait soutenir la divulgation multipartite coordonnée de vulnérabilité au niveau de l'Union et fournir des services à valeur ajoutée, tels que des conseils sur les vulnérabilités, l'attribution de scores de gravité et des listes de produits, ainsi qu'un catalogue européen amélioré des vulnérabilités exploitables constatées afin d'aider les entités à gérer les vulnérabilités.

(40) Le rôle joué de l'ENISA dans le développement de l'ECCF devrait être un aspect essentiel de son mandat. L'ENISA devrait fournir son expertise technique tout au long du cycle de vie des schémas européens de certification de cybersécurité. Dans la perspective d'un futur schéma, l'ENISA devrait recenser les normes ou spécifications techniques existantes susceptibles d'être à la base d'un tel schéma et, le cas échéant, élaborer elle-même des spécifications techniques qui peuvent être incluses dans un schéma. L'ENISA devrait être chargée de préparer des schémas candidats à la demande de la Commission. L'ENISA devrait être chargée de la maintenance des schémas déjà en place Ce faisant, l'ENISA devrait contribuer à la mise en place et au développement d'un écosystème de certification dans lequel les retours d'information des États membres et des parties prenantes privées sont sollicités et leurs capacités de certification sont renforcées. Il convient également d'y inclure la gestion d'un site web consacré à la certification sur lequel les informations pertinentes relatives aux schémas adoptés, y compris les certificats et les déclarations de conformité, sont librement et publiquement accessibles.

(41) Afin de faciliter la mise en œuvre de la législation pertinente de l'Union, l'ENISA devrait façonner l'état de la technique en matière de cybersécurité en fournissant des spécifications techniques pour soutenir la mise en œuvre de la législation pertinente de l'Union, y compris en vue de leur référencement potentiel dans les schémas européens de certification de cybersécurité. L'ENISA devrait également surveiller la création et l'évolution des normes élaborées par les organismes de normalisation compétents en vue de suivre les tendances en matière de normalisation aux niveaux européen et mondial et, si nécessaire, de façonner ces normes en y participant, y compris en élaborant des contributions, et en jouant un rôle de premier plan dans les activités des organisations de normalisation. Dans ce cadre, l'ENISA devrait rester impartiale. Par exemple, il pourrait y avoir des situations dans lesquelles l'ENISA devrait se retirer des activités pertinentes menées au sein des organismes de normalisation si elle est invitée à évaluer des normes européennes qui ont été demandées par la Commission à l'appui de la législation de l'Union. L'ENISA ne devrait pas contribuer à l'élaboration des normes qu'elle est chargée d'évaluer.

(42) Afin de soutenir la mise en œuvre des politiques de l'Union et la préparation d'éventuelles activités de normalisation, l'ENISA devrait contribuer au développement et à l'évaluation d'algorithmes cryptographiques, en particulier dans le domaine de la cryptographie post-quantique. Dans ce contexte, à la demande de la Commission et sous réserve d'une convention de contribution telle que définie dans le règlement (UE, Euratom) 2024/2509 du Parlement européen et du Conseil[50], l'ENISA peut mettre en place un processus en vue de demander et d'évaluer les algorithmes

[50] Règlement (UE, Euratom) 2024/2509 du Parlement européen et du Conseil du 23 septembre 2024 relatif aux règles financières applicables au budget général de l'Union (JO L, 2024/2509, 26.09.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

utilisés pour les algorithmes cryptographiques par les parties prenantes concernées, en particulier le monde universitaire, la communauté des chercheurs et la communauté cryptographique, ainsi que les fabricants, les CSIRT, les autorités nationales de certification de cybersécurité et les autorités compétentes conformément à la directive (UE) 2022/2555. Lorsque l'ENISA contribue à la mise en place de tels processus, elle devrait promouvoir la collaboration entre les parties prenantes concernées et mettre en œuvre les aspects organisationnels. Le processus devrait être formel, ouvert, transparent et inclusif et comprendre une consultation des parties prenantes concernées sur les projets d'exigences minimales et le processus et les critères d'évaluation, notamment en ce qui concerne la sécurité et la réalisation des évaluations.

(43) Afin de soutenir la mise en œuvre des activités d'évaluation de la conformité au titre des schémas européens de certification de cybersécurité et d'autres actes législatifs pertinents de l'Union, l'ENISA peut fournir des outils de tests techniques pertinents pour aider les États membres, les entreprises et les organismes d'évaluation de la conformité à mener leurs activités d'évaluation. Ces outils devraient viser à créer des synergies au niveau de l'Union et à garantir un fonctionnement efficace des procédures d'évaluation de la conformité afin de répondre aux besoins des États membres et du marché. De tels besoins peuvent se présenter, par exemple, dans le domaine de la sécurité dès la conception afin de soutenir les entreprises, y compris les petites et moyennes entreprises, dans leurs efforts de mise en œuvre dans le cadre du règlement (UE) 2024/2847. Dans ce contexte, l'ENISA devrait percevoir des redevances pour couvrir les coûts pertinents liés à la mise en place, à la conception, au développement, à la maintenance et à la mise à jour des capacités logicielles et matérielles nécessaires à ces outils de tests.

(44) Afin de soutenir les États membres dans leurs efforts visant à remédier à la pénurie de professionnels de la cybersécurité et au besoin grandissant de main-d'œuvre qualifiée, diversifiée, y compris en ce qui concerne l'équilibre entre les hommes et les femmes, et souple, et de permettre la mobilité et la préparation de la main-d'œuvre dans tous les États membres, l'ENISA devrait s'appuyer sur les principes et les travaux lancés dans le cadre de l'académie des compétences en matière de cybersécurité. En particulier, l'ENISA devrait établir le cadre européen des compétences en matière de cybersécurité (ECSF) en tant que cadre commun pour les profils de rôles professionnels dans le domaine de la cybersécurité. L'ENISA devrait aider davantage les États membres à lutter contre les disparités entre les hommes et les femmes dans les rôles en matière de cybersécurité. Cette approche est conforme à la vision exposée dans la communication de la Commission sur l'union des compétences et contribuerait à la réalisation de ses objectifs. Il convient d'étudier plus avant la possibilité de créer un label de qualité pour les attestations individuelles européennes de compétences en matière de cybersécurité.

(45) L'ECSF devrait être un outil pratique et flexible à utiliser sur une base volontaire, fournissant une compréhension et une terminologie communes des rôles pertinents et des tâches, compétences et connaissances connexes principalement requises dans les rôles en matière de cybersécurité, en vue de faciliter le recensement des ensembles de compétences critiques, y compris les compétences transversales, requises pour la main-d'œuvre et de permettre aux prestataires de services d'apprentissage, y compris les entreprises, les établissements d'enseignement supérieur ou les prestataires d'enseignement et de formation professionnels, de concevoir des programmes et d'aider les décideurs politiques à élaborer des initiatives visant à remédier aux déficits de compétences. Cet outil, qui peut se prêter à une utilisation en tant que cadre de

référence pour la reconnaissance des compétences, devrait également être interopérable avec la classification européenne des aptitudes, compétences, certifications et professions (ESCO) afin d'aider les services des ressources humaines à comprendre les exigences en matière de planification des ressources, de recrutement et d'évolution de carrière qui sont nécessaires pour répondre aux besoins en matière de cybersécurité. Alors que le DigComp 3.0 décrit les connaissances, les aptitudes et les attitudes qui sont nécessaires pour être compétentes sur le plan numérique dans la vie quotidienne, la vie sociale, le travail et l'apprentissage, et peut être utilisé à la fois par les adultes et les enfants, l'ECSF offre un cadre simple recensant les rôles en matière de cybersécurité et les tâches, connaissances et compétences connexes nécessaires pour les exercer. À cet égard, il s'adresse à un public spécialisé dans la cybersécurité, allant des professionnels de la cybersécurité actuels ou potentiels aux employeurs, en passant par les établissements d'enseignement. L'ECSF devrait également encourager le développement d'attestations individuelles européennes de compétences en matière de cybersécurité en étant le principal instrument utilisé pour développer les schémas, en permettant l'émergence de nouveaux acteurs du marché et en soutenant la concurrence sur le marché dans un cadre commun. L'ECSF devrait faire l'objet d'une évaluation et d'une mise à jour à intervalles réguliers afin de veiller à ce qu'il reflète de manière adéquate les besoins du marché du travail en matière de cybersécurité ainsi que les évolutions technologiques et stratégiques. L'ENISA devrait encourager l'adoption de l'ECSF par les États membres et les entités de l'Union et au sein de ceux-ci et fournir un soutien adéquat lorsqu'une telle assistance est nécessaire.

(46) Les compétences et qualifications en matière de cybersécurité devraient être rendues comparables, transparentes et fiables dans l'ensemble du marché intérieur. À cette fin, les attestations individuelles européennes de compétences en matière de cybersécurité[51] devraient aider les employeurs, y compris les PME et les jeunes pousses, à recruter efficacement des professionnels de la cybersécurité, existants ou en devenir, au sein des États membres et entre eux, conformément aux objectifs énoncés dans la communication sur l'union des compétences. Afin de garantir une mise en œuvre cohérente dans tous les États membres, les attestations individuelles européennes de compétences en matière de cybersécurité devraient être fondées sur une compréhension commune, au niveau de l'Union, des compétences nécessaires pour atteindre ces objectifs et devraient être délivrées par des fournisseurs agréés par l'ENISA sur la base d'un ensemble commun de critères. Cette approche devrait être cohérente avec les objectifs de la future initiative sur la transférabilité des compétences et y contribuer.

(47) L'élaboration de programmes d'attestation individuelle européenne des compétences en matière de cybersécurité devrait viser à compléter les actions des États membres en offrant aux autorités publiques et aux acteurs économiques la possibilité de recourir à un mécanisme d'attestation européen, en application de la compétence d'appui de l'Union dans le domaine de l'enseignement et de la formation professionnels visée à l'article 6, point e), à l'article 165, paragraphe 1, et à l'article 166, paragraphe 1, TFUE. Ces schémas, ainsi que les travaux de l'académie des compétences en matière de cybersécurité, peuvent également servir de base aux programmes d'enseignement

[51] Les attestations individuelles européennes de compétences en matière de cybersécurité devraient être interprétées comme répondant à une approche similaire à ce que le marché appelle des «certifications de cybersécurité». Toutefois, afin d'éviter toute confusion avec le cadre européen de certification de cybersécurité, l'expression «attestation», déjà utilisée dans la communication sur l'académie des compétences en matière de cybersécurité, est privilégiée.

supérieur, tels que les diplômes européens du secteur, et au développement des microcertifications. Par conséquent, les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité ne devraient pas viser à harmoniser la législation et la réglementation des États membres, mais devraient plutôt être considérés comme un catalyseur et une opportunité que les États membres et les acteurs économiques pourraient vouloir saisir et promouvoir.

(48) L'ENISA devrait veiller à ce que les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité restent proches des besoins du marché et s'appuyer sur l'expérience des fournisseurs publics et privés de certifications individuelles, y compris les États membres, les établissements d'enseignement supérieur, les établissements d'enseignement et de formation professionnels et les entreprises. L'ENISA devrait consulter la Commission en ce qui concerne la hiérarchisation des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, en tenant dûment compte de la mise en œuvre des politiques et des besoins du marché.

(49) Afin de garantir l'alignement entre l'ECSF et les schémas, la révision d'un profil de rôle de l'ECSF devrait automatiquement déclencher une évaluation de l'adéquation du ou des schémas européens individuels d'attestation de compétences en matière de cybersécurité associés, qui pourrait conduire à leur réexamen.

(50) Compte tenu de la diversité des profils de rôle en matière de cybersécurité et des tâches, compétences et connaissances associées, il se peut que l'évaluation des personnes et les méthodes d'évaluation doivent être adaptées dans chaque schéma européen individuel d'attestation de compétences en matière de cybersécurité. Chaque schéma devrait garantir que l'évaluation des aptitudes requises d'une personne en termes d'acquis d'apprentissage, y compris, le cas échéant, l'évaluation de son niveau de compétence, est systématiquement évaluée par rapport à un profil de rôle de l'ECSF ou à un sous-ensemble de profils de rôles. Les méthodes d'évaluation peuvent inclure des éléments tels qu'un examen des connaissances théoriques, un examen pratique, des prérequis et une évaluation par les pairs. L'expérience des individus doit être dûment prise en considération.

(51) Afin de garantir une mise en œuvre cohérente des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, en particulier en ce qui concerne l'évaluation des personnes, l'ENISA devrait fournir une formation obligatoire au personnel chargé de procéder à cette évaluation. Ce personnel devrait disposer d'une expérience dans le domaine de la cybersécurité, qui pourrait être démontrée au moyen d'une attestation individuelle européenne des compétences en matière de cybersécurité correspondant au profil de fonction évalué et à un niveau de compétence au moins équivalent à celui des personnes qu'il évalue.

(52) Le rôle des fournisseurs d'attestations agréés est d'attester les connaissances et compétences d'une personne habilitant celle-ci à exercer l'une des fonctions de l'ECSF et de donner des assurances aux employeurs dans l'ensemble de l'Union. Les employeurs qui exploitent des infrastructures critiques de l'Union s'appuieraient eux aussi sur l'assurance de la qualité des aptitudes et des compétences des personnes ayant obtenu une attestation individuelle européenne de compétences en matière de cybersécurité; par conséquent, les fournisseurs agréés qui attestent le niveau d'aptitudes et de compétences devraient être dignes de confiance du point de vue de la cybersécurité et ne devraient pas être soumis à une influence indue de la part d'un pays tiers susceptible de susciter des préoccupations en matière de cybersécurité. Par

conséquent, les entités établies dans un pays tiers suscitant des préoccupations en matière de cybersécurité et désigné comme tel conformément au présent règlement, ou qui sont contrôlées par un tel pays tiers, par une entité établie dans un tel pays tiers ou par un ressortissant d'un tel pays tiers (fournisseurs à haut risque) conformément au présent règlement ne devraient pas pouvoir prétendre au statut de fournisseur agréé des attestations individuelles européennes de compétences en matière de cybersécurité visées au titre II, section 4.

(53) Afin que les personnes titulaires d'une attestation européenne de compétences en matière de cybersécurité puissent facilement l'utiliser et la partager et que cette attestation puisse être utilisée dans tous les États membres, les fournisseurs d'attestations agréés devraient veiller à ce que les attestations électroniques des attestations individuelles européennes de compétences en matière de cybersécurité soient délivrées au portefeuille européen d'identité numérique (portefeuille EUDi) établi par le règlement (UE) nº 910/2014 à la demande de la personne. Les fournisseurs d'attestations agréés devraient être considérés comme des prestataires de services de confiance et être soumis au régime de contrôle et de responsabilité prévu par le règlement (UE) nº 910/2014. Le schéma utilisé pour les attestations d'attributs conformément au règlement d'exécution (UE) 2025/1569[52] de la Commission devrait être enregistré dans le catalogue de schémas d'attestations d'attributs prévu par ledit règlement d'exécution.

(54) Afin de contribuer au développement de la main-d'œuvre dans le domaine de la cybersécurité et à la transférabilité des compétences dans l'ensemble de l'Union, l'ENISA devrait mettre les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité et la liste des fournisseurs d'attestations agréés à la disposition du public au moyen d'un site web dédié.

(55) L'ENISA devrait être régie et exploitée en prenant en considération les principes de l'approche commune sur les agences décentralisées de l'Union, adoptée le 19 juillet 2012 par le Parlement européen, le Conseil et la Commission[53]. Il convient par ailleurs de tenir compte, s'il y a lieu, des recommandations de l'approche commune dans les programmes de travail de l'ENISA, les évaluations de l'ENISA ainsi que les pratiques de l'ENISA en matière d'établissement de rapports et ses pratiques administratives.

(56) Pour que le conseil d'administration puisse s'acquitter efficacement de ses fonctions, notamment en guidant l'orientation générale des activités de l'ENISA et en fixant ses priorités stratégiques, il est essentiel qu'il soit composé de représentants de haut niveau des États membres et de la Commission. À cette fin, chaque État membre devrait nommer le dirigeant d'une autorité nationale compétente de cet État membre responsable de la cybersécurité désigné conformément à l'article 8, paragraphe 1, de la directive (UE) 2022/2555 en tant que membre du conseil d'administration.

(57) Afin de garantir que les suppléants au sein du conseil d'administration puissent remplir leur rôle de manière adéquate, les États membres devraient nommer des

---

52 Règlement d'exécution (UE) 2025/1569.

53 Approche commune figurant en annexe de la déclaration commune du Parlement européen, du Conseil de l'UE et de la Commission européenne sur les agences décentralisées, adoptée le 19 juillet 2012 et disponible (en anglais) à l'adresse suivante: https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.

suppléants possédant l'expertise et l'expérience professionnelles appropriées. La Commission et les États membres, en ce qui concerne les suppléants, devraient s'efforcer de parvenir à une représentation équilibrée entre les hommes et les femmes au sein du conseil d'administration et limiter le roulement de leurs représentants afin de garantir la continuité des travaux du conseil d'administration.

(58) Afin de permettre à l'ENISA de remplir efficacement sa mission, le conseil d'administration, composé de représentants des États membres et de la Commission, devrait définir l'orientation générale des activités de l'ENISA, y compris ses priorités stratégiques, et veiller à ce qu'elle exécute ses tâches conformément au présent règlement. Le conseil d'administration devrait être doté des pouvoirs nécessaires pour établir le budget et vérifier son exécution, adopter des règles financières appropriées, instaurer des procédures de travail transparentes pour la prise de décisions par l'ENISA, adopter le document unique de programmation de l'ENISA, adopter son propre règlement intérieur, nommer le directeur exécutif, statuer sur la prorogation et la cessation du mandat du directeur exécutif et décider s'il y a lieu de créer une fonction de directeur exécutif adjoint et, si une telle fonction est créée, de la nomination de ce directeur exécutif adjoint, ainsi que de la prolongation et de la fin de son mandat. Toute personne exerçant une fonction exécutive au sein de l'ENISA devrait donc être nommée par le conseil d'administration. Le conseil d'administration devrait également être chargé de nommer ou de révoquer les membres de la chambre de recours, ainsi que d'établir des règles visant à prévenir ou à gérer les conflits d'intérêts à cet égard.

(59) Afin de contribuer à ce que l'ENISA établisse ses priorités stratégiques et les tienne à jour, le conseil d'administration devrait tenir au moins une réunion par an consacrée aux priorités stratégiques de l'ENISA. Afin de veiller à ce que les réunions du conseil d'administration soient efficaces et éclairées, le conseil d'administration peut y inviter toute personne dont l'avis pourrait être pertinent et présenter un intérêt pour les sujets abordés afin de fournir des informations, une expertise ou des conseils. Cette personne serait un observateur ad hoc sans droit de vote.

(60) Le conseil d'administration devrait adopter ses décisions à la majorité absolue de ses membres disposant du droit de vote, sauf disposition contraire du présent règlement. En raison de l'importance des questions de budget et de ressources humaines, en particulier les questions relatives au budget annuel, au rapport annuel d'activité, à la stratégie antifraude, aux modalités d'application du statut des fonctionnaires, à la nomination du directeur exécutif, du directeur exécutif adjoint et du comptable, au suivi des conclusions de l'Office européen de lutte antifraude (OLAF) et du Parquet européen et à l'adoption des règles financières de l'ENISA, le conseil d'administration ne devrait adopter de telles décisions que si le représentant de la Commission exprime un vote favorable. Aux fins de la prise d'une décision relative à l'adoption d'un document de programmation unique final après prise en considération de l'avis de la Commission, un vote favorable du représentant de la Commission ne devrait être requis que sur les éléments de la décision qui ne sont pas liés au programme de travail annuel et pluriannuel de l'ENISA.

(61) Le conseil exécutif devrait contribuer au fonctionnement efficace du conseil d'administration. Dans le cadre de ses travaux préparatoires liés aux décisions du conseil d'administration, le conseil exécutif devrait examiner de manière approfondie les informations pertinentes, étudier les options disponibles et proposer des conseils et des solutions afin de préparer les décisions du conseil d'administration. Il devrait

également assister et conseiller le directeur exécutif dans la mise en œuvre des décisions du conseil d'administration.

(62) Le bon fonctionnement de l'ENISA exige que le directeur exécutif de celle-ci soit nommé sur la base de son mérite et de ses aptitudes attestées dans le domaine de l'administration et de la gestion, ainsi que de ses compétences et de son expérience pertinentes en matière de cybersécurité. Il convient que le directeur exécutif exerce ses fonctions en toute indépendance. Le conseil d'administration devrait nommer le directeur exécutif à partir de la liste de candidats établie par la Commission, au terme d'une procédure ouverte et transparente qui respecte le principe de l'équilibre entre les hommes et les femmes.

(63) Le directeur exécutif devrait élaborer une proposition de document de programmation unique pour l'ENISA, après consultation préalable de la Commission, et prendre toutes les mesures nécessaires pour garantir la bonne mise en œuvre de ce document unique de programmation. Le directeur exécutif devrait préparer un rapport annuel à soumettre au conseil d'administration, portant sur la mise en œuvre du programme de travail annuel de l'ENISA, établir un projet d'état prévisionnel des recettes et des dépenses de l'ENISA et exécuter le budget. Le directeur exécutif devrait, en outre, avoir la possibilité de créer des groupes de travail ad hoc pour traiter de questions spécifiques, en particulier de questions de nature scientifique, technique, juridique ou socio-économique. La création d'un groupe de travail ad hoc est notamment jugée nécessaire pour la préparation d'un schéma européen de certification de cybersécurité candidat spécifique (ci-après dénommé «schéma candidat»). La création d'un groupe de travail ad hoc pourrait également être nécessaire pour les activités de maintenance liées à des schémas européens de certification de cybersécurité spécifiques adoptés. Des groupes de travail ad hoc devraient également être créés pour l'élaboration et la maintenance des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité et pour aider l'Agence dans la gouvernance, la mise en œuvre et l'évolution de l'ECSF. Le directeur exécutif devrait veiller à ce que les membres des groupes de travail ad hoc soient sélectionnés selon les critères de compétence les plus élevés, visant à assurer un équilibre hommes-femmes et un équilibre adéquat, en fonction des questions spécifiques concernées, entre les administrations publiques des États membres, les entités de l'Union et le secteur privé, y compris l'industrie, les utilisateurs et les experts universitaires en matière de sécurité des réseaux et de l'information, ainsi que les experts universitaires en produits comportant des éléments numériques.

(64) Le conseil d'administration peut décider de créer une fonction de directeur exécutif adjoint pour assister le directeur exécutif lorsqu'il estime qu'une telle fonction est nécessaire pour assurer ou maintenir le bon fonctionnement de l'ENISA. Lorsqu'il décide de créer ou non cette fonction, le conseil d'administration peut tenir compte de l'avis du directeur exécutif.

(65) L'ENISA devrait disposer d'un groupe consultatif chargé d'assurer un dialogue régulier avec le secteur privé, les organisations de consommateurs et d'autres parties prenantes concernées. Le groupe consultatif de l'ENISA, institué par le conseil d'administration sur proposition du directeur exécutif, devrait s'attacher à examiner des questions pertinentes pour les parties prenantes et devrait les porter à l'attention de l'ENISA. Le groupe consultatif de l'ENISA devrait être consulté en particulier au sujet du projet de programme de travail annuel de l'ENISA. La composition du groupe consultatif de l'ENISA et les tâches assignées à ce groupe devraient assurer une représentation suffisante des parties prenantes dans les travaux de l'ENISA. Les

représentants des autorités chargées de l'application de la loi, de la protection des données et de la surveillance du marché au niveau national et à l'échelon de l'Union devraient pouvoir être représentés au sein du groupe consultatif de l'ENISA.

(66) Les demandeurs qui souhaitent devenir des fournisseurs d'attestations agréés ou renouveler leur agrément devraient avoir accès aux voies de recours nécessaires lorsqu'ils sont affectés par des décisions prises par l'ENISA. Par conséquent, il convient de mettre en place un mécanisme de recours approprié afin que les décisions correspondantes de l'ENISA puissent être contestées devant une commission de recours dont les décisions peuvent être soumises au contrôle juridictionnel de la Cour de justice de l'Union européenne en vertu des traités. L'obligation d'épuiser les voies de recours internes de l'ENISA avant d'introduire un recours devant la Cour de justice de l'Union européenne ne s'applique qu'aux personnes ayant qualité pour agir devant la chambre de recours.

(67) Pour garantir l'autonomie et l'indépendance complètes de l'ENISA et lui permettre d'exécuter ses tâches, il convient de la doter d'un budget suffisant et autonome principalement financé par une contribution de l'Union, mais aussi par des contributions des pays tiers participant aux travaux de l'ENISA et par des redevances payées par les fournisseurs d'attestations agréés et les organismes d'évaluation de la conformité qui participent aux programmes et qui délivrent des certificats de cybersécurité européens et des déclarations de conformité de l'UE. L'État membre d'accueil et tout autre État membre devrait être autorisé à apporter des contributions volontaires au budget de l'ENISA. Aucune contribution, qu'elle soit financière ou en espèces, reçue par l'ENISA de la part d'États membres, de pays tiers ou d'autres entités ou personnes ne devrait compromettre son indépendance ou son impartialité. La procédure budgétaire de l'Union devrait être applicable en ce qui concerne la contribution de l'Union et toute autre subvention imputable sur le budget général de l'Union. La Cour des comptes devrait contrôler les comptes de l'ENISA afin de garantir la transparence et la responsabilité. Afin de permettre à l'Agence de participer à tous les projets futurs dans le domaine en cause, il convient de lui accorder la possibilité d'obtenir des subventions.

(68) Afin de garantir que l'ENISA puisse répondre aux demandes relatives aux tâches qui lui incombent, en particulier en ce qui concerne les décisions d'autoriser des fournisseurs à délivrer des attestations individuelles européennes de compétences en matière de cybersécurité, et en ce qui concerne la maintenance des schémas européens de certification de cybersécurité et des outils de tests, l'ENISA devrait être habilitée à percevoir des redevances. Les redevances ayant trait au traitement des demandes visant à devenir fournisseur d'attestation agréé devraient être fixées de manière appropriée afin de contribuer suffisamment à couvrir les coûts estimés supportés pour élaborer et maintenir les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité et pour évaluer si les exigences et obligations à remplir pour devenir et rester un fournisseur d'attestation agréé sont et continuent d'être respectées. Les redevances imposées aux prestataires de services d'attestation agréés pour les coûts de délivrance et de renouvellement des autorisations devraient inclure les coûts liés aux évaluations réalisées par l'ENISA ou sous sa supervision. Les redevances ayant trait à la participation à des schémas européens de certification de cybersécurité et à la délivrance de certificats au titre de ces schémas devraient être fixées de manière appropriée afin de contribuer suffisamment à couvrir les coûts estimés de la maintenance de ces schémas. Le paiement de ces redevances devrait permettre aux organismes d'évaluation de la conformité notifiés et, le cas échéant, aux

titulaires de certificats dans le cadre d'un schéma de participer à ces activités ainsi qu'aux activités pertinentes de renforcement des capacités et de promotion afin d'encourager l'échange de meilleures pratiques et de favoriser l'adoption de schémas et de solutions certifiées.

(69) Afin de garantir la proportionnalité, la transparence et la sécurité juridique, les redevances devraient être fixées de manière transparente et équitable. Ces coûts incluent toutes les dépenses de l'ENISA réalisées en faveur des membres du personnel participant aux activités soumises à redevance, notamment la part des cotisations au régime de retraite versées par l'employeur et les coûts afférents à la chambre de recours. Les redevances ne doivent pas entraîner l'imposition de charges financières ou administratives inutiles pour les demandeurs. Des délais raisonnables devraient être fixés pour leur paiement.

(70) Il est nécessaire de mettre en place un ensemble d'indicateurs afin de mesurer la charge de travail, l'efficacité et l'efficience de l'Agence en ce qui concerne les activités financées par des redevances. L'Agence devrait tenir compte de ces indicateurs pour adapter ses prévisions en termes d'effectifs et sa gestion des ressources liées aux redevances afin d'être en mesure de répondre de manière adéquate à ces demandes et à toute fluctuation des recettes générées par les redevances.

(71) Afin de déceler et de gérer adéquatement les risques de conflits d'intérêts réels ou potentiels, l'ENISA devrait disposer de règles en matière de prévention et de gestion des conflits d'intérêts. L'ENISA devrait aussi appliquer les règles relatives à l'accès aux documents énoncées dans le règlement (CE) nº 1049/2001 du Parlement européen et du Conseil[54]. Le traitement des données à caractère personnel devrait être régi par le règlement (UE) 2018/1725 du Parlement européen et du Conseil[55]. L'ENISA devrait respecter les dispositions applicables aux entités de l'Union et la législation nationale concernant le traitement des informations, notamment les informations non classifiées sensibles et les informations classifiées de l'Union européenne (ICUE).

(72) Dans l'accomplissement de ses tâches, l'ENISA peut avoir accès à des informations sensibles, telles que des informations concernant les cybermenaces et les incidents. Par conséquent, il est essentiel qu'elle préserve la confidentialité des informations qu'elle traite. En particulier, conformément à l'article 339 du traité sur le fonctionnement de l'Union européenne (TFUE), les fonctionnaires et autres agents de l'ENISA sont tenus, même après la cessation de leurs fonctions, de ne pas divulguer les informations qui, par leur nature, sont couvertes par le secret professionnel et notamment les renseignements relatifs aux entreprises et concernant leurs relations commerciales ou les éléments de leur prix de revient.

(73) Afin de réaliser pleinement ses objectifs, l'ENISA devrait se concerter avec les autorités de contrôle de l'Union compétentes et avec d'autres autorités compétentes de l'Union ainsi qu'avec les entités pertinentes de l'Union, notamment le CERT-UE, l'EC3 au sein d'Europol, le CECC, l'Agence européenne de défense (AED), l'Agence

---

54 Règlement (CE) no 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43, ELI: http://data.europa.eu/eli/reg/2001/1049/oj).

55 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).

de l'Union européenne pour le programme spatial (EUSPA), l'Organe des régulateurs européens des communications électroniques (ORECE), l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), la Banque centrale européenne (BCE), l'Autorité bancaire européenne (ABE), le comité européen de la protection des données, l'Agence de coopération des régulateurs de l'énergie (ACER), l'Agence de l'Union européenne pour la sécurité aérienne (AESA) et toute autre agence de l'Union jouant un rôle dans le domaine de la cybersécurité. L'ENISA devrait aussi se concerter avec les autorités compétentes au titre de la directive (UE) 2022/2555, les autorités de surveillance du marché et les autorités chargées de la protection des données en vue de procéder à des échanges de savoir-faire et de bonnes pratiques et devrait leur fournir des conseils sur les questions liées à la cybersécurité qui sont susceptibles d'avoir une incidence sur leurs travaux.

(74) Europol joue un rôle important dans la prévention et la lutte contre la cybercriminalité, y compris la cybercriminalité concernant les incidents liés à la sécurité des réseaux et de l'information. Afin de créer des synergies entre les tâches respectives de chaque agence, l'ENISA devrait coopérer avec Europol, notamment en partageant des informations sur les tendances en matière de techniques, d'exigences et d'incidences des attaques par rançongiciel. Cette coopération peut également consister à recenser les souches de rançongiciels les plus courantes ciblant les entités énumérées aux annexes I et II de la directive (UE) 2022/2555 afin d'aider les entités essentielles et importantes à réagir aux incidents et à s'en remettre.

(75) Afin de favoriser la coopération opérationnelle et la conscience situationnelle commune en matière de cybermenaces et d'incidents, il est essentiel que l'ENISA coopère avec les parties prenantes et, en particulier, avec les entreprises et les organisations du secteur privé, avec lesquelles elle peut nouer des partenariats public-privé.

(76) En vue d'atteindre efficacement les objectifs énoncés dans le présent règlement, l'ENISA peut collaborer, en particulier, avec des établissements universitaires qui mènent des initiatives de recherche dans des domaines pertinents et mettre au point des canaux appropriés pour les contributions d'organisations de consommateurs et d'autres organisations.

(77) Compte tenu de la nature transfrontière des cybermenaces et incidents, le niveau de cybersécurité et de préparation des pays tiers peut avoir une incidence sur les entités de l'Union. Par conséquent, l'ENISA devrait être en mesure de fournir des activités de renforcement des capacités, y compris des formations, des activités de renforcement des capacités, des activités de jumelage dans des pays tiers, et, en particulier, des activités de renforcement des capacités sur mesure pour les pays candidats à l'adhésion à l'Union ou pour d'autres pays partenaires conformément aux priorités de l'Union. Ces activités devraient être menées à la suite d'une demande spécifique d'obtention d'un soutien adéquat, en tenant compte des priorités de l'Union, et être mises en œuvre au moyen d'arrangements spéciaux, y compris au moyen des conventions de contribution visées dans le règlement (UE, Euratom) 2024/2509. Le cadre européen de certification de cybersécurité vise à offrir une protection contre les cybermenaces telles que les vulnérabilités de cybersécurité exploitées de manière malveillante ou les incidents de cybersécurité affectant la fonctionnalité (conception et fonctionnement) des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou de la posture de cybersécurité des entités. En se concentrant sur les risques techniques liés aux produits TIC, aux services TIC, aux processus TIC, aux

services de sécurité gérés ou à la posture de cybersécurité des entités, l'ECCF devrait compléter le cadre relatif à la sécurité des chaînes d'approvisionnement des TIC, qui vise à garantir une approche harmonisée au niveau de l'Union pour faire face aux risques non techniques dans les secteurs hautement critiques et d'autres secteurs critiques.

(78) Les États membres devraient avoir la possibilité de recourir à la certification européenne de cybersécurité dans le cadre des marchés publics conformément à la directive nº 2014/24/UE du Parlement européen et du Conseil[56].

(79) Afin de simplifier le respect des règles pour les entités, l'ECCF devrait prévoir la possibilité de certifier leur posture de cybersécurité. Les entités, notamment celles qui fournissent plusieurs types de services dans plusieurs États membres, peuvent être confrontées à des obligations différentes en matière de cybersécurité et de sécurité des données au titre d'instruments horizontaux, tels que le règlement (UE) 2016/679 du Parlement européen et du Conseil[57] et la directive (UE) 2022/2555 du Parlement européen et du Conseil[58], ainsi que d'instruments sectoriels. Afin de rationaliser la mise en œuvre du cadre réglementaire global en matière de cybersécurité et de faciliter son respect, la législation de l'Union devrait pouvoir prévoir la possibilité pour les entités de démontrer leur conformité avec les exigences en matière de gestion des risques de cybersécurité au moyen d'un certificat de cybersécurité européen. Un schéma pertinent pourrait contribuer à rationaliser les exigences de conformité découlant de différents instruments réglementaires, sans préjudice de leurs exigences de certification spécifiques. Ces mesures de simplification sont susceptibles de réduire la charge administrative, en débloquant des ressources pour renforcer la préparation opérationnelle en matière de cybersécurité des entités dans les secteurs critiques de l'Union.

(80) La certification européenne des exigences en matière de gestion des risques de cybersécurité élaborée au sein de l'ECCF devrait permettre aux entités de démontrer qu'elles respectent la législation pertinente de l'Union lorsqu'un schéma couvre les exigences juridiques correspondantes énoncées dans cette législation et lorsqu'il le prévoit. Sur cette base, un acte juridique de l'Union peut également prévoir une présomption de conformité à ces exigences. De tels schémas pourraient contribuer à améliorer la mise en œuvre cohérente des exigences de cybersécurité de la législation de l'Union afin d'assurer des conditions de concurrence équitables entre les États membres et d'alléger la charge de mise en conformité.

(81) Le cadre européen de certification de cybersécurité devrait prévoir la possibilité de certifier les processus TIC, définis comme un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la

---

56 Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).

57 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

58 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).

maintenance. Un profil de protection est un exemple de processus TIC, comme spécifié dans le règlement d'exécution (UE) 2024/482 de la Commission[59]. Un autre exemple de processus TIC est la série d'activités réalisées par un fabricant afin de concevoir et de développer en toute sécurité un produit TIC, y compris les mesures physiques, logiques, procédurales, relatives au personnel et autres mesures de sécurité qui sont nécessaires pour protéger la confidentialité et l'intégrité de la conception et de la mise en œuvre d'un produit TIC dans son environnement de développement. La certification de ces activités est souvent appelée «certification de site» dans le cadre d'un processus de certification au titre du règlement d'exécution (UE) 2024/482 de la Commission.

(82) La définition des services de sécurité gérés figurant dans le présent règlement devrait être cohérente avec la définition des fournisseurs de services de sécurité gérés figurant dans la directive (UE) 2022/2555. Lesdits services consistent à effectuer des activités liées à la gestion des risques en matière de cybersécurité de leurs clients, ou à fournir une assistance dans le cadre de ces activités, et ont gagné en importance en ce qui concerne la prévention et la limitation des incidents. En conséquence, les fournisseurs de tels services sont considérés comme étant des entités essentielles ou importantes appartenant à un secteur hautement critique au titre de la directive (UE) 2022/2555. Les fournisseurs de services de sécurité gérés dans des domaines comme la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil jouent un rôle particulièrement important pour ce qui est de soutenir les efforts mis en œuvre par les entités pour prévenir et détecter les incidents, y réagir ou se rétablir après ceux-ci. Toutefois, des fournisseurs de services de sécurité gérés ont eux-mêmes été la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Il est donc nécessaire que les entités essentielles et importantes au sens de la directive (UE) 2022/2555 fassent preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés.

(83) Les schémas européens de certification de cybersécurité sont utiles pour une large communauté de parties prenantes, dont les fournisseurs de solutions TIC, les organismes d'évaluation de la conformité et les utilisateurs. Afin d'encourager un large engagement des parties prenantes, l'assemblée européenne pour la certification de cybersécurité (ci-après l'«assemblée») devrait être organisée au moins une fois par an dans le but de favoriser la collaboration entre la Commission, l'ENISA, les États membres et les parties prenantes concernées. Cette assemblée jouera un rôle central pour recenser et relever les nouveaux défis en matière de cybersécurité et les priorités stratégiques en matière de certification, ainsi que pour veiller à ce que les schémas de certification facilitent l'intégration sécurisée des technologies numériques et soient adaptés aux besoins des utilisateurs. L'assemblée devrait encourager l'Union à continuer à jouer un rôle moteur dans les activités de certification et préserver la capacité du cadre de certification à susciter la confiance des entreprises, des pouvoirs publics et du public.

(84) La Commission devrait tenir à jour un site web dédié afin de garantir la transparence en publiant des informations actualisées sur l'état d'avancement de la mise en œuvre de l'ECCF. Ce site web devrait contenir des informations sur les schémas de

[59] Règlement d'exécution (UE) 2024/482 de la Commission du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

certification en cours d'élaboration, les priorités stratégiques pour les futurs schémas de certification, les demandes adressées à l'ENISA en vue de l'élaboration de schémas de certification candidats et des informations sur l'adoption des schémas de certification. Le site web de la Commission complétera le site web de l'ENISA sur les schémas européens de certification de cybersécurité, qui devrait fournir des informations complètes sur la préparation technique des schémas candidats et sur la maintenance des schémas, en mettant l'accent sur les certificats de cybersécurité européens délivrés et les déclarations de conformité de l'Union.

(85) Afin de renforcer le dialogue entre les institutions de l'Union et de contribuer à un processus de consultation formel, ouvert, transparent et inclusif, la Commission devrait tenir compte des éléments découlant des avis exprimés par le Parlement européen et le Conseil ainsi que par l'assemblée européenne pour la certification de cybersécurité lors de l'évaluation du présent règlement.

(86) Les études de faisabilité menées par l'ENISA devraient contribuer à préparer la planification et le développement de schémas de certification de cybersécurité. Les études devraient prendre en considération les points de vue des parties prenantes concernées et aligner les futurs schémas de certification sur les activités de recherche, de développement et d'évaluation technologique en cours, en tenant compte, en particulier, des contributions des initiatives de recherche de l'Union et des États membres. Ces études peuvent aider à déterminer les normes et les spécifications techniques disponibles. Elles devraient être réalisées à la demande de la Commission ou conformément aux priorités stratégiques de l'Union afin de veiller à ce que l'évolution du paysage technologique et des besoins en matière de cybersécurité soit dûment prise en considération lors de la demande et de l'élaboration des schémas.

(87) La conception du schéma candidat et sa couverture des objectifs et éléments de sécurité devraient être proportionnées au sujet et à la portée de l'objet de la certification. Par exemple, un schéma de certification des services en nuage pourrait répondre à des objectifs de sécurité pertinents pour les services TIC et la sécurité organisationnelle. À titre d'autre exemple, un objectif de sécurité lié à la non-inclusion de vulnérabilités exploitables connues ne sera probablement pas pertinent pour la certification de processus TIC.

(88) Afin de garantir que les schémas européens de certification de cybersécurité sont mis en œuvre de manière harmonisée dans tous les États membres, il est nécessaire de prévoir des règles relatives à leur maintenance. Des activités de maintenance sont également nécessaires pour veiller à ce que les schémas et leurs documents justificatifs restent à jour, en particulier dans un domaine de cybersécurité où le paysage des menaces et les technologies évoluent constamment. Les schémas de certification devraient donc être conçus et maintenus de manière à éviter qu'ils deviennent rapidement obsolètes. Les activités de maintenance devraient généralement comprendre la rédaction et la mise à jour de documents justificatifs, y compris de spécifications techniques et de lignes directrices, ainsi que la détermination de normes ou de spécifications techniques pertinentes pour le schéma. L'analyse du fonctionnement du schéma, de ses lacunes potentielles et des améliorations nécessaires devrait également faire partie des activités de maintenance. En outre, les activités de maintenance devraient inclure le partage d'informations entre les États membres en ce qui concerne la mise en œuvre des schémas et les contributions aux mécanismes d'examen et d'évaluation par les pairs.

(89) En raison de la nature technique des activités de maintenance, l'ENISA devrait en assurer la gestion, en coopération avec la Commission et avec le soutien du groupe européen de certification de cybersécurité (GECC) et de son sous-groupe pertinent sur la maintenance. La création du sous-groupe du GCEC sur la maintenance permet de recueillir des contributions et des informations techniques auprès des États membres en vue d'harmoniser les approches.

(90) Les activités de maintenance devraient impliquer des interactions avec les groupes de parties prenantes concernés afin de veiller à ce que les schémas restent pertinents pour le marché et à jour, y compris en partageant et en recevant des contributions techniques. Ces groupes de parties prenantes peuvent être des organisations de normalisation, des organismes d'évaluation de la conformité, des fournisseurs, des utilisateurs, des autorités publiques ou des associations professionnelles. Compte tenu des spécificités de chaque schéma, y compris des forums techniques et des industries qui s'y rapportent, il devrait être possible de recueillir des contributions techniques de différentes manières d'un schéma à l'autre. Pour certains schémas, l'ENISA devrait pouvoir s'appuyer sur un groupe de travail ad hoc réunissant des experts des administrations publiques des États membres, des entités de l'Union et du secteur privé. Les contributions techniques pourraient également provenir d'ISAC ou d'organismes de normalisation. L'ENISA devrait déterminer quel format est le plus adapté à chaque schéma et inclure une stratégie de maintenance dans chaque schéma candidat.

(91) Les schémas européens de certification de cybersécurité devraient s'appuyer sur des normes ou des spécifications techniques, notamment pour la définition des exigences de sécurité et des méthodes d'évaluation. L'ENISA devrait avoir la possibilité d'élaborer des spécifications techniques afin de faciliter l'élaboration et la maintenance des schémas, notamment en l'absence de publications d'organisations de normalisation ou lorsque ces publications ne sont pas appropriées pour atteindre les objectifs du schéma. Dans le cadre du processus d'élaboration, l'ENISA devrait recevoir le soutien du GECC et, le cas échéant, du groupe de travail ad hoc mis en place pour le schéma concerné. L'ENISA devrait également solliciter les contributions des groupes de parties prenantes. Elle devrait par ailleurs tenir compte de l'acceptation par le marché, ainsi que des normes européennes et internationales. Compte tenu de la qualité des spécifications techniques et des objectifs du schéma, la Commission devrait avoir la possibilité de faire référence aux spécifications techniques élaborées par l'ENISA dans un schéma européen de certification de cybersécurité.

(92) Les spécifications techniques élaborées par l'ENISA et mentionnées dans un schéma devraient être mises à disposition sur le site web de l'ENISA consacré aux schémas européens de certification de cybersécurité afin que toutes les parties intéressées puissent y accéder. Toutefois, dans certains cas spécifiques, la publication sur le site web pourrait présenter un risque pour la cybersécurité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou de la posture de cybersécurité des entités ayant fait l'objet d'une certification et, par extension, pour la sécurité publique. Par exemple, les spécifications techniques pourraient contenir des informations précises sur les nouveaux chemins d'attaque et si elles sont accessibles au public, elles pourraient être utilisées par des acteurs malveillants. Ce type d'informations devrait être diffusé de manière restreinte, sur la base du besoin d'en connaître, aux parties prenantes concernées, telles que les autorités nationales de certification de cybersécurité, les organismes d'évaluation de la conformité et les fournisseurs certifiés. En raison de leur diffusion restreinte, ces spécifications

techniques ne devraient pas être référencées dans les schémas européens de certification de cybersécurité et devraient donc être de nature non contraignante.

(93) Les schémas de certification de la posture de cybersécurité devraient être conçus de manière modulaire, en vue de permettre la démonstration de la conformité et la présomption de conformité avec les exigences pertinentes en matière de cybersécurité énoncées dans d'autres actes législatifs de l'Union, lorsque ces actes législatifs prévoient cette possibilité. La présomption de conformité aux exigences de ces actes juridiques ne prendra donc effet en tant que voie possible pour démontrer la conformité que si les actes juridiques concernés permettent une telle présomption de conformité. Les détails d'un tel schéma, à savoir sa finalité, ses objectifs ou ses éléments, différeront donc probablement de ceux d'autres schémas. En particulier, les schémas de certification de la posture de cybersécurité des entités devraient être élaborés de manière à permettre l'évaluation de la conformité continue d'une entité avec la législation de l'Union. Il n'est donc pas nécessaire que ces schémas couvrent tous les éléments d'un schéma européen de certification de cybersécurité, tels que les niveaux d'assurance, et cela devrait se refléter dans les règles qui leur sont applicables.

(94) Un cadre pour la certification de la posture de cybersécurité au sein de l'ECCF permet d'élaborer un schéma offrant aux entités qui fournissent des services dans plusieurs États membres la possibilité de démontrer qu'elles respectent les obligations en matière de gestion des risques de cybersécurité énoncées dans la directive 2022/2555 du Parlement européen et du Conseil. Ainsi, en ayant la capacité de démontrer leur conformité, les entités peuvent bénéficier d'approches prudentielles plus cohérentes et moins contraignantes dans l'ensemble du marché intérieur. L'élaboration d'un tel schéma de certification devrait être facilitée par l'adoption d'actes d'exécution au titre de la directive (UE) 2022/2555. Au moyen de profils d'extension, un schéma de certification de posture de cybersécurité permet de démontrer le respect des exigences lorsqu'un État membre a adopté ou maintenu des dispositions garantissant un niveau plus élevé de cybersécurité conformément à la directive (UE) 2022/2555. Une entité qui fournit des services dans plusieurs États membres peut ainsi démontrer sa conformité avec tous les profils d'extension pertinents au moyen d'un seul certificat de cybersécurité européen.

(95) Les objectifs et exigences de sécurité énoncés dans les schémas européens de certification de cybersécurité en ce qui concerne la sécurité des produits devraient être compatibles avec les exigences essentielles de cybersécurité énoncées à l'annexe I du règlement (UE) 2024/2847. Cette cohérence est nécessaire pour faire en sorte que les fabricants dont les produits relèvent du champ d'application du règlement (UE) 2024/2847 ne soient pas confrontés à des exigences contradictoires lorsqu'ils certifient leurs produits dans le cadre d'un schéma européen de certification de cybersécurité. En outre, des exigences cohérentes facilitent la présomption de conformité prévue à l'article 27 du règlement (UE) 2024/2847, en vertu de laquelle les fabricants de produits comportant des éléments numériques qui ont été certifiés dans le cadre d'un schéma européen de certification de cybersécurité peuvent bénéficier, sous certaines conditions, d'une présomption de conformité aux exigences essentielles de cybersécurité énoncées à l'annexe I dudit règlement.

(96) Dans le cadre du schéma européen de certification de cybersécurité, il devrait être possible de définir un profil d'extension, en fixant des exigences supplémentaires ou spécifiques pour les cas d'utilisation, y compris des capacités supplémentaires telles que des caractéristiques améliorées des produits, des offres de services ou des actifs spécialisés, des processus optimisés et des mesures de sécurité avancées. Étant donné

que les profils d'extension ne correspondent pas à un niveau d'assurance spécifique, leur finalité devrait être décrite de manière détaillée, en précisant les menaces de sécurité qu'ils couvrent. Les profils d'extension visent en particulier à démontrer la conformité avec des normes et exigences réglementaires spécifiques, y compris, le cas échéant, des exigences en matière de mesures supplémentaires de gestion des risques de cybersécurité établies par un État membre selon le principe d'harmonisation minimale conformément à la directive (UE) 2022/2555.

(97) Sans préjudice du système général d'examen par les pairs à mettre en place par toutes les autorités nationales de certification de cybersécurité au sein de l'ECCF, il devrait être possible d'inclure dans les schémas européens de certification de cybersécurité un mécanisme d'évaluation par les pairs pour les organismes qui délivrent des certificats de cybersécurité européens pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités, en particulier pour les organismes qui délivrent des certificats de niveau d'assurance «élevé» dans le cadre de ces schémas. Ces organismes devraient également inclure les organismes de certification des autorités nationales de certification de cybersécurité qui délivrent des certificats de niveau d'assurance «élevé». Le GECC devrait soutenir la mise en œuvre de ces mécanismes d'évaluation par les pairs. Les évaluations par les pairs devraient en particulier évaluer si les organismes concernés s'acquittent de leurs tâches de façon harmonisée, et peuvent comporter des mécanismes de recours.

(98) Les crises telles que les guerres, les catastrophes naturelles et les pandémies pourraient avoir une incidence négative sur les activités de certification. Dans des scénarios de crise d'une telle nature, il pourrait s'avérer impossible, par exemple, d'assurer la sécurité du site, en raison de la destruction des infrastructures, de cyberattaques, d'une indisponibilité de personnel ou d'une inaccessibilité du site. Un schéma européen de certification de cybersécurité devrait donc préciser les règles temporaires relatives à la continuité des activités de certification dans de tels scénarios.

(99) La traduction de schémas techniques candidats en actes d'exécution nécessite des connaissances techniques et juridiques complexes et peut engendrer une charge administrative importante. En outre, certains éléments des schémas européens de certification de cybersécurité, tels que la gestion des vulnérabilités ou les conditions dans lesquelles de telles marques ou de tels labels peuvent être utilisés, sont de nature transsectorielle et des dispositions de référence harmonisées pourraient leur être bénéfiques. Afin de garantir la qualité des schémas européens de certification de cybersécurité adoptés et de réduire la charge de mise en conformité pour les entreprises, la Commission devrait être habilitée à adopter des dispositions types couvrant certains éléments des schémas européens de certification de cybersécurité.

(100) Pour assurer la cohérence du cadre européen de certification de cybersécurité, il devrait être possible, dans le cadre d'un schéma européen de certification de cybersécurité, de préciser les niveaux d'assurance pour les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne délivrés dans le cadre de ce schéma. Un certificat de cybersécurité européen devrait faire référence à l'un des niveaux d'assurance suivants: «élémentaire», «substantiel» ou «élevé», tandis que la déclaration de conformité de l'UE ne devrait faire référence qu'au niveau d'assurance «élémentaire». Les niveaux d'assurance devraient fournir la rigueur et l'ampleur correspondantes de l'évaluation du produit TIC, du service TIC, du processus TIC, du service de sécurité géré ou de la posture de cybersécurité d'une entité et devraient être caractérisés par référence aux spécifications techniques, aux normes et aux procédures connexes, y compris les contrôles techniques, l'objectif

étant de réduire le risque d'incidents de cybersécurité ou de les prévenir. Chaque niveau d'assurance devrait être cohérent dans les différents domaines sectoriels dans lesquels la certification s'applique.

(101) Le choix de la certification appropriée et des exigences de sécurité associées par les utilisateurs de certificats de cybersécurité européens devrait être fondé sur une analyse des risques associés à l'utilisation des produits TIC, des services TIC, des processus TIC et des services de sécurité gérés ou sur le contexte de la certification des entités. Le niveau d'assurance devrait donc correspondre au niveau de risque associé à l'utilisation prévue du produit TIC, service TIC, processus TIC ou service de sécurité géré ou à l'environnement opérationnel et à la nature de l'entité dont la position de cybersécurité fait l'objet de la certification.

(102) Pour le niveau d'assurance «élémentaire», l'évaluation devrait être guidée au moins par les composants d'assurance suivants: l'évaluation devrait au moins comprendre un examen de la documentation technique du produit TIC, du service TIC, du processus TIC, du service de sécurité géré ou de la posture de cybersécurité d'une entité par l'organisme d'évaluation de la conformité. Lorsque la certification comprend des processus TIC, le processus utilisé pour concevoir, développer et maintenir un produit TIC, un service TIC, un service de sécurité géré ou une posture de cybersécurité d'une entité devrait également faire l'objet de l'examen technique. Lorsqu'un schéma européen de certification de cybersécurité prévoit une autoévaluation de la conformité, il devrait suffire que le fabricant ou le fournisseur de produits TIC, de services TIC, de processus TIC ou de services de sécurité gérés, ou l'entité dont la posture de cybersécurité est certifiée, ait procédé à une autoévaluation de la conformité du produit TIC, du service TIC, du processus TIC, du service de sécurité géré ou de la posture de cybersécurité de l'entité avec le schéma de certification.

(103) Pour le niveau d'assurance «substantiel», l'évaluation devrait au moins porter, en plus des exigences applicables au niveau d'assurance «élémentaire», sur la vérification de la conformité des fonctionnalités de sécurité du produit TIC, du service TIC, du processus TIC, du service de sécurité géré ou de la posture de cybersécurité de l'entité avec sa documentation technique.

(104) Pour le niveau d'assurance «élevé», l'évaluation devrait au moins porter sur, outre les exigences liées au niveau d'assurance «substantiel», un test d'efficacité évaluant la résistance des fonctionnalités de sécurité face à des cyberattaques élaborées lancées par des personnes aux aptitudes solides et aux ressources importantes. Les activités d'évaluation de la conformité devraient être réalisées dans l'Espace économique européen pour un niveau d'assurance «élevé» ou lorsqu'un schéma est conçu pour démontrer la conformité et prévoir une présomption de conformité avec d'autres actes législatifs de l'Union. Cette exigence est justifiée par le fait que les activités d'évaluation menées en dehors de l'Espace économique européen donnent lieu à des menaces supplémentaires pour la cybersécurité, en particulier pour la propriété intellectuelle des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou des entités faisant l'objet de l'évaluation. Par exemple, le code source d'un produit TIC pourrait être observé au moment où le produit franchit la frontière d'un pays tiers, ce qui constitue un risque pour la propriété intellectuelle. En outre, les laboratoires d'essai établis dans des pays tiers n'exercent pas leurs activités dans un environnement concerné par les mesures de cybersécurité imposées par la législation de l'Union, telles que la directive (UE) 2022/2555 ou le règlement (UE) 2024/2847. Ils peuvent, par exemple, faire appel à des prestataires tiers de services en nuage qui ne respectent pas les exigences de cybersécurité de la directive (UE)

2022/2555. Les schémas de certification devraient néanmoins être autorisés à prévoir des mécanismes de dérogation en ce qui concerne, par exemple, la certification des sites, ou dans d'autres cas où les activités d'évaluation de la conformité ne peuvent pas être raisonnablement réalisées dans l'Espace économique européen.

(105) Dans certains cas, il pourrait être nécessaire d'adopter différentes approches pour atteindre les objectifs de sécurité d'un niveau d'assurance donné afin de tenir compte des spécificités d'un produit TIC, d'un service TIC, d'un processus TIC, de services de sécurité gérés ou de la posture de cybersécurité d'entités. Afin de pouvoir appliquer une approche plus détaillée, il devrait être possible, dans un schéma européen de certification de cybersécurité, de spécifier un ou plusieurs niveaux d'évaluation correspondant à l'un des niveaux d'assurance. Cela permettra d'élaborer des schémas dans lesquels plusieurs niveaux d'évaluation conçus à des fins différentes correspondront au niveau de sécurité associé à un niveau d'assurance donné.

(106) Les schémas européens de certification de cybersécurité devraient pouvoir permettre la réalisation d'une évaluation de la conformité sous la seule responsabilité du fabricant ou du fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés, ou de l'entité dont la posture de cybersécurité est certifiée (ci-après l'«autoévaluation de la conformité»). Dans de tels cas, il devrait suffire que le fabricant, le fournisseur ou l'entité dont la posture de cybersécurité est certifiée effectue lui-même toutes les vérifications nécessaires pour s'assurer que les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité d'une entité sont conformes au schéma européen de certification de cybersécurité. L'autoévaluation de la conformité devrait être considérée comme appropriée pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou les postures de cybersécurité qui sont peu complexes, qui présentent un faible risque pour le public et dont les mécanismes de conception ou de production sont simples.

(107) Lorsqu'un schéma européen de certification de cybersécurité permet à la fois des autoévaluations de la conformité et des certifications de produits TIC, de services TIC, de processus TIC, de services de sécurité gérés ou de postures de cybersécurité d'entités, le schéma de certification devrait prévoir des moyens clairs et compréhensibles pour les consommateurs ou autres utilisateurs d'opérer une distinction entre les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou les postures de cybersécurité d'entités qui ont été autoévalués et ceux qui ont été certifiés par un tiers.

(108) Le fabricant ou le fournisseur de produits TIC, de services TIC, de processus TIC ou de services de sécurité gérés, ou les entités dont la posture de cybersécurité est certifiée, devraient pouvoir établir et signer la déclaration de conformité de l'UE dans le cadre de la procédure d'évaluation de la conformité. Une déclaration de conformité de l'UE est un document indiquant qu'un produit TIC, un service TIC, un processus TIC, un service de sécurité géré ou la posture de cybersécurité d'une entité est conforme aux exigences du schéma européen de certification de cybersécurité. En établissant et en signant la déclaration de conformité de l'UE, le fabricant ou le fournisseur de produits TIC, de services TIC, de processus TIC ou de services de sécurité gérés, ou l'entité dont la posture de cybersécurité est certifiée, assume la responsabilité de la conformité du produit TIC, du service TIC, du processus TIC, du service de sécurité géré ou de la posture de cybersécurité de l'entité avec les exigences de sécurité du schéma européen de certification de cybersécurité. Une copie de la

déclaration de conformité de l'Union européenne devrait être soumise à l'autorité nationale de certification de cybersécurité et à l'ENISA.

(109) Les fabricants ou fournisseurs de produits TIC, de services TIC, de processus TIC ou de services de sécurité gérés, ou les entités dont la posture de cybersécurité est certifiée, devraient mettre la déclaration de conformité de l'UE, la documentation technique et toutes les autres informations pertinentes relatives à la conformité avec un schéma européen de certification de cybersécurité à la disposition de l'autorité nationale de certification de cybersécurité compétente pendant une période spécifiée dans le schéma européen de certification de cybersécurité concerné et conformément à la législation de l'Union applicable. La documentation technique devrait préciser les exigences applicables au titre du schéma dans la mesure nécessaire à l'autoévaluation de la conformité. La documentation technique devrait être établie de manière à permettre d'évaluer si un produit TIC, un service TIC, un processus TIC ou un service de sécurité géré ou la posture de cybersécurité de l'entité est conforme aux exigences applicables au titre du schéma.

(110) Les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne devraient aider les utilisateurs à faire des choix éclairés. Les informations pertinentes devraient donc être publiées sur un site web géré par l'ENISA. En outre, les produits TIC, services TIC et processus TIC qui ont été certifiés ou pour lesquels une déclaration de conformité de l'Union européenne a été émise, devraient être accompagnés d'informations structurées, adaptées au niveau technique attendu de l'utilisateur auquel ils sont destinés. Tous les utilisateurs devraient avoir accès aux informations relatives au numéro de référence du schéma de certification, à l'autorité ou l'organisme émetteur et, le cas échéant, au niveau d'assurance ou devraient pouvoir obtenir une copie du certificat de cybersécurité européen. Ces informations devraient être actualisées régulièrement et être mises à disposition sur un site internet dédié aux schémas européens de certification de cybersécurité. En outre, afin de garantir une accessibilité continue, les fabricants et les fournisseurs devraient être tenus d'informer l'organisme de certification compétent de tout changement du lieu où se trouvent les informations en ligne ou, le cas échéant, les informations physiques.

(111) Une évaluation de la conformité est une procédure destinée à évaluer si les exigences spécifiées relatives à un produit TIC, un service TIC, un processus TIC, un service de sécurité géré ou une entité ont été respectées. Cette procédure est exécutée par un tiers indépendant qui n'est ni le fabricant ou le fournisseur des produits TIC, des services TIC, des processus TIC ou des services de sécurité gérés qui sont certifiés, ni l'entité dont la posture de cybersécurité est évaluée. Un certificat de cybersécurité européen devrait être délivré à la suite de l'évaluation concluante d'un produit TIC, d'un service TIC, d'un processus TIC, d'un service de sécurité géré ou de la posture de cybersécurité de l'entité. Il convient de considérer le certificat de cybersécurité européen comme une confirmation que l'évaluation a été dûment réalisée.

(112) Il est important d'observer une séparation stricte entre les activités de surveillance et de certification afin d'éviter les distorsions et les interférences susceptibles de survenir lorsque l'entité chargée de la surveillance du marché livre également concurrence sur le même marché. Par conséquent, les activités pour lesquelles les autorités nationales de certification de cybersécurité exercent simplement leur rôle de surveillance, par exemple en donnant leur approbation préalable à la délivrance d'un certificat, n'ont pas besoin d'être de nouveau séparées, en interne, des autres activités de surveillance. Il s'agit, par exemple, des situations dans lesquelles l'autorité nationale de certification de cybersécurité recueille activement des informations tout au long du processus de

certification mené par des organismes privés d'évaluation de la conformité et donne ensuite son avis sur la délivrance du certificat par ces organismes («modèle d'approbation préalable»).

(113) Les schémas européens de certification de cybersécurité devraient préciser les conditions dans lesquelles les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité d'une entité peuvent avoir besoin d'une nouvelle certification ou dans lesquelles il peut être nécessaire de réduire le champ d'application d'un certificat de cybersécurité européen spécifique. En outre, les schémas européens de certification de cybersécurité devraient tenir compte de tout effet négatif éventuel, sur la conformité avec les exigences de sécurité de ce certificat, de vulnérabilités ou de non-conformités détectées ultérieurement concernant le produit TIC, le service TIC, le processus TIC, le service de sécurité géré ou la posture de cybersécurité d'une entité ayant fait l'objet une certification.

(114) L'harmonisation joue un rôle crucial pour garantir une cybersécurité solide et améliorer l'accès des entreprises au marché. En revanche, la fragmentation et l'absence de reconnaissance mutuelle des certificats constituent des obstacles importants à la fluidité des flux de données, ce qui augmente les coûts opérationnels pour l'industrie de l'Union. Pour atténuer ces difficultés, il est essentiel d'éviter la fragmentation du champ d'application des contrôles de sécurité et des méthodes d'évaluation de la conformité dans l'ensemble de l'Union.

(115) Les États membres devraient informer la Commission et le GECC suffisamment à l'avance avant d'adopter un nouveau schéma national de certification de cybersécurité pour des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou la posture de cybersécurité d'entités afin de les aider à évaluer l'incidence de ce nouveau schéma sur le bon fonctionnement du marché intérieur, à la lumière de tout intérêt stratégique à demander un schéma européen de certification de cybersécurité.

(116) Les références faites dans la législation nationale à des normes nationales qui ont cessé de produire leurs effets en raison de l'entrée en vigueur d'un schéma européen de certification de cybersécurité peuvent être une source de confusion. Dès lors, le cas échéant, les États membres devraient tenir compte, dans leur législation nationale, de l'adoption d'un schéma européen de certification de cybersécurité.

(117) Afin de faciliter la croissance d'un marché intérieur fiable, tout en créant des partenariats avec des pays tiers, le processus de certification établi dans l'ECCF devrait être mis en œuvre d'une manière qui facilite la reconnaissance internationale, la reconnaissance mutuelle et l'alignement sur les normes internationales.

(118) Pour faciliter encore davantage les échanges, et compte tenu du fait que les chaînes d'approvisionnement des TIC sont mondiales, des accords de reconnaissance mutuelle concernant les certificats de cybersécurité européens peuvent être conclus par l'Union conformément à l'article 218 TFUE. La Commission devrait être habilitée à adopter des actes d'exécution pour reconnaître unilatéralement l'équivalence de certificats de pays tiers avec les certificats de cybersécurité européens. Il devrait être possible de prévoir des conditions spécifiques pour cette reconnaissance de certificats de pays tiers.

(119) Pour parvenir à une mise en œuvre équivalente du cadre dans toute l'Union, faciliter la reconnaissance mutuelle et favoriser l'acceptation globale des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne, il est nécessaire de mettre en place un système d'examen par les pairs entre les autorités

nationales de certification de cybersécurité. L'examen par les pairs devrait couvrir les procédures de contrôle de la conformité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés et de la posture de cybersécurité des entités avec les certificats de cybersécurité européens, de surveillance du respect des obligations des fabricants ou des fournisseurs de produits TIC, de services TIC, de processus TIC, de services de sécurité gérés et d'entités certifiées qui procèdent à une autoévaluation de la conformité, et de surveillance des organismes d'évaluation de la conformité ainsi que de l'adéquation des compétences du personnel des organismes qui délivrent les certificats pour les niveaux d'assurance dits «élevés». L'ENISA devrait participer aux examens par les pairs en qualité d'observateur et soutenir l'organisation du mécanisme d'examen par les pairs et des examens par les pairs, y compris en élaborant des documents d'orientation et des modèles pertinents, en coopération avec la Commission et le GECC. L'ENISA devrait également mettre à la disposition du public, sur son site web consacré aux schémas européens de certification de cybersécurité, les informations relatives au programme d'examens par les pairs et à la liste des autorités nationales de certification de cybersécurité évaluées par les pairs qui doivent mettre en œuvre ce programme. Le règlement d'exécution (UE) 2025/2540 de la Commission[60], adopté en vertu du règlement (UE) 2019/881, établit le plan pour l'examen par les pairs qui est utilisé par les schémas européens de certification de cybersécurité adoptés. Il est nécessaire de veiller à ce que les examens par les pairs se poursuivent. Néanmoins, la Commission devrait pouvoir, par voie d'actes d'exécution, lorsque cela est nécessaire, établir un nouveau plan pour les examens par les pairs d'une durée d'au moins cinq ans et fixer les critères et les méthodes de fonctionnement du système d'examen par les pairs.

(120) Une fois qu'un schéma européen de certification de cybersécurité a été adopté, les fabricants ou les fournisseurs de produits TIC, de services TIC, de processus TIC et de services de sécurité gérés ou les entités dont la posture de cybersécurité fait l'objet d'une certification devraient être en mesure de soumettre des demandes de certification de leurs produits TIC, de leurs services TIC, de leurs processus TIC, de leurs services de sécurité gérés ou de leur posture de cybersécurité à l'organisme d'évaluation de la conformité de leur choix établi où que ce soit dans l'Union. Les organismes d'évaluation de la conformité devraient être accrédités par un organisme national d'accréditation s'ils satisfont aux exigences énoncées dans le présent règlement et, le cas échéant, aux exigences spécifiées par la Commission conformément au présent règlement. Le système défini dans le présent règlement devrait être complété par le système d'accréditation prévu dans le règlement (CE) nº 765/2008 du Parlement européen et du Conseil[61].

(121) Les organismes d'évaluation de la conformité qui ont été accrédités ou notifiés en vertu de la législation existante de l'Union, notamment du règlement (UE) 2024/2847 ou du règlement d'exécution (UE) 2024/482, pourraient posséder des compétences pertinentes pour les schémas européens de certification de cybersécurité nouvellement

---

60 Règlement d'exécution (UE) 2025/2540 de la Commission du 9 décembre 2025 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'établissement du plan pour l'examen par les pairs (JO L 2023/2540, 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).

61 Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

adoptés. Afin d'éviter toute charge financière et administrative inutile, il convient de créer des synergies pour l'accréditation des organismes d'évaluation de la conformité au titre du présent règlement. C'est pourquoi les exigences en matière d'accréditation des schémas devraient être établies de manière à être aussi alignées que possible sur les exigences relatives aux organismes notifiés énoncées dans le règlement (UE) 2024/2847 et sur les exigences en matière d'accréditation prévues par le règlement d'exécution (UE) 2024/482. En outre, les organismes d'évaluation de la conformité qui font l'objet d'une procédure d'accréditation au titre du présent règlement devraient pouvoir se fonder sur leurs précédents résultats d'évaluation de leurs compétences au titre d'autres actes législatifs de l'Union, en cas de chevauchement des exigences en matière d'accréditation.

(122) En vue de faciliter l'harmonisation des services d'évaluation de la conformité dans l'ensemble de l'Union, il devrait être possible d'établir dans un schéma européen de certification de cybersécurité des exigences supplémentaires ou spécifiques pour les organismes d'évaluation de la conformité. Dans le contexte de la certification, une autorisation devrait s'entendre comme une décision d'une autorité nationale de certification de cybersécurité selon laquelle un organisme d'évaluation de la conformité satisfait aux exigences spécifiques ou supplémentaires énoncées dans un schéma européen de certification de cybersécurité pour mener une activité spécifique d'évaluation de la conformité.

(123) Lorsqu'un schéma européen de certification de cybersécurité fixe des exigences supplémentaires ou spécifiques en application du présent règlement, les organismes d'évaluation de la conformité devraient être autorisés par les autorités nationales de certification de cybersécurité à effectuer les tâches prévues dans le cadre de ce schéma. Afin d'éviter toute autorisation multiple, de favoriser l'acceptation et la reconnaissance des décisions d'autorisation et d'exercer une supervision efficace des organismes d'évaluation de la conformité autorisés, les organismes d'évaluation de la conformité devraient solliciter une autorisation auprès de l'autorité nationale de certification de cybersécurité de l'État membre où ils ont leur siège. Toutefois, il convient de veiller à ce qu'un organisme d'évaluation de la conformité puisse demander une autorisation dans un autre État membre lorsqu'il n'existe pas d'autorité nationale de certification de cybersécurité dans son propre État membre ou lorsqu'une telle autorité existe, mais n'est pas compétente pour fournir les services d'autorisation requis. Dans ces cas-là, il y a lieu de mettre en place une coopération et un échange d'informations appropriés entre les autorités nationales de certification de cybersécurité. La Commission devrait être habilitée à adopter des actes d'exécution établissant les procédures d'autorisation, y compris pour la coopération transfrontière en matière d'autorisation.

(124) Afin de préserver le niveau de protection requis pour un produit TIC, un service TIC, un processus TIC, un service de sécurité géré ou la posture de cybersécurité d'une entité, il est primordial que les sous-traitants et les filiales qui réalisent l'évaluation de la conformité soient tenus de respecter les mêmes exigences que les organismes d'évaluation de la conformité qui ont fait l'objet d'une notification pour ce qui est de la réalisation des tâches d'évaluation de la conformité. Les organismes d'évaluation de la conformité devraient par conséquent disposer des compétences appropriées et être en mesure de vérifier que leurs sous-traitants satisfont aux exigences applicables.

(125) La mesure dans laquelle l'organisme d'évaluation de la conformité souhaite faire appel à des sous-traitants établis en dehors de l'Union ou recourir à du personnel ou à des installations situés en dehors de l'État membre de notification devrait être évaluée

de manière appropriée par l'autorité notifiante. L'autorité publique d'un État membre devrait avoir la possibilité de décider qu'elle ne peut assumer l'entière responsabilité d'un tel accord en tant qu'autorité nationale de certification de cybersécurité, et de retirer la notification ou en limiter le champ d'application.

(126) Afin d'évaluer les exigences de cybersécurité applicables aux produits TIC, aux services TIC, aux processus TIC, aux services de sécurité gérés ou à la posture de cybersécurité des entités, les autorités nationales de certification de cybersécurité devraient notifier les organismes d'évaluation de la conformité accrédités à la Commission et aux autres États membres. La notification d'organismes d'évaluation de la conformité accrédités et, le cas échéant, autorisés indique que ces organismes sont considérés comme fiables pour réaliser des activités d'évaluation et de certification conformément au présent règlement, contribuant ainsi à asseoir la réputation globale de la certification de cybersécurité européenne. Il est donc essentiel de veiller à ce que les organismes d'évaluation de la conformité qui ont été notifiés continuent à satisfaire aux exigences imposées et à remplir leurs obligations dans le temps et à ce que la liste des organismes d'évaluation de la conformité notifiés soit tenue à jour.

(127) Le règlement d'exécution (UE) 2024/3143 de la Commission[62], adopté en vertu du règlement (UE) 2019/881, établit les circonstances, formats et procédures pour les notifications des organismes d'évaluation de la conformité qui sont utilisés par les schémas européens de certification de cybersécurité adoptés. Il est donc nécessaire de veiller à ce que les activités de notification se poursuivent. Néanmoins, la Commission devrait être habilitée à adopter des actes d'exécution afin d'adapter ces circonstances, formats et procédures pour la notification des organismes d'évaluation de la conformité. Dans ce contexte, la Commission devrait s'appuyer sur l'expérience acquise dans le cadre des schémas existants et s'efforcer de s'aligner sur les autres législations et cadres pertinents de l'Union, en particulier le règlement (UE) 2024/2847 et le nouveau cadre législatif, en vue de réduire la charge que représente la mise en conformité pour les organismes d'évaluation de la conformité actifs au titre de différents instruments juridiques.

(128) Les chaînes d'approvisionnement des technologies de l'information et de la communication (TIC) se composent d'un ensemble de ressources et de processus interconnectés entre les opérateurs économiques. Les chaînes d'approvisionnement des TIC jouent un rôle crucial pour maintenir la stabilité de la société et stimuler l'activité économique dans l'ensemble de l'Union. Elles jouent également un rôle essentiel dans la mise en place des infrastructures numériques dans l'Union et soutiennent le fonctionnement de la société et de l'économie de l'Union. Les chaînes d'approvisionnement des TIC permettent la fabrication, la production, la distribution et la maintenance de services TIC, de systèmes TIC et de produits TIC nécessaires à divers secteurs critiques et hautement critiques, dont les soins de santé, la finance, les transports, les télécommunications, l'énergie et les douanes. La sécurité des chaînes d'approvisionnement des TIC de ces secteurs critiques peut également avoir une

---

62 Règlement d'exécution (UE) 2024/3143 de la Commission du 18 décembre 2024 établissant les circonstances, formats et procédures pour les notifications en application de l'article 61, paragraphe 5, du règlement (UE) 2019/881 du Parlement européen et du Conseil relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications (JO L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

incidence sur la sécurité des infrastructures militaires et de défense, lorsque ces infrastructures dépendent de secteurs critiques civils et de leurs chaînes d'approvisionnement des TIC. Toutefois, selon le rapport sur le panorama des menaces de cybersécurité publié par l'ENISA (ENISA Threat Landscape 2025)[63], les attaques contre les chaînes d'approvisionnement comptent parmi les cinq principales menaces pour la cybersécurité, ce qui montre que les auteurs d'attaques exploitent activement des vecteurs d'attaque indirects tels que des fournisseurs tiers et des dépendances. Les perturbations des chaînes d'approvisionnement des TIC peuvent nuire à la poursuite des activités économiques sur le marché intérieur, entraîner des pertes financières, entamer la confiance des utilisateurs et causer un préjudice majeur à l'économie et la société de l'Union. La préparation à la cybersécurité et l'effectivité de la cybersécurité sont dès lors plus essentielles que jamais pour le bon fonctionnement du marché intérieur.

(129) Au-delà des risques techniques couverts par la directive (UE) 2022/55 du Parlement européen et du Conseil[64], le règlement (UE) 2024/2847 du Parlement européen et du Conseil[65] et le cadre européen de certification de cybersécurité établi par le règlement (UE) 2019/881, les chaînes d'approvisionnement des TIC sont de plus en plus exposées à des risques de nature non technique. Ces risques non techniques peuvent être liés, sans pour autant s'y limiter, à la juridiction à laquelle est soumis un fournisseur de certains composants, en particulier lorsqu'un pays tiers ou des acteurs de la menace contrôlés depuis ce pays se livrent à des activités d'espionnage économique ou mènent des actes ou des campagnes de cybermalveillance contre l'Union ou ses États membres, ou lorsque l'État se livre à un comportement irresponsable dans le cyberespace. Les risques non techniques peuvent également être liés à des vulnérabilités dissimulées, à des portes dérobées ou à d'éventuelles ruptures d'approvisionnement systémiques, en particulier en cas de verrouillage technologique ou de dépendance à l'égard de fournisseurs. Par exemple, des coupe-circuits pourraient être utilisés pour nuire à la disponibilité des réseaux de communication et des réseaux électriques.

(130) La communication conjointe sur le renforcement de la sécurité économique de l'UE[66] a souligné le risque que des pays tiers aient accès aux informations et données sensibles de l'Union ou de ses États membres, par le biais de l'espionnage industriel, de la fourniture de matériel ou de logiciels utilisés dans certains produits ou par le biais des liens de propriété et de contrôle de certaines entreprises détenant des informations et données sensibles. Elle a également souligné le risque que les infrastructures critiques de l'Union – y compris les infrastructures critiques dans les domaines des transports, des systèmes spatiaux, de l'énergie et des communications,

63 ENISA Threat Landscape 2025, octobre 2025.

64 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: https://eur-lex.europa.eu/eli/dir/2022/2555/oj).

65 Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) no 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng).

66 Communication conjointe au Parlement européen et au Conseil, «Renforcer la sécurité économique de l'UE», 3 décembre 2025, JOIN(2025) 977 final.

en particulier celles qui sont considérées comme stratégiques pour la mobilité militaire – pourraient être perturbées par des acteurs étrangers, ce qui pourrait avoir des effets en cascade sur l'économie de l'Union. Ces perturbations pourraient survenir à la suite d'attaques physiques, informatiques ou hybrides, y compris le sabotage d'installations entières ou de certains de leurs composants ou éléments. Elles pourraient également affecter les chaînes d'approvisionnement des TIC, qui sous-tendent des éléments ou services critiques pour les infrastructures essentielles.

(131) En réponse aux défis que posent les risques non techniques pour la sécurité de la chaîne d'approvisionnement des TIC, certains États membres ont pris des mesures réglementaires, y compris la désignation de fournisseurs à haut risque, tandis que d'autres États membres pourraient leur emboîter le pas. Cela risque de conduire à de nouvelles divergences dans les approches nationales et, en fin de compte, à une vulnérabilité accrue de certains États membres, ce qui pourrait avoir des retombées dans l'ensemble de l'Union. Par conséquent, il est nécessaire d'harmoniser certains aspects liés aux risques non techniques de cybersécurité pour la chaîne d'approvisionnement des TIC. Une telle intervention au niveau de l'Union est également justifiée compte tenu de la nécessité de garantir un niveau élevé de cybersécurité dans l'ensemble de l'Union. Les dispositions relatives à la sécurité de la chaîne d'approvisionnement des TIC visent à supprimer ces divergences importantes entre les États membres, notamment en établissant des règles pour les mécanismes d'évaluation des risques liés à la sécurité de la chaîne d'approvisionnement des TIC au niveau de l'Union et des normes minimales de protection contre les risques liés à la chaîne d'approvisionnement des TIC.

(132) Afin de réduire les dépendances et les vulnérabilités critiques, il est nécessaire d'établir un cadre fiable pour les chaînes d'approvisionnement des TIC, qui tiendrait compte des risques non techniques liés aux fournisseurs à haut risque et aux dépendances dans les secteurs hautement critiques et dans d'autres secteurs critiques. Par conséquent, il est nécessaire de fournir un cadre objectif, fondé sur les risques, à l'épreuve du temps et neutre sur le plan technologique au niveau de l'Union, d'identifier les actifs de TIC essentiels et de prévoir un ensemble de mesures d'atténuation proportionnées pour faire face aux risques.

(133) Des risques de cybersécurité, y compris des risques liés à la dépendance à l'égard de fournisseurs à haut risque, peuvent être observés dans plusieurs chaînes d'approvisionnement des TIC critiques dans l'Union, notamment celles des équipements de détection, des véhicules connectés et automatisés, des systèmes d'approvisionnement en électricité et du stockage de l'électricité, des systèmes d'approvisionnement en eau, des drones et systèmes antidrones, des services d'informatique en nuage, des dispositifs médicaux, des équipements de surveillance, des services spatiaux et des semi-conducteurs. Par exemple, les vulnérabilités des équipements de détection de sécurité pourraient permettre à des acteurs malveillants d'accéder aux systèmes TIC afin de manipuler les scanners de telle sorte que des articles interdits puissent passer le point de contrôle de sécurité sans être détectés, ce qui pourrait avoir des conséquences catastrophiques.

(134) Le présent règlement ne fait pas obstacle à l'adoption ou au maintien par les États membres de dispositions assurant un niveau plus élevé de cybersécurité en ce qui concerne la sécurité des chaînes d'approvisionnement des TIC, à condition que ces dispositions soient compatibles avec les obligations des États membres prévues par le droit de l'Union. Ces dispositions peuvent inclure, par exemple, l'imposition de mesures d'atténuation plus strictes en ce qui concerne les actifs de TIC essentiels.

(135) Afin de recenser les risques potentiels en matière de cybersécurité affectant certaines chaînes d'approvisionnement des TIC, le groupe de coopération institué par l'article 14 de la directive (UE) 2022/2555 (ci-après le «groupe de coopération SRI») peut évaluer certaines chaînes d'approvisionnement des TIC au moyen d'évaluations coordonnées au niveau de l'Union des risques pour la sécurité. Les évaluations coordonnées au niveau de l'Union des risques pour la sécurité devraient porter, entre autres, sur les principaux acteurs de la menace, ainsi que sur les principales menaces et vulnérabilités touchant les actifs de TIC essentiels. Les évaluations coordonnées au niveau de l'Union des risques pour la sécurité devraient établir une liste de scénarios de risque et une liste de mesures visant à atténuer les risques. Les évaluations coordonnées au niveau de l'Union des risques pour la sécurité devraient être achevées dans un délai de six mois. En cas d'urgence particulière, il devrait être possible de raccourcir les délais.

(136) Lorsque la Commission a des raisons suffisantes de croire qu'il existe une cybermenace importante pour la sécurité de l'Union liée aux chaînes d'approvisionnement critiques des TIC et qu'une action pourrait être nécessaire pour préserver le bon fonctionnement du marché intérieur, elle devrait consulter sans tarder les États membres sur la nécessité de mesures d'atténuation et procéder à une évaluation des risques pour la sécurité, en tenant compte de la consultation des États membres.

(137) Lorsque, à la suite d'une évaluation des risques pour la sécurité réalisée par le groupe de coopération SRI ou la Commission, il apparaît qu'un pays tiers donné présente des risques non techniques graves et structurels en matière de cybersécurité pour les chaînes d'approvisionnement des TIC, la Commission devrait vérifier la menace que représente ce pays. Elle peut également lancer une telle vérification en s'appuyant sur d'autres sources, telles qu'une déclaration publique au nom de l'Union ou d'un État membre en réponse à des cas de comportement irresponsable d'un État dans le cyberespace ayant entraîné un incident de cybersécurité. Afin d'évaluer le niveau de menace, la Commission devrait tenir compte d'éléments tels que l'existence de lois ou de pratiques dans le pays tiers qui imposent aux entités relevant de leur juridiction de communiquer aux autorités de ce pays tiers des informations sur les vulnérabilités logicielles ou matérielles avant que ces vulnérabilités soient réputées avoir été exploitées. Un autre élément important est l'absence de recours juridictionnels effectifs et de mécanismes de contrôle indépendants et démocratiques susceptibles de remédier aux préoccupations en matière de sécurité, y compris en ce qui concerne les pratiques existantes, les informations étayées sur les incidents impliquant des acteurs de la menace opérant hors du territoire de ce pays et menant des actes ou des campagnes de cybermalveillance et le manque de capacité ou de volonté du pays tiers de coopérer avec la Commission ou les États membres pour faire face au risque découlant des activités de ces acteurs de la menace. La Commission devrait également tenir compte des informations provenant des évaluations coordonnées au niveau de l'Union des risques pour la sécurité ou des rapports publiés par les États membres ou des organisations internationales telles que l'OTAN.

(138) Aux fins du présent règlement, la notion de contrôle devrait s'entendre comme la capacité d'exercer une influence déterminante sur une entité juridique, directement ou indirectement via une ou plusieurs entités juridiques intermédiaires. Il convient également de déterminer le contrôle exercé sur les entités d'un pays tiers suscitant des préoccupations en matière de cybersécurité lorsque ces entités possèdent des structures de gestion exécutive dans ce pays.

(139) L'Union ne devrait pas financer de projets impliquant des fournisseurs à haut risque, qui compromettraient la sécurité de l'Union et porteraient atteinte à ses intérêts et à sa crédibilité. Les fournisseurs à haut risque recensés au titre du présent règlement ne devraient donc pas être autorisés à participer à des programmes et instruments de financement de l'Union mis en œuvre en gestion directe et indirecte conformément à l'article 136 du règlement (UE/Euratom) 2024/2509 et aux réglementations sectorielles pertinentes de l'Union, ni à des activités de financement de l'Union mises en œuvre en gestion partagée, y compris au titre du prochain cadre financier pluriannuel en ce qui concerne la fourniture de composants TIC ou de composants comprenant des composants TIC à utiliser dans des actifs de TIC essentiels identifiés. Les partenaires de l'Union chargés de la mise en œuvre, tels que le Groupe Banque européenne d'investissement et les banques et institutions nationales de développement, devraient s'abstenir de soutenir des projets qui contredisent ce qui précède, y compris dans le cadre d'opérations à leurs propres risques.

(140) Les marchés publics peuvent constituer un outil puissant permettant aux pouvoirs publics de contribuer à une économie plus innovante, plus durable et plus compétitive et de dépenser l'argent public de manière stratégique. Les marchés publics liés aux chaînes d'approvisionnement des TIC ne devraient pas être utilisés au profit de fournisseurs qui menacent la sécurité des infrastructures critiques de l'Union. Les fournisseurs à haut risque recensés au titre du présent règlement ne devraient donc pas être autorisés à participer à des marchés publics concernant la fourniture de composants TIC ou de composants qui incluent des composants TIC destinés à être utilisés dans des actifs de TIC essentiels identifiés en tant que tels.

(141) La certification de cybersécurité joue un rôle dans le renforcement de la sécurité globale et la lutte contre les cybermenaces, en servant de référence de confiance. Cette confiance pourrait être érodée si les attestations de compétences en matière de cybersécurité étaient délivrées par des fournisseurs à haut risque. Ces derniers ne devraient donc pas être autorisés à demander à devenir des fournisseurs agréés d'attestations individuelles européennes des compétences en matière de cybersécurité. Dans le même ordre d'idées, il convient également d'empêcher les fournisseurs à haut risque d'obtenir une certification de cybersécurité dans le cadre de l'ECCF et de devenir des organismes d'évaluation de la conformité accrédités habilités à délivrer de tels certificats.

(142) Les normes de cybersécurité jouent un rôle essentiel dans la sécurité et la fiabilité des infrastructures numériques. Il est nécessaire de prendre des mesures appropriées pour assurer la normalisation dans le domaine de la cybersécurité. La participation d'entités établies dans des pays dont il a été établi qu'ils suscitaient des préoccupations en matière de cybersécurité pour les chaînes d'approvisionnement des TIC conformément au présent règlement ou contrôlées depuis de tels pays peut conduire à influencer les normes de cybersécurité d'une manière qui compromet leur sécurité et leur fiabilité.

(143) Sur la base des résultats des évaluations des risques pour la sécurité, la Commission peut déterminer, au moyen d'actes d'exécution, quels actifs de TIC devraient être considérés comme des actifs de TIC essentiels en raison de leur importance critique et sous réserve de mesures d'atténuation spécifiques. La simple existence de la possibilité d'une connectivité de l'actif devrait être suffisante pour tenir compte du risque qu'il pose pour la cybersécurité.

(144) Lorsque cela est nécessaire pour garantir un niveau élevé de cybersécurité, de cyberrésilience et de confiance au sein de l'Union, les mesures d'atténuation peuvent

être appliquées aux entités en ce qui concerne leur chaîne d'approvisionnement des TIC et, en particulier, aux actifs de TIC essentiels identifiés en tant que tels. Les mesures d'atténuation proposées devraient être fondées sur l'évaluation des risques et dépendances potentiels, y compris sur l'incidence économique et sociétale potentielle de ces mesures sur les entités concernées opérant dans des secteurs hautement critiques ou dans d'autres secteurs critiques, en particulier les PME. L'évaluation de l'incidence économique devrait porter sur les coûts de la mise en œuvre des mesures d'atténuation, y compris sur la durée du cycle de vie des composants concernés dans les actifs de TIC essentiels, lorsque les mesures comprennent le remplacement de fournisseurs. La disponibilité d'autres fournisseurs sur le marché devrait également être évaluée afin de garantir la continuité de la fourniture des services.

(145) Étant donné que les mesures d'atténuation pourraient avoir un effet restrictif sur le commerce international de biens et de services, elles devraient être proportionnées et ciblées afin de poursuivre l'objectif légitime consistant à garantir la cybersécurité des chaînes d'approvisionnement des TIC en ce qui concerne les entités du type visé aux annexes I et II de la directive (UE) 2022/2555, conformément aux obligations internationales de l'Union.

(146) L'utilisation, l'installation ou tout autre type d'intégration de composants provenant de fournisseurs à haut risque dans le cadre de l'exploitation d'actifs de TIC essentiels peut entraîner des risques de transferts ultérieurs de données vers un pays tiers. En particulier, des risques peuvent apparaître lorsque le niveau de protection offert aux données dans le pays tiers est insuffisant, par exemple en ce qui concerne la protection des droits fondamentaux, de la propriété intellectuelle ou des secrets d'affaires, ou lorsque ces données sont consultées et exploitées illégalement en vue d'éventuelles perturbations futures de la chaîne d'approvisionnement et à des fins d'espionnage. Pour atténuer ces risques, des restrictions peuvent être appliquées concernant le transfert de certains types de données vers des pays tiers.

(147) Le manque de diversité des équipements utilisés par les entités du type visé aux annexes I et II de la directive (UE) 2022/2555 engendre d'importantes vulnérabilités. La dépendance à l'égard d'un seul fournisseur crée une dépendance à l'égard d'équipements ou de solutions spécifiques. Le manque de diversité des fournisseurs accroît la vulnérabilité globale des infrastructures critiques, en particulier si les entités se procurent leurs composants TIC utilisés dans des actifs de TIC sensibles auprès d'un fournisseur présentant un degré élevé de risque. La dépendance a également une incidence significative sur la résilience au niveau national et à l'échelle de l'Union et crée des points uniques de défaillance. Pour atténuer ces risques, il pourrait être imposé d'avoir plusieurs fournisseurs pour certains actifs de TIC essentiels spécifiques.

(148) Les entités de l'Union peuvent également utiliser des actifs essentiels tels que définis par le présent règlement. Par conséquent, les règles énoncées dans le présent règlement concernant la sécurité des chaînes d'approvisionnement des TIC devraient également leur être applicables. Afin de veiller à ce que la spécificité des entités de l'Union soit prise en considération, il est important de tenir compte des risques non techniques découlant des chaînes d'approvisionnement des TIC en ce qui concerne les entités de l'Union lors de la réalisation d'évaluations coordonnées au niveau de l'Union des risques pour la sécurité.

(149) Dans des circonstances exceptionnelles qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur et lorsqu'il existe des éléments de

preuve clairs donnant à la Commission des raisons suffisantes de considérer que l'utilisation de composants TIC ou de composants qui comprennent des composants TIC provenant d'un fournisseur spécifique représente une menace de cybersécurité importante pour les activités économiques ou sociétales d'au moins trois États membres, la Commission peut proposer, en étroite concertation avec les États membres, d'interdire l'utilisation, l'installation ou l'intégration de ces composants provenant du fournisseur concerné par des entités d'un type visé aux annexes I et II de la directive (UE) 2022/2555.

(150) Afin de garantir la proportionnalité des mesures appliquées, les entités établies dans un pays tiers suscitant des préoccupations en matière de cybersécurité et désigné comme tel conformément au présent règlement, ou qui sont contrôlées par un tel pays tiers, par une entité établie dans un tel pays tiers ou par un ressortissant d'un tel pays tiers peuvent demander à être exemptées de l'interdiction de fournir aux entités d'un type visé aux annexes I et II de la directive (UE) 2022/2555 des composants TIC ou des composants comprenant des composants TIC en vue de leur utilisation, de leur installation ou de leur intégration dans des actifs de TIC essentiels de cette entité et de participer à des procédures de passation de marchés publics organisées conformément à la législation transposant les directives 2014/24/UE[67] et 2014/25/UE du Parlement européen et du Conseil[68] en ce qui concerne la fourniture de composants TIC ou de composants comprenant des composants TIC destinés à être utilisés dans des actifs de TIC essentiels déterminés. À cette fin, l'entité devrait démontrer clairement qu'elle applique des mesures efficaces pour faire face aux risques non techniques et garantir l'absence de toute ingérence indue éventuelle de la part d'un pays tiers suscitant des préoccupations en matière de cybersécurité.

(151) Les réseaux de communications électroniques constituent la cheville ouvrière d'un large éventail de services essentiels au fonctionnement du marché intérieur et au maintien et à l'exercice de fonctions sociétales et économiques vitales, dans les domaines de l'énergie, des transports, de la banque, de la santé et de la défense, ainsi que des systèmes de commande industriels, par exemple. Par conséquent, ces réseaux hautement critiques sont des cibles attrayantes pour tous les types de cyberattaques et de menaces hybrides, pour les perturbations, l'espionnage et la collecte de renseignements, ainsi que pour la fraude et la criminalité financière. L'évaluation effectuée par le groupe de coopération SRI concernant les risques pesant sur la cybersécurité et la résilience des infrastructures et réseaux de communication européens a mis en évidence un certain nombre de risques et de menaces d'importance stratégique du point de vue de l'Union, tels que les logiciels malveillants d'effacement de données/rançongiciels, les attaques, les attaques de la chaîne d'approvisionnement, les intrusions dans les réseaux et les attaques collectives par saturation de service (ACSS).

(152) Compte tenu de l'interconnexion et de l'interdépendance entre les différents réseaux nationaux de communications électroniques, il est nécessaire que tous les États

---

67 Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65, ELI: https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng).

68 Directive 2014/25/UE du Parlement européen et du Conseil du 26 février 2014 relative à la passation de marchés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et des services postaux et abrogeant la directive 2004/17/CE (JO L 94 du 28.3.2014, p. 243, ELI: https://eur-lex.europa.eu/eli/dir/2014/25/oj?locale=fr).

membres prennent les mesures appropriées pour assurer la sécurité de leurs réseaux. Pour les mêmes raisons, il est nécessaire de mettre en place un cadre juridique efficace au niveau de l'Union qui tienne également compte des risques non techniques et garantisse la sécurité des réseaux de communications électroniques interconnectés de manière globale.

(153) En particulier, la cybersécurité des réseaux 5G revêt une importance stratégique pour l'Union, étant donné que ces réseaux constituent l'épine dorsale d'un large éventail de services essentiels au fonctionnement du marché intérieur et qu'ils jouent également un rôle crucial dans notre préparation en matière de défense, y compris en ce qui concerne la mobilité militaire. Les réseaux 5G sont capables de fournir une connectivité ultrarapide fiable, par exemple pour le partage de données et d'informations, la détection de drones et la coordination en temps réel sur le champ de bataille.

(154) La 5G est principalement déployée sous la forme de réseaux non autonomes, pour lesquels seul le réseau d'accès radio est en technologie 5G, tandis que les autres fonctionnalités de réseau continueront à reposer sur les cœurs de réseaux 4G existants. Les réseaux 5G non autonomes s'appuient principalement sur les infrastructures déjà en place, ce qui signifie que la sécurité des futurs réseaux 5G est, dans une certaine mesure, déterminée par les équipements de réseau déjà en place ainsi que par leur configuration. Par conséquent, les mesures d'atténuation devraient également couvrir les réseaux 4G sur lesquels repose le déploiement de la 5G.

(155) Afin de relever d'importants défis en matière de sécurité dans les réseaux 5G, les États membres réunis au sein du groupe de coopération SRI, en collaboration avec la Commission et l'ENISA, ont procédé à une évaluation coordonnée au niveau de l'Union des risques pour la sécurité des réseaux 5G, en examinant à la fois les risques techniques et non techniques. Cette évaluation a mis en évidence plusieurs risques, y compris l'ingérence potentielle de pays tiers ou d'acteurs de pays tiers par l'intermédiaire de la chaîne d'approvisionnement, et a classé les actifs en fonction de leur importance critique. Cette évaluation devrait servir de base à la définition des actifs de TIC essentiels pour les réseaux de communications 5G.

(156) Afin d'atténuer les risques recensés dans l'évaluation coordonnée au niveau de l'Union des risques pour la sécurité des réseaux 5G, le groupe de coopération SRI a adopté la boîte à outils sur la cybersécurité des réseaux 5G, qui définit des mesures stratégiques et techniques. Bien qu'une majorité d'États membres disposent de cadres juridiques qui permettent de restreindre ou d'exclure les fournisseurs à haut risque, comme le recommande la boîte à outils 5G, la mise en œuvre de ces cadres n'a pas été uniforme. En conséquence, un nombre important de sites 5G dans l'ensemble de l'Union sont approvisionnés par des fournisseurs à haut risque, comme indiqué dans la communication de la Commission sur la mise en œuvre de la boîte à outils sur la cybersécurité des réseaux 5G[69]. Cette situation crée des vulnérabilités, y compris une dépendance stratégique et une exposition potentielle à l'ingérence de pays tiers, qui pourraient également avoir une incidence sur les futures infrastructures 6G fondées sur les réseaux 5G existants. La mise en œuvre fragmentée des mesures recommandées dans la boîte à outils 5G, en particulier en ce qui concerne la portée des restrictions imposées aux fournisseurs à haut risque, a entraîné des divergences entre les États

[69] Communication de la Commission – Mise en œuvre de la boîte à outils sur la cybersécurité des réseaux 5G, 15 juin 2023, C(2023) 4049 final.

membres et, partant, des conditions de concurrence inégales qui divisent le marché intérieur et affaiblissent la sécurité globale des réseaux. La Cour des comptes européenne a attiré l'attention sur ces disparités, en mettant en garde sur le fait que l'absence d'approche coordonnée nuit au fonctionnement du marché intérieur. La dépendance persistante à l'égard de fournisseurs à haut risque entraîne de graves risques pour la sécurité des infrastructures critiques dans l'Union et pourrait éroder la confiance dans le marché intérieur; en effet, des niveaux de sécurité incohérents peuvent décourager les consommateurs et les entreprises d'avoir recours aux produits et services fondés sur la 5G dans l'ensemble de l'Union. Il est donc essentiel de disposer de mesures au niveau de l'Union pour garantir une approche harmonisée de la sécurité des réseaux 5G.

(157) Aux fins de la détermination d'une période de suppression progressive des actifs de TIC essentiels des réseaux de communications électroniques fixes et par satellite, la Commission devrait procéder à une évaluation en tenant dûment compte du degré des risques pour la sécurité de chaque actif de TIC essentiel spécifique des réseaux fixes et par satellite, de la durée de vie des composants concernés et de l'incidence économique que la suppression de ces composants aurait sur les opérateurs concernés. Sur la base des résultats de cette évaluation, la Commission peut envisager de fixer des périodes de suppression progressive différentes pour les actifs de TIC essentiels particuliers et les éléments qui les composent.

(158) Aux fins d'une surveillance et d'une exécution efficaces du respect des obligations concernant les fournisseurs de réseaux de communications électroniques mobiles, fixes et par satellite, les autorités compétentes concernées en vertu du présent règlement devraient assurer une coopération étroite avec les autorités compétentes en vertu de la [proposition de règlement sur les réseaux numériques]. À la demande d'une autorité compétente désignée en vertu du présent règlement, les autorités de régulation nationales ou d'autres autorités compétentes pour le spectre radioélectrique, le cas échéant, devraient retirer les droits visés à l'article 9 et à l'article 20 [de la proposition de règlement sur les réseaux numériques] si le fournisseur de réseaux de communications électroniques publics ne respecte pas les obligations prévues par le présent règlement, y compris s'il ne supprime pas progressivement les composants TIC ou composants comprenant des composants TIC provenant de fournisseurs à haut risque utilisés dans l'exploitation d'actifs de TIC essentiels dans le délai fixé conformément au présent règlement.

(159) Compte tenu des divergences entre les structures de gouvernance nationales, les États membres devraient désigner ou créer une ou plusieurs autorités compétentes chargées des mesures de supervision et d'exécution au titre du présent règlement.

(160) Les autorités compétentes devraient aider les entités du type visé aux annexes I et II de la directive (UE) 2022/2555 à se conformer aux obligations qui leur incombent en vertu du présent règlement. À cette fin, la Commission devrait évaluer si les fournisseurs susceptibles d'être concernés par des interdictions spécifiques sont établis dans un pays tiers qui suscite des préoccupations en matière de cybersécurité ou sont contrôlés par un tel pays, par une entité établie dans un tel pays ou par un ressortissant d'un tel pays. Les autorités compétentes devraient coopérer étroitement avec la Commission et les autres autorités compétentes au sein du réseau établi en vertu du présent règlement. Sur la base de l'évaluation effectuée par la Commission, les autorités compétentes devraient partager les informations pertinentes concernant les fournisseurs à haut risque avec les entités concernées du type visé aux annexes I et II de la directive (UE) 2022/2555. Les entités ne sont pas censées vérifier si un

fournisseur est sous contrôle étranger, mais peuvent s'appuyer pleinement sur les informations reçues des autorités compétentes. Les autorités compétentes devraient veiller à ce qu'aucune charge administrative inutile ne soit imposée à ces entités.

(161) Afin de garantir le respect effectif des obligations, le présent règlement devrait prévoir des mesures de supervision et d'exécution permettant aux autorités compétentes de surveiller les entités du type visé aux annexes I et II de la directive (UE) 2022/2555. Lorsque les autorités compétentes exécutent leurs tâches de supervision et d'exécution à l'égard de ces entités, elles ne devraient pas aller au-delà de ce qui est nécessaire et être proportionnées aux risques recensés.

(162) Afin de rendre l'exécution effective et cohérente dans l'ensemble de l'Union, il est nécessaire de prévoir des pouvoirs d'exécution que les autorités compétentes peuvent exercer en cas de violation des obligations énoncées dans le présent règlement. Dans l'exercice de ces pouvoirs d'exécution, les autorités compétentes devraient tenir dûment compte d'un certain nombre de facteurs, y compris de la nature, de la gravité et de la durée de la violation, du dommage matériel, corporel ou moral causé, du fait que la violation ait été commise intentionnellement ou par négligence, des mesures prises pour prévenir ou atténuer le dommage matériel, corporel ou moral subi, du degré de responsabilité ou de toute violation antérieure pertinente, du degré de coopération avec l'autorité compétente et de toute autre circonstance aggravante ou atténuante. Les mesures d'exécution, y compris les sanctions, devraient être proportionnées et leur imposition soumise à des garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et à la Charte des droits fondamentaux de l'Union européenne, y compris le droit à un recours effectif et à accéder à un tribunal impartial, la présomption d'innocence et les droits de la défense.

(163) Il importe de prévoir également le pouvoir d'imposer des astreintes pour contraindre une entité du type visé à l'annexe I ou II de la directive (UE) 2022/2555 à mettre un terme à une violation du présent règlement conformément à une décision préalable de l'autorité compétente.

(164) Afin de garantir une exécution efficace des obligations prévues par le présent règlement, chaque autorité compétente devrait avoir le pouvoir d'imposer ou de demander l'imposition de sanctions.

(165) Aux fins de l'imposition de sanctions à une entité du type visé aux annexes I et II de la directive (UE) 2022/2555 qui est une entreprise, le terme «entreprise» devrait être compris comme une entreprise conformément aux articles 101 et 102 TFUE. Lorsqu'une amende est imposée à une personne qui n'est pas une entreprise, l'autorité compétente devrait tenir compte, lorsqu'elle examine quel serait le montant approprié des sanctions, du niveau général des revenus dans l'État membre ainsi que de la situation économique de la personne en cause. Il devrait appartenir aux États membres de déterminer si et dans quelle mesure les autorités publiques devraient faire l'objet de sanctions. L'imposition d'une sanction ne devrait pas avoir d'incidence sur l'application d'autres pouvoirs des autorités compétentes.

(166) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission en ce qui concerne l'adoption d'actes d'exécution établissant des règles détaillées relatives redevances perçues par l'ENISA, d'actes d'exécution prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités, d'actes d'exécution établissant des principes communs et des dispositions de référence

destinés à établir des éléments dans l'ensemble des schémas européens de certification de cybersécurité, d'actes d'exécution précisant les procédures pour les modèles d'approbation préalable ou de délégation générale, d'actes d'exécution visant à reconnaître des certificats de cybersécurité d'un pays tiers ou d'une organisation internationale comme équivalents aux certificats de cybersécurité européens, d'actes d'exécution établissant un plan pour les examens par les pairs, d'actes d'exécution visant à établir les procédures d'autorisation des organismes d'évaluation de la conformité, y compris concernant la coopération transfrontière, d'actes d'exécution visant à établir les circonstances, formats et procédures pour les notifications des organismes d'évaluation de la conformité, d'actes d'exécution désignant un pays tiers comme suscitant des préoccupations en matière de cybersécurité pour les chaînes d'approvisionnement des TIC, d'actes d'exécution identifiant les actifs TIC essentiels utilisés pour la fabrication de produits ou la fourniture de services par des entités du type visé aux annexes I et II de la directive (UE) 2022/2555, d'actes d'exécution établissant que les entités opérant dans des secteurs hautement critiques et d'autres secteurs critiques font l'objet de mesures d'atténuation spécifiques et précisant les délais pour la suppression progressive des composants TIC ou composants qui incluent des composants TIC provenant de fournisseurs à haut risque, d'actes d'exécution précisant davantage les conditions relatives à l'exemption des entités établies dans des pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlées par des entités de tels pays tiers et d'actes d'exécution établissant des règles détaillées relatives aux redevances perçues par la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil et il convient de recourir à la procédure d'examen. Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer également des compétences d'exécution à la Commission en ce qui concerne l'établissement d'une liste de fournisseurs à haut risque pour certaines mesures prévues par le présent règlement.

(167) Il est nécessaire que les schémas européens de certification de cybersécurité tiennent compte des dernières évolutions technologiques, des nouvelles menaces connexes et de l'adoption de nouveaux actes législatifs de l'Union établissant la démonstration de la conformité et la présomption de conformité, au moyen de la certification européenne de cybersécurité, avec les exigences pertinentes en matière de cybersécurité énoncées dans ces actes législatifs. Pour ces raisons, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 TFUE afin d'ajouter ou de modifier les objectifs de sécurité poursuivis par les schémas européens de certification de cybersécurité. De même, afin de garantir cadre fiable pour les chaînes d'approvisionnement des TIC, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 TFUE afin de modifier l'annexe II du présent règlement en vue de l'adapter aux évolutions technologiques. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer». En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil devraient recevoir tous les documents au même moment que les experts des États membres, et leurs experts devraient avoir systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(168) Les activités de l'ENISA devraient faire l'objet d'évaluations régulières et indépendantes. Ces évaluations devraient porter sur les objectifs et la pertinence des tâches de l'ENISA, en particulier les tâches qui ont trait à la coopération opérationnelle au niveau de l'Union. En cas de réexamen, la Commission devrait évaluer comment renforcer le rôle joué par l'ENISA en tant que point de référence pour les conseils et compétences.

(169) Le règlement d'exécution (UE) 2024/482 de la Commission établit des règles en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC). L'EUCC est le premier et unique schéma européen de certification de cybersécurité adopté au titre du règlement (UE) 2019/881. Il concerne la certification des produits TIC, y compris des produits relevant des domaines techniques «cartes à puce et dispositifs similaires» et «dispositifs matériels avec boîtier de sécurité», et les profils de protection (en tant que processus TIC). Il est donc nécessaire de veiller à ce que les activités de certification ainsi que les activités de l'Agence se poursuivent.

(170) 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[70] et ont rendu un avis conjoint le [date].

(171) Il y a lieu d'abroger le règlement (UE) 2019/881.

(172) Étant donné que les objectifs du présent règlement ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent, en raison de ses dimensions et de ses effets, 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 (TUE). Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

TITRE I
DISPOSITIONS GÉNÉRALES

Article premier
Objet et champ d'application

1. Le présent règlement établit:

   (a) la mission, les objectifs, les tâches et les questions organisationnelles concernant l'ENISA (l'Agence de l'Union européenne pour la cybersécurité);

   (b) un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC, services de sécurité gérés dans l'Union, ou pour la posture de cybersécurité des entités, ainsi que dans le but

[70] 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 e 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d’éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l’Union; et

(c) un cadre digne de confiance pour la chaîne d’approvisionnement des TIC.

2. Le cadre mentionné au paragraphe 1, point b), s’applique sans préjudice des dispositions spécifiques d’autres actes juridiques de l’Union en matière de certification volontaire ou obligatoire.

3. Le cadre visé au paragraphe 1, point c), s’applique aux entités publiques ou privées correspondant à un des types énumérés à l’annexe I ou II de la directive (UE) 2022/2555, qui fournissent leurs services ou exercent leurs activités au sein de l’Union.

4. Le présent règlement est sans préjudice des fonctions essentielles des États membres, notamment celles d’assurer l’intégrité territoriale de l’État, de maintenir l’ordre public et de préserver la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre.

Article 2
Définitions

Aux fins du présent règlement, on entend par:

(1) «cybersécurité»: les actions nécessaires pour protéger les réseaux et les systèmes d’information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces;

(2) «entités de l’Union»: les entités de l’Union telles qu’elles sont définies à l’article 3, point 1), du règlement (UE, Euratom) 2023/2841;

(3) «prestataire d’attestation agréé»: une entité, publique ou privée, autorisée en vertu d’une décision adoptée par l’ENISA à délivrer des attestations individuelles européennes des compétences en matière de cybersécurité, telles que définies dans un programme d’attestation individuelle européenne des compétences en matière de cybersécurité;

(4) «attestation individuelle européenne des compétences en matière de cybersécurité»: un enregistrement, sous forme numérique ou physique, attestant qu’une personne connaît, comprend et est en mesure d’exécuter les tâches associées à un profil de fonction ou à un sous-ensemble de profil de fonction du cadre européen de compétences en matière de cybersécurité (ECSF), à la suite d’une évaluation telle que définie dans un programme d’attestation individuelle européenne des compétences en matière de cybersécurité;

(5) «programme d’attestation individuelle européenne des compétences en matière de cybersécurité»: un ensemble complet de règles, d’exigences, de normes et de procédures établies par l’ENISA et associées à un profil de fonction de l’ECSF ou à un sous-ensemble de celui-ci, qui s’appliquent aux fournisseurs d’attestation agréés et sont appliquées par ceux-ci;

(6) «réseau et système d’information»: un réseau et système d’information tel qu’il est défini à l’article 6, point 1), de la directive (UE) 2022/2555;

(7) «stratégie nationale en matière de cybersécurité»: une stratégie nationale en matière de cybersécurité telle qu'elle est définie à l'article 6, point 4), de la directive (UE) 2022/2555;

(8) «incident»: un incident tel qu'il est défini à l'article 6, point 6), de la directive (UE) 2022/2555;

(9) «incident de cybersécurité majeur»: un incident de cybersécurité majeur tel qu'il est défini à l'article 6, point 7), de la directive (UE) 2022/2555;

(10) «traitement des incidents»: le traitement des incidents tel qu'il est défini à l'article 6, point 8), de la directive (UE) 2022/2555;

(11) «cybermenace»: toute circonstance, tout événement ou toute action potentiels susceptibles d'endommager ou de perturber les réseaux et systèmes d'information, ou de porter autrement atteinte à ces réseaux et systèmes ainsi qu'à leurs utilisateurs et à d'autres personnes;

(12) «schéma européen de certification de cybersécurité»: un ensemble complet de règles, d'exigences techniques, de normes et de procédures qui sont établies à l'échelon de l'Union et qui s'appliquent à la certification ou à l'évaluation de la conformité de produits TIC, de services TIC, de processus TIC, de services de sécurité gérés ou de la posture de cybersécurité des entités;

(13) «schéma national de certification de cybersécurité»: un ensemble complet de règles, d'exigences techniques, de normes et de procédures élaborées et adoptées par une autorité publique nationale et qui s'appliquent à la certification ou à l'évaluation de la conformité de produits TIC, de services TIC, de processus TIC, de services de sécurité gérés, ou de la posture de cybersécurité des entités relevant de ce schéma spécifique;

(14) «certificat de cybersécurité européen»: un document délivré par un organisme compétent attestant qu'un produit TIC, un service TIC, un processus TIC, des services de sécurité gérés ou la posture de cybersécurité d'une entité ont été évalués en ce qui concerne leur conformité aux exigences de sécurité spécifiques fixées dans un schéma européen de certification de cybersécurité;

(15) «déclaration de conformité de l'UE»: un document délivré par un fabricant ou un fournisseur de produits TIC, de services TIC, de processus TIC, de services de sécurité gérés ou par l'entité dont la posture de cybersécurité fait l'objet d'une certification, indiquant que le respect des exigences correspondant au niveau d'assurance «élémentaire» énoncées dans le schéma européen de certification de cybersécurité a été démontré au moyen d'une autoévaluation de la conformité;

(16) «produit TIC»: un élément ou un groupe d'éléments appartenant à un réseau ou à un système d'information;

(17) «service TIC»: un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information;

(18) «processus TIC»: un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance;

(19) «service de sécurité géré»: un service fourni à un tiers consistant à effectuer des activités liées à la gestion des risques en matière de cybersécurité, ou à fournir une assistance dans le cadre de ces activités, telles que le traitement des incidents, les

tests d'intrusion, les audits de sécurité et le conseil, y compris les conseils d'experts liés à l'assistance technique;

(20) «accréditation»: une accréditation tel qu'elle est définie à l'article 2, point 10), du règlement (CE) nº 765/2008;

(21) «organisme national d'accréditation»: un organisme national d'accréditation tel qu'il est défini à l'article 2, point 11), du règlement (CE) nº 765/2008;

(22) «évaluation de la conformité»: une évaluation de la conformité tel qu'elle est définie à l'article 2, point 12), du règlement (CE) nº 765/2008;

(23) «organisme d'évaluation de la conformité»: un organisme d'évaluation de la conformité tel qu'il est défini à l'article 2, point 13), du règlement (CE) nº 765/2008;

(24) «norme»: une norme telle qu'elle est définie à l'article 2, point 1), du règlement (UE) nº 1025/2012 du Parlement européen et du Conseil[71];

(25) «spécification technique»: une spécification technique telle qu'elle est définie à l'article 2, point 4), du règlement (UE) nº 1025/2012;

(26) «norme harmonisée»: une norme harmonisée telle qu'elle est définie à l'article 2, point 1), c), du règlement (UE) nº 1025/2012;

(27) «niveau d'assurance»: le fondement permettant de garantir qu'un produit TIC, un service TIC, un processus TIC, un service de sécurité géré ou la posture de cybersécurité d'une entité satisfont aux exigences de sécurité d'un schéma européen de certification de cybersécurité donné, et indique le niveau auquel un produit TIC, un service TIC, un processus TIC, un service de sécurité géré ou la posture de cybersécurité d'une entité ont été évalués mais, en tant que tel, ne mesure pas la sécurité du produit TIC, du service TIC, du processus TIC, du service de sécurité géré ou de la posture de cybersécurité concernés;

(28) «autoévaluation de la conformité»: une action effectuée par un fabricant ou un fournisseur de produits TIC, de services TIC, de processus TIC, de services de sécurité gérés, ou par l'entité dont la posture de cybersécurité fait l'objet d'une certification, qui évalue si ces produits TIC, ces services TIC, ces processus TIC, ces services de sécurité gérés ou cette posture de cybersécurité des entités satisfont aux exigences fixées dans un schéma européen de certification de cybersécurité donné;

(29) «posture de cybersécurité des entités»: le niveau de cybersécurité des entités en ce qui concerne les exigences de sécurité spécifiques;

(30) «modèle d'approbation préalable»: un modèle en vertu duquel un organisme d'évaluation de la conformité peut délivrer un certificat de cybersécurité européen sur la base de l'évaluation effectuée par une autorité nationale de certification de cybersécurité au titre d'un processus de certification spécifique dans le cadre d'un schéma pertinent;

---

[71] Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(31) «modèle de délégation générale»: un modèle en vertu duquel un organisme d'évaluation de la conformité peut délivrer un certificat de cybersécurité européen sur la base d'une délégation des activités de certification par une autorité nationale de certification de cybersécurité;

(32) «centre de réponse aux incidents de sécurité informatique (CSIRT)»: un CSIRT désigné ou créé conformément à l'article 10 de la directive (UE) 2022/2555;

(33) «composants TIC»: les produits TIC, services TIC ou processus TIC qui peuvent être utilisés dans l'exploitation d'actifs TIC;

(34) «actifs TIC»: actifs logiciels ou matériels des réseaux et systèmes d'information utilisés par une entité d'un des types visé aux annexes I et II de la directive (UE) 2022/2555;

(35) «actifs TIC essentiels »: les actifs TIC identifiés conformément à l'article 102;

(36) «réseau de communications électroniques»: un réseau de communications électroniques au sens de l'article 2, point 1), du règlement (UE) XX/XXXX (proposition de règlement sur les réseaux numériques);

(37) «contrôle»: la capacité d'exercer une influence déterminante sur une entité juridique, soit de manière directe, soit de manière indirecte par l'entremise d'une ou de plusieurs entités juridiques intermédiaires;

(38) «établissement»: l'exercice effectif d'une activité au moyen d'installations stables dans le pays où se trouvent l'administration centrale ou le principal établissement de l'entité;

(39) «fournisseur à haut risque»: soit

(a) une entité établie dans un pays tiers qui suscite des préoccupations en matière de cybersécurité et qui est désigné conformément à l'article 100, ou contrôlée par ce pays tiers, par une entité établie dans ce pays tiers, ou par un ressortissant de ce pays tiers;

(b) une entité désignée conformément à l'article 103, paragraphe 7, et les entités qu'elle contrôle;

(40) «chaîne d'approvisionnement des TIC»: un ensemble de services TIC, de produits TIC et de processus TIC qui englobent des activités et des acteurs intervenant à tous les stades en amont de la mise à disposition d'un produit ou de la fourniture d'un service sur le marché;

(41) «pays tiers»: un pays tiers au sens de l'article 3, point 4), du règlement (UE) 2023/2675 du Parlement européen et du Conseil[72];

(42) «risque non technique»: la probabilité que le fournisseur soit soumis à l'influence d'un pays tiers susceptible de causer la perte ou la perturbation du service fourni, de compromettre le produit fabriqué par une entité ou d'entraîner l'exfiltration de données, y compris à des fins d'espionnage ou de génération de revenus;

(43) «risque de cybersécurité non technique important»: un risque de cybersécurité non technique qui peut être présumé hautement susceptible de donner lieu à un incident

[72] Règlement (UE) 2023/2675 du Parlement européen et du Conseil du 22 novembre 2023 relatif à la protection de l'Union et de ses États membres contre la coercition économique exercée par des pays tiers (JO L, 2023/2675, 7.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2675/oj).

pouvant avoir des répercussions négatives graves, notamment en causant une perte ou une perturbation matérielle ou immatérielle considérable;

(44) «fonctions de cœur de réseau des réseaux de communications électroniques mobiles»: l'élément architectural central des réseaux de communications électroniques mobiles reliant les principaux nœuds de réseau à l'internet et gérant les fonctions essentielles du système, qui comprend l'authentification des équipements utilisateurs, les fonctions d'interception légale (LI), les passerelles de sécurité (SeGW) à la périphérie du réseau, les fonctions de sécurité de la signalisation, la gestion de l'itinérance et de la session, le transport des données des plans d'utilisateur et de contrôle, la gestion de la politique d'accès, l'enregistrement et l'autorisation des services de réseau, le stockage des données des utilisateurs finaux et des données de réseau, les services de réseau critiques, y compris le système de noms de domaine (DNS), l'interconnexion avec les réseaux mobiles tiers, l'exposition des fonctions de cœur de réseau à des applications externes, ainsi que la sélection et la gestion des tranches de réseau;

(45) «virtualisation des fonctions de réseau (NFV) et gestion et orchestration (MANO) des réseaux de communications électroniques mobiles»: le cadre logiciel et architectural assurant la gestion du cycle de vie, l'orchestration et l'automatisation des fonctions de réseau virtualisées (VNF) et des fonctions de réseau natif en nuage (CNF), ainsi que la sélection et la gestion des tranches de réseau dans les réseaux de communications électroniques mobiles;

(46) «réseau d'accès radioélectrique (RAN) des réseaux de communications électroniques mobiles»: le réseau reliant l'équipement utilisateur mobile au cœur de réseau, y compris les stations de base (eNodeB pour la 4G, gNodeB pour la 5G), les têtes radio distantes (RRH) et les unités de bande de base (BBU), les systèmes à antenne active (AAS) et, le cas échéant, les composants RAN désagrégés tels que les unités centralisées (CU) et les unités distribuées (DU), ainsi que le contrôleur intelligent (RIC) du RAN;

(47) «fonctions de cœur de réseau des réseaux de communications électroniques fixes»: l'intelligence dorsale du réseau, qui relie les principaux nœuds et gère une série de fonctions essentielles, notamment l'authentification et l'autorisation des utilisateurs (AAA), les fonctions d'interception légale (LI), le système de noms de domaine (DNS) et les services d'adressage IP (DHCP), la gestion de la politique d'accès, le stockage des données des utilisateurs finaux et des données de réseau, la commutation et le routage IP et les passerelles internet internationales (IIG);

(48) «système de gestion de réseau des réseaux de communications électroniques fixes»: l'ensemble des plateformes centralisées et des composants logiciels nécessaires à l'exploitation, à l'administration, à la maintenance et au provisionnement (OAM&P) du réseau et à la surveillance des informations liées au réseau;

(49) «fonctions de transport et de transmission des réseaux de communications électroniques fixes»: tous les composants nécessaires à la collecte et à l'agrégation du trafic sur l'ensemble du réseau, notamment les équipements de transport optique, les liaisons hyperfréquences et les systèmes de câbles sous-marins qui comprennent les équipements sous-marins ainsi que les équipements de terminaison de ligne sous-marine (SLTE) et les installations physiques des stations d'atterrissement;

(50) «réseau d'accès des réseaux de communications électroniques fixes»: le réseau reliant les locaux de l'utilisateur final au réseau d'agrégation ou au cœur de réseau, y

compris la terminaison de ligne optique (OLT) et la terminaison de réseau optique (ONT) pour les réseaux en fibre optique; le système de terminaison de modem câble (CMTS), et les modems câbles pour les réseaux de câbles coaxiaux et les composants pour l'accès fixe sans fil lorsqu'il est utilisé en remplacement d'une ligne fixe.

TITRE II
L'AGENCE DE L'UNION EUROPÉENNE POUR LA CYBERSÉCURITÉ

Chapitre I
Mission et objectifs

Article 3
Mission de l'ENISA

1. La mission de l'ENISA est d'aider les États membres et les entités de l'Union à atteindre un niveau élevé de cybersécurité, de cyberrésilience et de confiance au sein de l'Union.
2. L'ENISA sert de point de référence pour les conseils et l'expertise en matière de cybersécurité pour les États membres ainsi que pour les autres parties prenantes concernées de l'Union.
3. L'ENISA contribue à réduire la fragmentation du marché intérieur en s'acquittant des tâches qui lui sont assignées en vertu du présent règlement.
4. L'ENISA exécute les tâches qui lui sont assignées par des actes juridiques de l'Union.
5. L'ENISA développe ses capacités propres, y compris les capacités et les aptitudes techniques et humaines, nécessaires pour exécuter les tâches qui lui sont assignées en vertu du présent règlement.

Article 4
Objectifs de l'ENISA

1. L'ENISA est un centre d'expertise en matière de cybersécurité du fait de son indépendance, de la qualité scientifique et technique des conseils, des contributions et de l'assistance qu'elle dispense, des informations qu'elle fournit, de la transparence de ses procédures de fonctionnement, des modes de fonctionnement et de sa diligence à exécuter ses tâches.
2. L'ENISA aide les États membres et, le cas échéant, les entités de l'Union à mettre en œuvre les politiques et la législation horizontales et sectorielles de l'Union en matière de cybersécurité, y compris les activités de surveillance du marché.
3. L'ENISA apporte son expertise et assiste la Commission dans l'élaboration des politiques et de la législation de l'Union relatives à la cybersécurité.
4. L'ENISA soutient le renforcement des capacités et contribue à l'état de préparation au sein de l'Union en aidant les États membres, les entités de l'Union, par l'intermédiaire du service de cybersécurité pour les institutions, organes et organismes de l'Union (CERT-UE) visé au chapitre IV du règlement (UE, Euratom) 2023/2841, et les parties prenantes publiques et privées à accroître la protection de

leurs réseaux et systèmes d'information et à développer et à améliorer la cyberrésilience ainsi que les capacités de réaction.

5. L'ENISA contribue à la mise en œuvre de l'académie des compétences en matière de cybersécurité et à la croissance de la main-d'œuvre dans le domaine de la cybersécurité dans l'Union. Pour ce faire, elle soutient les efforts destinés à développer la portabilité des compétences dans l'ensemble de l'Union, y compris par la maintenance et la promotion de l'adoption de l'ECSF et l'élaboration, la maintenance et la promotion de l'adoption de programmes d'attestation individuelle européenne des compétences en matière de cybersécurité conformément au chapitre II, section 4, du présent titre, et en dispensant des formations conformément à l'article 6, paragraphe 8.

6. L'ENISA favorise la coopération, notamment le partage d'informations et la coordination au niveau de l'Union, entre les États membres, les entités de l'Union conformément au règlement (UE, Euratom) 2023/2841, et les parties prenantes concernées des secteurs public et privé en ce qui concerne les questions liées à la cybersécurité.

7. L'ENISA contribue à renforcer les capacités dans le domaine de la cybersécurité au niveau de l'Union afin de soutenir les actions des États membres pour prévenir les cybermenaces et réagir à celles-ci.

8. L'ENISA soutient la coopération opérationnelle au niveau de l'Union, notamment en contribuant à une conscience situationnelle commune du paysage des cybermenaces et incidents parmi les États membres et, en coopération avec le CERT-UE, parmi les entités de l'Union.

9. L'ENISA coopère étroitement avec Europol, les CSIRT et les autres autorités nationales compétentes afin d'améliorer l'état de préparation en matière de cybersécurité et la réaction aux incidents liés aux rançongiciels.

10. L'ENISA contribue à l'établissement et à la maintenance d'un cadre européen de certification de cybersécurité conformément au titre III du présent règlement. L'ENISA favorise le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur.

11. L'ENISA contribue à l'harmonisation du marché unique numérique en participant à des travaux de normalisation pertinents pour les politiques de l'Union en matière de cybersécurité et en élaborant des spécifications techniques.

12. L'ENISA promeut un niveau élevé de sensibilisation à la cybersécurité parmi les organisations et les entreprises.

Chapitre II
Missions

Section 1
Soutien à la mise en œuvre de la politique et du droit de l'Union

Article 5
Soutien à la mise en œuvre de la politique et du droit de l'Union

1. L'ENISA contribue à la mise en œuvre de la politique et du droit de l'Union:

(a) en aidant les États membres à mettre en œuvre la politique et le droit de l'Union en matière de cybersécurité de manière cohérente, notamment en publiant des orientations et des rapports techniques, en fournissant des conseils et en partageant les meilleures pratiques, et en facilitant l'échange des meilleures pratiques entre les autorités compétentes à cet égard;

(b) en soutenant le partage d'informations au sein des secteurs et entre ceux-ci, en particulier en ce qui concerne les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555 et les produits comportant des éléments numériques relevant du champ d'application du règlement (UE) 2024/2847, en fournissant des meilleures pratiques et des orientations sur les outils et procédures disponibles;

(c) en apportant son aide aux États membres, à la demande de la Commission, sous la forme d'un soutien, par exemple des orientations techniques, y compris sur les mesures de gestion des risques en matière de cybersécurité, d'outils d'évaluation de la maturité en matière de cybersécurité, et de manuels de réaction en cas d'incident, adaptés aux secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555, ou d'une assistance à la mise en œuvre de principes de sécurité dès la conception pour les produits comportant des éléments numériques conformément au règlement (UE) 2024/2847, en vue de faciliter l'amélioration des niveaux de maturité en matière de cybersécurité et du respect du droit de l'Union en matière de cybersécurité;

(d) en contribuant aux travaux du groupe de coopération institué en vertu de l'article 14, paragraphe 1, de la directive (UE) 2022/2555 (ci-après le «groupe de coopération SRI»), du groupe de coopération européen en matière d'identité numérique institué en vertu de l'article 46 *sexies*, paragraphe 1, du règlement (UE) nº 910/2014, du groupe européen de certification de cybersécurité (ci-après le «GECC») visé à l'article 90 du présent règlement et du groupe de coopération administrative (ADCO) institué en vertu de l'article 52, paragraphe 15, du règlement (UE) 2024/2847;

(e) en aidant les États membres et les entités pertinentes de l'Union à élaborer et à promouvoir des politiques en matière de cybersécurité visant à soutenir la disponibilité et l'intégrité générales du noyau public de l'internet ouvert;

(f) en fournissant, conformément au règlement (UE) 2024/2847, des conseils et un soutien techniques aux États membres et à la Commission sur les questions liées à la mise en œuvre dudit règlement;

(g) en aidant les États membres à se prêter mutuellement assistance et en facilitant ces processus de coopération pour les entités essentielles et importantes conformément à [l'article 37 *bis* de la directive (UE) 2022/2555];

(h) en prodiguant, à la demande du comité européen de la protection des données, des conseils sur la mise en œuvre d'aspects particuliers liés à la cybersécurité de la politique et du droit de l'Union en matière de protection des données et de la vie privée.

2. L'ENISA contribue aux évaluations coordonnées au niveau de l'Union des risques de cybersécurité, y compris celles effectuées conformément à l'article 22 de la directive (UE) 2022/2555.

3. L'ENISA publie des lignes directrices concernant l'interopérabilité des réseaux et des systèmes d'information utilisés pour le partage d'informations, y compris en ce

qui concerne les cyberpôles transfrontières visés à l'article 6, paragraphe 3, du règlement (UE) 2025/38.

4. L'ENISA est membre du groupe de coopération SRI, conformément à l'article 14, paragraphe 3, de la directive (UE) 2022/2555.

5. À la demande de la Commission, l'ENISA fournit une expertise, des conseils techniques, des informations ou des analyses ou effectue des travaux préparatoires sur des questions de cybersécurité particulières en vue d'éclairer l'élaboration des politiques de la Commission et le suivi de la mise en œuvre de la législation de l'Union.

Article 6
Renforcement des capacités

L'ENISA assiste:

(1) les États membres dans leurs efforts pour améliorer la prévention, la détection et l'analyse des cybermenaces et incidents, ainsi que la capacité d'y réagir, en leur fournissant des connaissances et une expertise;

(2) les États membres, à leur demande, pour l'établissement et la mise en œuvre, sur une base volontaire, des politiques en matière de divulgation des vulnérabilités;

(3) conformément au règlement (UE, Euratom) 2023/2841, le CERT-UE et le conseil interinstitutionnel de cybersécurité dans les efforts qu'ils déploient pour aider les entités de l'Union à renforcer leur cybersécurité, à améliorer la prévention, la détection et l'analyse des cybermenaces et incidents et à améliorer leurs capacités de réaction à ces cybermenaces et incidents;

(4) les États membres dans la mise en place de CSIRT nationaux, lorsqu'ils le demandent conformément à l'article 10, paragraphe 10, de la directive (UE) 2022/2555;

(5) les États membres dans l'élaboration ou la mise à jour de stratégies nationales en matière de cybersécurité et d'indicateurs clés de performance pour évaluer ces stratégies, lorsqu'ils le demandent conformément à l'article 7, paragraphe 4, de la directive (UE) 2022/2555, en favorisant la diffusion de ces stratégies et en observant l'avancement de leur mise en œuvre dans toute l'Union afin de promouvoir les meilleures pratiques;

(6) les institutions de l'Union, à leur demande, dans l'élaboration et la révision des stratégies de l'Union en matière de cybersécurité, la promotion de leur diffusion et le suivi de l'avancement de leur mise en œuvre;

(7) les CSIRT nationaux dans le relèvement du niveau de leurs capacités, y compris en favorisant le dialogue et les échanges d'informations, pour faire en sorte que chaque CSIRT, eu égard à l'état de l'art, possède un socle commun de capacités minimales et fonctionne selon les meilleures pratiques;

(8) les États membres, les entités de l'Union et les parties prenantes publiques et privées dans les efforts qu'ils déploient pour évaluer, accroître et renforcer la main-d'œuvre dans le domaine de la cybersécurité, y compris dans l'élaboration et la maintenance d'outils pertinents, tels que l'ECSF et les programmes d'attestation individuelle européenne des compétences en matière

de cybersécurité, et en en favorisant l'adoption, conformément à la section 4 du présent chapitre;

(9) les organismes publics concernés ainsi que les parties prenantes privées, en organisant des formations ciblées, le cas échéant en coopération avec les parties prenantes;

(10) le groupe de coopération SRI pour l'échange de meilleures pratiques et d'informations relatives, en particulier, à la mise en œuvre de la directive (UE) 2022/2555, conformément à l'article 14, paragraphe 4, point c), de ladite directive;

(11) les autorités de surveillance du marché désignées en vertu du règlement (UE) 2024/2847 dans le cadre de leurs activités visant à garantir la mise en œuvre effective dudit règlement, y compris le soutien aux orientations et aux conseils techniques destinés aux opérateurs économiques, l'assistance dans le cadre de contrôles de conformité, l'évaluation des risques, les activités conjointes et les opérations «coup de balai» prévues par le règlement (UE) 2024/2847;

(12) les membres du GECC, dans le cadre de l'échange des meilleures pratiques et, à la demande des différents États membres, les autorités nationales de certification de cybersécurité dans la mise en œuvre des schémas européens de certification de cybersécurité au niveau national;

(13) les autorités publiques et les parties prenantes privées en ce qui concerne les activités d'évaluation et d'appréciation de la conformité, y compris les organismes d'évaluation de la conformité et les petites et moyennes entreprises, afin de soutenir un écosystème d'évaluation de la conformité solide, compétitif, inclusif et harmonisé à l'appui de la mise en œuvre du règlement (UE) 2024/2847 et du cadre européen de certification de cybersécurité;

(14) le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination établis en vertu du règlement (UE) 2021/887, en partageant des informations sur les risques actuels et émergents et les cybermenaces, y compris en ce qui concerne les technologies de l'information et de la communication nouvelles et émergentes;

(15) les États membres, en fournissant un soutien technique, y compris pour la mise en place et le fonctionnement de bacs à sable réglementaires dans le domaine de la cybersécurité conformément à la législation pertinente de l'Union.

Article 7
Sensibilisation et réservoir de talents

L'ENISA aide les États membres dans leurs efforts de sensibilisation aux politiques et à la législation de l'Union en matière de cybersécurité et favorise la visibilité de celles-ci en élaborant des outils et des orientations utilisables. L'ENISA soutient les initiatives visant à élargir le réservoir européen de talents dans le domaine de la cybersécurité, notamment en coordonnant les concours.

Article 8
Connaissance du marché et analyses

1. L'ENISA effectue et diffuse des analyses portant sur les principales tendances du marché de la cybersécurité, tant du côté de l'offre que de la demande, en particulier en ce qui concerne les domaines dans lesquels des schémas européens de certification de cybersécurité existent ou sont prévus, les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555 et les catégories de produits couvertes par le règlement (UE) 2024/2847, y compris les annexes III et IV dudit règlement.
2. L'ENISA effectue et diffuse des analyses portant sur les tendances technologiques en matière de cybersécurité, en particulier en ce qui concerne les activités et entités relevant du champ d'application de la directive (UE) 2022/2555 et les produits comportant des éléments numériques couverts par le règlement (UE) 2024/2847.
3. L'ENISA développe des connaissances et diffuse des conseils et des analyses techniques relatifs aux outils, aux cadres, aux normes et aux meilleures pratiques les plus récents en matière de cybersécurité.

Article 9
Coopération internationale

L'ENISA contribue aux efforts de l'Union pour coopérer avec les pays tiers et les organisations internationales, ainsi qu'au sein des cadres internationaux de coopération pertinents, afin de promouvoir une coopération internationale sur les problèmes de cybersécurité:

(a) le cas échéant, en s'impliquant en tant qu'observateur dans l'organisation d'exercices internationaux, ainsi qu'en analysant les résultats de ces exercices et en en rendant compte au conseil d'administration;

(b) à la demande de la Commission, en facilitant l'échange de meilleures pratiques avec les pays tiers et les organisations internationales;

(c) à la demande de la Commission, en la faisant bénéficier de son expertise;

(d) en fournissant à la Commission des conseils d'experts et une aide sur les questions relatives à la reconnaissance internationale des certificats de cybersécurité européens conformément à l'article 87;

(e) en fournissant à la Commission des conseils d'experts et une aide sur les questions relatives à la normalisation internationale et au dialogue avec les organisations internationales de normalisation, le cas échéant, en collaboration avec le GECC institué en vertu de l'article 90.

Section 2

Coopération opérationnelle

Article 10
Coopération opérationnelle au niveau de l'Union

1. L'ENISA apporte son soutien à la coopération opérationnelle entre les États membres, entre les entités de l'Union par l'intermédiaire du CERT-UE, et entre d'autres parties prenantes.

2. L'ENISA est membre du réseau des CSIRT nationaux établi en vertu de l'article 15, paragraphe 1, de la directive (UE) 2022/2555 et assure le secrétariat de ce réseau conformément à l'article 15, paragraphe 2, de la directive (UE) 2022/2555.

3. L'ENISA assure le secrétariat du réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) conformément à l'article 16, paragraphe 2, deuxième alinéa, de la directive (UE) 2022/2555.

4. L'ENISA soutient la coopération technique et opérationnelle entre les États membres, notamment par l'intermédiaire du réseau des CSIRT et d'EU-CyCLONe. Ce soutien prend notamment les formes suivantes:

   (a) des conseils sur l'amélioration des capacités visant à prévenir et à détecter les incidents, à y réagir et à s'en rétablir;

   (b) la fourniture de conseils et d'évaluations, à la demande d'un ou de plusieurs États membres, en ce qui concerne un incident ou une cybermenace donnés, en cours ou potentiels, notamment en apportant une expertise et en facilitant la gestion technique de tels incidents, en particulier en soutenant le partage volontaire d'informations et de solutions techniques pertinentes entre États membres;

   (c) l'analyse des vulnérabilités, menaces et incidents;

   (d) à la demande d'un ou de plusieurs États membres, la fourniture d'une aide en rapport avec les enquêtes techniques ex post sur les incidents considérés comme importants au sens de l'article 23, paragraphe 3, de la directive (UE) 2022/2555.

   (e) une contribution à la gestion coordonnée des incidents et crises de cybersécurité majeurs au niveau opérationnel, notamment en aidant EU-CyCLONe à élaborer des rapports destinés aux décideurs politiques et en facilitant le partage d'informations en temps utile entre le réseau des CSIRT et EU-CyCLONe;

5. À la demande d'un État membre ou d'une entité de l'Union en coopération avec le CERT-UE, l'ENISA contribue à une communication publique cohérente relative à un incident ou à une cybermenace.

6. L'ENISA soutient la coopération entre les États membres et, par l'intermédiaire du CERT-UE, entre les entités de l'Union en ce qui concerne le déploiement d'outils de communication sécurisés. L'ENISA utilise, au sein du réseau des CSIRT et d'EU-CyCLONe, des outils de communication sécurisés qui sont fournis par des entités juridiques établies ou réputées établies dans l'Union et contrôlées par des États membres ou par des ressortissants des États membres.

Article 11

Conscience situationnelle commune en matière de cybersécurité

1. Afin d'améliorer la conscience situationnelle commune du paysage des cybermenaces et des incidents parmi les États membres et parmi les entités de l'Union, l'ENISA:

   (a) élabore, en coopération avec EU-CyCLONe, le réseau des CSIRT, la Commission, le CERT-UE, Europol et d'autres entités de l'Union concernées, des fichiers de renseignements vérifiés et fiables sur les cybermenaces, y compris les tendances en matière d'incidents, de tactiques, de techniques et de procédures;

   (b) en application de l'article 12, émet des alertes précoces en cas d'incident important ou majeur potentiel ou en cours, ou de cybermenace de nature transfrontière potentielle, en particulier en ce qui concerne les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555;

   (c) fournit en temps utile des analyses ad hoc sur les tendances émergentes en matière d'incidents à la demande du réseau des CSIRT, d'EU-CyCLONe ou de la Commission;

   (d) fournit, à la demande des États membres ou de la Commission, une analyse ou d'autres informations concernant un risque ou une menace réels ou perçus en matière de cybersécurité;

   (e) fournit des analyses et des conseils techniques concernant les risques de cybersécurité dans les produits comportant des éléments numériques, notamment à l'appui de la surveillance du marché, et en élaborant un rapport technique bisannuel sur les tendances émergentes conformément à l'article 17, paragraphe 3, du règlement (UE) 2024/2847;

   (f) élabore régulièrement un rapport approfondi de situation technique en matière de cybersécurité de l'UE sur les incidents et les cybermenaces, et met ce rapport à la disposition du Conseil, d'EU-CyCLONe, du réseau des CSIRT, de la Commission, du Service européen pour l'action extérieure et d'Europol;

   (g) suit les tendances en matière de techniques, de demandes et d'incidence des attaques par rançongiciel et fournit des informations sur ces tendances à la Commission, au réseau des CSIRT, à EU-CyCLONe et à Europol.

2. Afin d'améliorer la conscience situationnelle commune du paysage des cybermenaces et des incidents parmi les parties prenantes, l'ENISA:

   (a) effectue des analyses des cybermenaces, des incidents, des tendances, des technologies émergentes et de leurs incidences, y compris une analyse régulière portant sur les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555 et les catégories de produits pertinentes couvertes par le règlement (UE) 2024/2847;

   (b) publie, en coopération avec la Commission et, le cas échéant, le réseau des CSIRT, des conseils, des orientations et des meilleures pratiques pour la sécurité des réseaux et des systèmes d'information, en particulier pour la sécurité des infrastructures soutenant les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555;

(c) procède à des analyses stratégiques à long terme des cybermenaces et des incidents afin d'identifier les tendances émergentes et de contribuer à prévenir les incidents;

3. L'ENISA peut rendre publics les analyses, conseils, orientations, bonnes pratiques et rapports visés au paragraphe 2, en accord avec les entités contributrices visées au paragraphe 2.

4. Pour exercer les activités énumérées au paragraphe 1, points a) à d) et point f), ainsi qu'au paragraphe 2, l'ENISA utilise ses propres analyses et, le cas échéant, les informations reçues dans le cadre de l'exécution de ses tâches, y compris:

(a) les informations figurant dans des sources accessibles au public, y compris les vulnérabilités notoires des produits TIC ou services TIC disponibles dans la base de données européenne des vulnérabilités établie en vertu de l'article 12, paragraphe 2, de la directive (UE) 2022/2555;

(b) les informations partagées par les États membres, les entités de l'Union, le CERT-UE, les partenaires du secteur privé ou non gouvernemental et les pays tiers et les organisations internationales, sous réserve que la distribution ultérieure de ces informations n'ait pas été exclue au moyen d'un marquage visible.

5. L'ENISA coopère étroitement avec les États membres en vue de l'élaboration du rapport de situation technique de cybersécurité de l'UE visé au paragraphe 1, point e). Ce rapport est fondé sur des informations publiquement disponibles, sur ses propres analyses et sur les rapports que lui communiquent notamment les CSIRT des États membres ou les points de contact uniques institués par la directive (UE) 2022/2555, sur une base volontaire dans les deux cas, l'EC3 et le CERT-UE. En accord avec les entités contributrices, l'ENISA peut mettre à la disposition du public une version agrégée du rapport.

Article 12
Alertes précoces

1. Les alertes précoces mentionnées à l'article 11, paragraphe 1, premier alinéa, point b), du présent règlement contiennent des informations pertinentes relatives à un incident important ou majeur potentiel ou en cours, ou à une cybermenace de nature transfrontière potentielle, en particulier en ce qui concerne les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555. Ces informations peuvent être relatives à des vulnérabilités notoires et à des indications concernant leur éventuelle incidence sur des produits comportant des éléments numériques couverts par le règlement (UE) 2024/2847, à des techniques et procédures, à des indicateurs de compromission, à des tactiques adverses, à des informations spécifiques aux acteurs de la menace et à des recommandations sur les mesures d'atténuation.

2. Les alertes précoces visées à l'article 11, paragraphe 1, premier alinéa, point b), sont envoyées dès que possible au CSIRT ou aux CSIRT concernés et, le cas échéant, au réseau des CSIRT et à EU-CyCLONe.

3. L'ENISA propose un service d'alerte précoce aux entités opérant dans les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555.

4. Le service visé au paragraphe 3 est fourni à la demande de l'entité et dans un format lisible par machine mis à la disposition du public. Ce service comprend le partage

d'informations sur les indicateurs de cybermenace et des recommandations sur les mesures d'atténuation.

5. L'ENISA établit une procédure pour diffuser les alertes précoces auprès des entités visées au paragraphe 3.

Article 13
Aide à la réaction en cas d'incident et à l'analyse des incidents

1. L'ENISA exploite et administre la réserve de cybersécurité de l'Union, en totalité ou en partie, conformément au règlement (UE) 2025/38.

2. À la demande de la Commission ou d'EU-CyCLONe, l'ENISA, avec le soutien du réseau des CSIRT et avec l'approbation de l'État membre concerné, analyse et évalue les incidents de cybersécurité importants ou les incidents de cybersécurité majeurs conformément à l'article 21 du règlement (UE) 2025/38.

3. L'ENISA aide, en coopération avec Europol et les CSIRT ou d'autres autorités compétentes, selon le cas, les différentes entités essentielles et entités importantes énumérées aux annexes I et II de la directive (UE) 2022/2555 à se préparer à un incident de rançongiciel, à y réagir et à s'en rétablir. À cette fin, l'ENISA met en place un service d'assistance et, en particulier, utilise la conscience situationnelle commune renforcée du paysage des cybermenaces et incidents conformément à l'article 11, paragraphe 1, premier alinéa, points a) et g), du présent règlement.

Article 14
Exercices de cybersécurité au niveau de l'Union

1. L'ENISA aide la Commission à élaborer un programme glissant annuel d'exercices de cybersécurité au niveau de l'Union.

2. L'ENISA tient un inventaire des enseignements tirés des exercices visés au paragraphe 1 et formule, à l'intention des États membres et, le cas échéant, des entités de l'Union, des recommandations sur la manière de mettre en œuvre de manière efficace et efficiente ces enseignements.

3. À la demande d'EU-CyCLONe et/ou de la Commission, l'ENISA organise ou contribue à l'organisation d'exercices de cybersécurité au niveau de l'Union, y compris pour tester l'état de préparation en vue de réagir à des incidents et crises de cybersécurité majeurs au niveau de l'Union.

4. L'ENISA aide les États membres, s'ils en font la demande, à organiser des exercices nationaux de cybersécurité.

5. À la demande du CERT-UE, l'ENISA contribue à l'organisation d'exercices de cybersécurité organisés par le CERT-UE conformément à l'article 13, paragraphe 7, du règlement (UE, Euratom) 2023/2841.

Article 15
Mise à disposition d'outils et de plateformes

1. L'ENISA établit, fournit, exploite, entretient et met à jour, si nécessaire, des outils techniques opérationnels, y compris des plateformes, liés à la cybersécurité au niveau de l'Union, en particulier la plateforme unique de signalement établie en vertu de l'article 16, paragraphe 1, du règlement (UE) 2024/2847 [et le guichet unique pour le

signalement des incidents établi en application de l'article 23 *bis* de la directive (UE) 2022/2555], et des outils de test pour soutenir la mise en œuvre des procédures d'évaluation de la conformité conformément à la législation pertinente de l'Union.

2. Le cas échéant, aux fins du paragraphe 1, l'ENISA coopère et échange des informations avec le réseau des CSIRT et, le cas échéant, avec les autorités de surveillance du marché.

Article 16
Services de gestion des vulnérabilités

L'ENISA développe une capacité commune de l'Union en matière de services de gestion des vulnérabilités et fournit des services de gestion des vulnérabilités aux parties prenantes:

(a) en tenant à jour la base de données européenne des vulnérabilités établie conformément à l'article 12, paragraphe 2, de la directive (UE) 2022/2555;

(b) en fournissant des services de gestion des vulnérabilités aux parties prenantes, en s'appuyant sur la base de données européenne des vulnérabilités et en utilisant les informations pertinentes dont dispose l'ENISA;

(c) le cas échéant, en s'engageant dans une coopération structurée avec les organisations fournissant des programmes, des registres ou des bases de données similaires à la base de données européenne des vulnérabilités;

(d) en apportant un soutien actif aux CSIRT désignés comme coordinateurs conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555, en ce qui concerne la gestion de la divulgation coordonnée des vulnérabilités susceptibles d'avoir un impact important sur des entités de plusieurs États membres;

(e) en élaborant et en tenant à jour des méthodes et des mécanismes de gouvernance pour l'identification des vulnérabilités et leur divulgation coordonnée, en coopération avec les autorités nationales compétentes, les CSIRT, l'industrie et la communauté de la recherche.

Section 3

Certification et normalisation en matière de cybersécurité

Article 17
Certification en matière de cybersécurité

1. L'ENISA contribue à l'élaboration et à la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité établie au titre III du présent règlement et en assure la promotion. L'ENISA est chargée:

   (a) de préparer des schémas européens de certification de cybersécurité candidats (ci-après dénommés «schémas candidats») pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités conformément à l'article 74 et, le cas échéant, d'élaborer des spécifications techniques conformément à l'article 77;

   (b) de tenir à jour les schémas européens de certification de cybersécurité adoptés conformément à l'article 75, y compris en vue d'un éventuel réexamen des

schémas européens de certification de cybersécurité adoptés conformément à l'article 76;

(c) de promouvoir l'adoption des schémas adoptés et de tenir à jour un site web spécifique fournissant des informations sur les schémas européens de certification de cybersécurité, les certificats de cybersécurité européens et les déclarations de conformité de l'UE, et les rendant publics, conformément à l'article 79;

(d) d'organiser le renforcement des capacités liées aux processus de certification, aux activités d'évaluation, ainsi qu'à l'examen et à l'évaluation par les pairs, notamment en apportant un soutien aux États membres qui en font la demande conformément à l'article 6, point 12).

2. L'ENISA assiste la Commission dans les activités suivantes:

(a) la gouvernance du GECC conformément à l'article 90;

(b) l'organisation d'une assemblée européenne de la certification de cybersécurité, conformément à l'article 72, paragraphe 1;

(c) les actions relatives à la reconnaissance internationale des certificats de cybersécurité européens conformément à l'article 87.

(d) l'organisation d'examens par les pairs, conformément à l'article 89;

(e) l'élaboration de dispositions types à faire figurer dans les schémas européens de certification de cybersécurité pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités conformément à l'article 81, paragraphe 5.

Article 18
Normalisation, spécifications techniques et orientations

1. L'ENISA élabore des spécifications techniques et des orientations pour soutenir la mise en œuvre de la législation de l'Union dans le domaine de la cybersécurité. Lorsqu'elle élabore ces spécifications techniques, l'ENISA tient compte des normes européennes et internationales existantes ainsi que d'autres spécifications techniques pertinentes. Elle veille à la cohérence de ses spécifications techniques et de ses orientations.

2. En vue de soutenir les politiques de l'Union liées à la cybersécurité, l'ENISA surveille les activités de développement de la normalisation au niveau de l'Union et, conformément à l'article 9, au niveau international, et, le cas échéant, y prend part et les dirige.

3. L'ENISA soutient la mise au point et l'évaluation d'algorithmes cryptographiques. Lorsqu'un algorithme cryptographique fait l'objet d'une évaluation positive par l'ENISA, celle-ci coopère, conformément au règlement (UE) nº 1025/2012, avec les organismes européens de normalisation pour soutenir la normalisation de l'algorithme.

4. L'ENISA fournit des conseils techniques à la Commission et, le cas échéant, aux États membres sur les normes ou spécifications techniques appropriées à l'appui des politiques de l'Union liées à la cybersécurité, y compris pour la législation d'harmonisation de l'Union dans le domaine de la cybersécurité, en particulier le règlement (UE) 2024/2847, sur les domaines techniques aux fins de l'article 25 de la

directive (UE) 2022/2555 et sur les schémas européens de certification de cybersécurité conformément à l'article 81, paragraphe 1, point d).

5. L'ENISA assiste la Commission dans l'évaluation des projets de normes harmonisées visant à soutenir la mise en œuvre de la législation d'harmonisation de l'Union dans le domaine de la cybersécurité.

6. L'ENISA promeut l'adoption de normes européennes et internationales en matière de cybersécurité.

7. L'ENISA exécute les tâches visées aux paragraphes 1 à 6 avec intégrité, impartialité et en toute confidentialité, y compris en mettant fin à sa participation à des organismes techniques spécifiques ou en la suspendant si cette participation est à l'origine d'un conflit avec d'autres tâches ou objectifs.

Section 4
Mise en œuvre de l'académie des compétences en matière de cybersécurité

Article 19
Cadre européen de compétences en matière de cybersécurité

1. L'ENISA élabore et met à la disposition du public un cadre européen de compétences en matière de cybersécurité (ci-après l'«ECSF»). Avant de mettre l'ECSF à la disposition du public ou de le mettre à jour conformément au paragraphe 4, l'ENISA consulte la Commission.

2. L'ECSF définit les profils des professionnels de la cybersécurité et associe des tâches, des compétences et des connaissances spécifiques à un profil de fonction donné. Le recours à l'ECSF est facultatif pour les entités publiques et privées.

3. L'ENISA peut consulter les parties prenantes dans le cadre de l'élaboration et de l'adoption de l'ECSF.

4. L'ENISA évalue régulièrement la nécessité de mettre à jour l'ECSF et, le cas échéant, l'actualise.

Article 20
Élaboration, adoption et maintenance des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité

1. L'ENISA élabore, adopte et tient à jour des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité L'utilisation de programmes d'attestation individuelle européenne des compétences en matière de cybersécurité est facultative pour les organismes publics nationaux et les entités privées, sauf disposition contraire du droit national.

2. Avant de lancer un nouveau programme d'attestation individuelle européenne des compétences en matière de cybersécurité, l'ENISA consulte la Commission. L'ENISA n'adopte ce programme qu'après avis favorable de la Commission. Dans le cadre de l'élaboration d'un programme d'attestation individuelle européenne des compétences en matière de cybersécurité, l'ENISA peut consulter les parties prenantes concernées.

3. Un programme d'attestation individuelle européenne des compétences en matière de cybersécurité comprend les éléments suivants:

(a) l'objet et le champ d'application du programme d'attestation sur la base des profils de fonction de l'ECSF ou de leurs sous-ensembles;

(b) les exigences applicables aux personnes formées pour effectuer des évaluations (ci-après les «évaluateurs») conformément à l'article 21, les compétences, les connaissances et l'expérience nécessaires ainsi que les méthodes de formation;

(c) l'analyse de la pénétration sur le marché spécifique à chaque programme d'attestation;

(d) les acquis d'apprentissage, les méthodes d'évaluation et les conditions que les fournisseurs d'attestation agréés doivent utiliser pour évaluer qu'une personne fournit pour apporter la preuve des compétences requises conformément à l'article 21;

(e) le cas échéant, un ou plusieurs niveaux de compétence;

(f) les règles relatives à la conservation des documents par les fournisseurs d'attestation agréés;

(g) le contenu et le format des attestations individuelles européennes des compétences en matière de cybersécurité, en tenant dûment compte de l'article 21, paragraphe 5, point e);

(h) la durée maximale de validité des attestations individuelles européennes des compétences en matière de cybersécurité délivrées dans le cadre du programme.

4. Un programme d'attestation individuelle européenne des compétences en matière de cybersécurité peut inclure le coût indicatif d'une attestation individuelle européenne des compétences en matière de cybersécurité.

5. L'ENISA veille à une coopération étroite avec les États membres tout au long de l'élaboration des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité.

6. La modification d'un programme d'attestation individuelle européenne des compétences en matière de cybersécurité n'affecte pas l'agrément accordé en vertu de l'article 22, paragraphe 3, point a), qui reste valable pour la période pour laquelle il est accordé.

Article 21
Fournisseurs d'attestation agréés

1. Les fournisseurs d'attestation agréés évaluent si les personnes satisfont aux exigences d'un programme d'attestation individuelle européenne des compétences en matière de cybersécurité et, lorsque ces exigences sont respectées, délivrent des attestations individuelles européennes des compétences en matière de cybersécurité. Les fournisseurs d'attestation agréés peuvent détenir plusieurs agréments, chacun étant accordé pour un programme d'attestation individuelle européenne des compétences en matière de cybersécurité donné.

2. L'ENISA fournit des orientations aux évaluateurs et leur dispense une formation obligatoire en ce qui concerne les exigences et les méthodes d'évaluation figurant dans le programme d'attestation individuelle européenne des compétences en matière de cybersécurité mentionnées à l'article 20, paragraphe 3, point b).

3. Les entités qui souhaitent devenir fournisseurs d'attestation agréés ou renouveler leur agrément (ci-après les «demandeurs») soumettent une demande à l'ENISA. Elles satisfont aux exigences suivantes:

(a) elles ont la personnalité juridique;

(b) elles sont capables d'exécuter les tâches définies dans le présent règlement en ce qui concerne les attestations individuelles européennes des compétences en matière de cybersécurité, que l'évaluation soit effectuée par le fournisseur d'attestation agréé lui-même ou en son nom et sous sa responsabilité;

(c) elles disposent des moyens nécessaires pour exécuter de manière appropriée les tâches techniques et administratives relatives au programme d'attestation individuelle européenne des compétences en matière de cybersécurité et ont accès à tous les équipements ou installations nécessaires.

Aux fins du premier alinéa, point b), toute sous-traitance ou consultation de personnel externe est documentée de manière appropriée, ne fait intervenir aucun intermédiaire et fait l'objet d'un accord écrit couvrant, entre autres, la confidentialité et les conflits d'intérêts.

4. Les demandeurs ne doivent pas être des fournisseurs à haut risque.

5. Les fournisseurs d'attestation agréés satisfont aux obligations suivantes:

(a) pour la mise en œuvre de chaque programme d'attestation individuelle européenne des compétences en matière de cybersécurité:

(i) ils disposent des évaluateurs et du personnel nécessaires pour exécuter en temps utile leurs activités telles qu'elles sont établies dans ce programme;

(ii) ils veillent à ce que les évaluateurs respectent le secret professionnel, à ce qu'ils soient impartiaux et à ce qu'ils accomplissent leur travail de manière indépendante et avec la plus haute intégrité professionnelle;

(iii) ils disposent de procédures écrites pour exercer leurs activités dans le cadre du programme pour lequel ils sont agréés.

(b) ils n'évaluent pas leurs propres évaluateurs ou ne leur délivrent pas d'attestations individuelles européennes des compétences en matière de cybersécurité;

(c) ils veillent, le cas échéant en mettant en place des garanties appropriées, à ce que leurs évaluateurs puissent accomplir leur tâche de manière indépendante, en particulier lorsqu'ils appartiennent à leur propre structure ou sont employés ou en formation auprès de celle-ci;

(d) ils ne se livrent à aucune activité susceptible d'entrer en conflit avec l'indépendance de jugement ou l'intégrité de leurs évaluateurs;

(e) ils veillent à ce que, à la demande de la personne concernée, les attestations électroniques individuelles européennes des compétences en matière de cybersécurité soient délivrées sous la forme d'attestations électroniques d'attributs dans un format pouvant être stocké dans les portefeuilles européens d'identité numérique prévus par le règlement (UE) nº 910/2014.

6. Les fournisseurs d'attestation agréés informent immédiatement l'ENISA si l'une des exigences énumérées aux paragraphes 3 et 4 ou l'une des obligations énumérées au

paragraphe 5 n'est plus respectée ou si le respect de ces exigences ou obligations est mis en doute, y compris en ce qui concerne l'indépendance des évaluateurs.

7. Les fournisseurs d'attestation agréés peuvent percevoir une redevance des particuliers pour l'évaluation et la délivrance des attestations individuelles européennes des compétences en matière de cybersécurité, en tenant compte du coût indicatif d'une attestation individuelle européenne des compétences en matière de cybersécurité conformément à l'article 20, paragraphe 4, lequel coût est rendu public sur un site web spécifique conformément à l'article 23, point d).

8. Les demandeurs et les fournisseurs d'attestation agréés permettent à l'ENISA de procéder à des évaluations dans le cadre de la procédure de demande ou du maintien de l'agrément et de partager toutes les informations pertinentes pour garantir que les exigences énoncées aux paragraphes 3 et 4 ou les obligations énoncées au paragraphe 5 sont respectées ou continuent d'être respectées conformément à l'article 22, paragraphe 2.

Article 22

Examen des demandes introduites en vue de devenir un fournisseur d'attestation agréé et maintien des agréments

1. Les demandeurs versent une redevance à l'ENISA pour l'examen de leur demande. Les fournisseurs d'attestation agréés versent une redevance à l'ENISA pour le maintien de leur agrément.

2. L'ENISA évalue si les exigences énoncées à l'article 21, paragraphes 3 et 4, et les obligations énoncées à l'article 21, paragraphe 5, sont respectées ou continuent d'être respectées par les demandeurs et les fournisseurs d'attestation agréés.

3. Après avoir examiné une demande au regard des exigences énoncées à l'article 21, paragraphes 3 et 4, l'ENISA peut prendre l'une des décisions suivantes:

   (a) accorder au demandeur le statut de fournisseur d'attestation agréé ou le renouveler;

   (b) rejeter la demande de statut de fournisseur d'attestation agréé ou ne pas renouveler ce statut;

   (c) clôturer le traitement de la demande si un demandeur n'a pas répondu à une demande d'informations complémentaires de l'ENISA.

   L'ENISA peut modifier, suspendre ou révoquer ces décisions sur la base de l'évaluation qu'elle mène en application de l'article 22, paragraphe 2, ou dans le cas prévu à l'article 21, paragraphe 6.

4. L'ENISA prend la décision visée au paragraphe 3 dans un délai de trois mois à compter de la date de dépôt d'une demande introduite conformément à l'article 21, paragraphe 3. Lorsque l'ENISA a demandé des informations complémentaires au demandeur, elle rend la décision visée au paragraphe 3 dans un délai d'un mois à compter de la réception des informations complémentaires.

5. La décision visée au paragraphe 3, point a), a une durée de validité maximale de trois ans et indique le montant de la redevance liée au maintien annuel de l'agrément.

6. L'ENISA veille à ce que ses activités liées à l'élaboration et à l'adoption de programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, telles que prévues à l'article 20, soient strictement séparées et menées

indépendamment des activités relatives à l'examen des demandes et aux évaluations énoncées aux paragraphes 2 et 3 du présent article.

Article 23
Information du public

L'ENISA gère et met régulièrement à jour un site web spécifique fournissant au public des informations sur les aspects suivants:

(a) l'ECSF, y compris le cadre et son calendrier de mise à jour;

(b) les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, leur état d'avancement et le calendrier prévu pour leur développement;

(c) les redevances associées à chaque programme d'attestation individuelle européenne des compétences en matière de cybersécurité adopté en vertu de l'article 47 du présent règlement;

(d) le coût indicatif d'une attestation individuelle européenne des compétences en matière de cybersécurité conformément à l'article 20, paragraphe 4;

(e) la liste des fournisseurs d'attestation agréés.

Chapitre III
Organisation de l'ENISA

Article 24
Structure administrative et de gestion de l'ENISA

La structure administrative et de gestion de l'ENISA comprend:

(a) un conseil d'administration, qui exerce les fonctions définies à l'article 28;

(b) un conseil exécutif, qui exerce les fonctions définies à l'article 30;

(c) un directeur exécutif, qui exerce les responsabilités définies à l'article 32;

(d) un directeur exécutif adjoint, qui exerce les responsabilités définies à l'article 34;

(e) un groupe consultatif de l'ENISA;

(f) une commission de recours, qui exerce les fonctions définies aux articles 39 à 42.

Section 1
Conseil d'administration

Article 25
Composition du conseil d'administration

1. Le conseil d'administration est composé d'un membre nommé par chaque État membre, et de deux membres nommés par la Commission. Tous les membres disposent du droit de vote.

2. Chaque membre du conseil d'administration dispose d'un suppléant. Les suppléants représentent les membres en leur absence.

3. Chaque État membre nomme le responsable d'une autorité nationale compétente désignée conformément à l'article 8, paragraphe 1, de la directive (UE) 2022/2555 en

tant que membre du conseil d'administration. Lorsque cela n'est pas possible, les États membres nomment un représentant à haut niveau d'une autorité nationale compétente désignée conformément à l'article 8, paragraphe 1, de la directive (UE) 2022/2555 en tant que membre du conseil d'administration.

4. Les membres du conseil d'administration nommés par la Commission et les suppléants sont nommés sur la base de leurs connaissances dans le domaine de la cybersécurité, compte tenu de leurs compétences dans le domaine de la gestion, de l'administration et du budget. En ce qui concerne les suppléants, la Commission et les États membres s'efforcent de parvenir à une représentation équilibrée des hommes et des femmes au sein du conseil d'administration et de limiter le roulement à ces postes afin d'assurer la continuité des travaux du conseil d'administration.

5. La durée du mandat des membres nommés par les États membres est égale à la durée de leur fonction visée au paragraphe 3.

6. La durée du mandat des suppléants et des membres nommés par la Commission est de quatre ans. Ce mandat est renouvelable.

Article 26
Présidence du conseil d'administration

1. Le conseil d'administration élit un président et un vice-président parmi ses membres disposant du droit de vote. Le président et le vice-président sont élus à la majorité des deux tiers des membres du conseil d'administration disposant du droit de vote.

2. Le vice-président remplace d'office le président lorsque celui-ci n'est pas en mesure d'assumer ses fonctions.

3. La durée du mandat du président et du vice-président est de quatre ans, renouvelable une fois. Cependant, si le président ou le vice-président perd sa qualité de membre du conseil d'administration à un moment quelconque de son mandat, ledit mandat expire automatiquement à cette date.

Article 27
Réunions du conseil d'administration

1. Le président convoque le conseil d'administration.

2. Le directeur exécutif participe aux réunions du conseil d'administration sans droit de vote.

3. Le conseil d'administration tient au moins deux réunions ordinaires par an. En outre, il se réunit à l'initiative de son président, à la demande de la Commission ou à la demande d'au moins un tiers de ses membres.

4. Un représentant du Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité établi par le règlement (UE) 2021/887 assiste en qualité d'observateur permanent, sans droit de vote, aux réunions du conseil d'administration.

5. Le conseil d'administration peut inviter toute personne dont l'avis peut présenter un intérêt à assister à une réunion, ou à une partie d'une réunion, en qualité d'observateur ad hoc, sans droit de vote et sous réserve du règlement intérieur du conseil d'administration.

6. Les membres du conseil d'administration et leurs suppléants peuvent, dans le respect du règlement intérieur du conseil d'administration, être assistés au cours des réunions du conseil d'administration par des conseillers ou des experts.

Article 28
Fonctions du conseil d'administration

1. Le conseil d'administration:

(a) fixe l'orientation générale du fonctionnement de l'ENISA et veille à ce que l'ENISA travaille conformément aux règles et principes énoncés dans le présent règlement; il assure aussi la cohérence des travaux de l'ENISA avec les activités menées par les États membres ainsi qu'au niveau de l'Union;

(b) adopte le projet de document unique de programmation de l'ENISA visé à l'article 44, avant de le soumettre pour avis à la Commission;

(c) adopte, en tenant compte de l'avis de la Commission, le document unique de programmation de l'ENISA conformément à l'article 29, paragraphe 2, point a);

(d) supervise la mise en œuvre des programmes annuel et pluriannuel contenus dans le document unique de programmation;

(e) adopte le budget annuel de l'ENISA conformément à l'article 29, paragraphe 2, point b), et exerce d'autres fonctions en ce qui concerne le budget de l'ENISA conformément au chapitre IV;

(f) évalue et adopte le rapport annuel consolidé sur les activités de l'ENISA, y compris les comptes et une description de la manière dont l'ENISA a atteint ses indicateurs de performance; transmet, au plus tard le 1er juillet de l'année suivante, le rapport annuel et l'évaluation de ce rapport au Parlement européen, au Conseil, à la Commission et à la Cour des comptes; publie le rapport annuel;

(g) adopte les règles financières applicables à l'ENISA, conformément à l'article 50;

(h) adopte une stratégie antifraude qui est proportionnée aux risques de fraude compte tenu de l'analyse coûts-bénéfices des mesures à mettre en œuvre;

(i) assure un suivi adéquat des conclusions et recommandations découlant de rapports d'audit et d'évaluations internes ou externes, ainsi que d'enquêtes de l'Office européen de lutte antifraude (OLAF) et du Parquet européen;

(j) adopte son règlement intérieur, y compris les règles relatives aux décisions provisoires sur la délégation de tâches spécifiques, en vertu de l'article 30, paragraphe 7;

(k) conformément au paragraphe 2 du présent article, exerce, à l'égard du personnel de l'ENISA, les compétences conférées par le statut des fonctionnaires de l'Union européenne (ci-après dénommé «statut») et par le régime applicable aux autres agents de l'Union européenne (ci-après dénommé «régime applicable aux autres agents») fixés par le règlement (CEE, Euratom, CECA) nº 259/68 du Conseil[73] respectivement à l'autorité investie du pouvoir

[73] JO L 56 du 4.3.1968, p. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.

de nomination et à l'autorité habilitée à conclure des contrats d'engagement, (ci-après dénommées «compétences dévolues à l'autorité investie du pouvoir de nomination»);

(l) adopte les règles d'exécution visant à donner effet au statut et au régime applicable aux autres agents, conformément à l'article 110, paragraphe 2, du statut des fonctionnaires;

(m) nomme le directeur exécutif et, s'il décide de créer la fonction de directeur exécutif adjoint, le directeur exécutif adjoint et, le cas échéant, prolonge leur mandat ou les démet de leurs fonctions conformément à l'article 31;

(n) nomme un comptable, soumis au statut des fonctionnaires et au régime applicable aux autres agents, qui est indépendant dans l'exercice de ses fonctions;

(o) prend toutes les décisions relatives à la mise en place des structures internes de l'ENISA et, le cas échéant, à leur modification, en tenant compte des besoins liés à l'activité de l'ENISA et en respectant le principe d'une gestion budgétaire saine;

(p) autorise la conclusion d'arrangements de travail conformément à l'article 68;

(q) autorise la conclusion d'arrangements de travail, conformément à l'article 70;

(r) nomme et révoque les membres de la commission de recours conformément à l'article 29, paragraphe 2, point d);

(s) adopte des règles de prévention et de gestion des conflits d'intérêts concernant les membres de la commission de recours.

2. Conformément à l'article 110, paragraphe 2, du statut, le conseil d'administration adopte une décision fondée sur l'article 2, paragraphe 1, du statut et sur l'article 6 du régime applicable aux autres agents, déléguant au directeur exécutif les compétences correspondantes dévolues à l'autorité investie du pouvoir de nomination et définissant les conditions dans lesquelles cette délégation de compétences peut être suspendue. Le directeur exécutif peut sous-déléguer ces compétences.

3. Lorsque des circonstances exceptionnelles l'exigent, le conseil d'administration peut adopter une décision en vue de suspendre temporairement la délégation au directeur exécutif des compétences dévolues à l'autorité investie du pouvoir de nomination ainsi que les compétences dévolues à l'autorité investie du pouvoir de nomination sous-déléguées par le directeur exécutif, pour les exercer lui-même ou les déléguer à l'un de ses membres ou à un membre du personnel autre que le directeur exécutif.

Article 29
Règles de vote du conseil d'administration

1. Le conseil d'administration prend ses décisions à la majorité absolue de ses membres disposant du droit de vote, sauf disposition contraire du présent règlement.

2. Une majorité des deux tiers des membres du conseil d'administration disposant du droit de vote est requise pour:

(a) adopter le document unique de programmation visé à l'article 28, paragraphe 1, point c).

(b) adopter le budget annuel visé à l'article 28, paragraphe 1, point e).

(c) nommer le directeur exécutif et le directeur exécutif adjoint visés aux articles 31 et 33, proroger leur mandat ou les révoquer;

(d) nommer et révoquer les membres de la commission de recours en application de l'article 36;

3. Les décisions en matière de budget ou de ressources humaines, en particulier les questions visées à l'article 28, paragraphe 1, points c), e), f), g), h), i), k), l), m) et n), ne sont adoptées que si les représentants de la Commission expriment un vote favorable. Aux fins de l'adoption des décisions visées à l'article 28, paragraphe 1, point c), concernant le document unique de programmation de l'ENISA, le vote favorable du représentant de la Commission n'est requis que sur les éléments de la décision qui ne sont pas liés aux programmes de travail annuel et pluriannuel de l'ENISA.

4. Chaque membre ayant le droit de vote dispose d'une voix. En l'absence d'un membre disposant du droit de vote, son suppléant peut exercer son droit de vote.

5. Le président du conseil d'administration prend part au vote.

6. Le directeur exécutif ne prend pas part au vote.

7. Le règlement intérieur du conseil d'administration fixe les modalités détaillées du vote, notamment les conditions dans lesquelles un membre peut agir au nom d'un autre membre.

Section 2
Conseil exécutif

Article 30
Conseil exécutif

1. Le conseil d'administration est assisté d'un conseil exécutif.

2. Le conseil exécutif:

(a) prépare les décisions qui doivent être adoptées par le conseil d'administration;

(b) assure, conjointement avec le conseil d'administration, un suivi adéquat des conclusions et recommandations découlant des rapports d'audit et des évaluations internes ou externes, ainsi que des enquêtes de l'OLAF et du Parquet européen;

(c) sans préjudice des responsabilités du directeur exécutif définies à l'article 32, assiste et conseille le directeur exécutif dans la mise en œuvre des décisions du conseil d'administration, en vue de renforcer la surveillance de la gestion administrative et budgétaire.

3. Le conseil exécutif est composé du président du conseil d'administration, d'un représentant de la Commission au conseil d'administration et de trois autres membres nommés par le conseil d'administration parmi ses membres disposant du droit de vote. Le président du conseil d'administration est également le président du conseil exécutif. Les nominations des membres du conseil exécutif visent à assurer une représentation hommes-femmes équilibrée au sein du conseil exécutif. Le directeur exécutif participe aux réunions du comité exécutif sans droit de vote.

4. La durée du mandat des membres du conseil exécutif est de quatre ans. Ce mandat est renouvelable. Le mandat des membres du conseil exécutif prend fin lorsque ces derniers cessent d'être membres du conseil d'administration.

5. Le conseil exécutif se réunit au moins tous les trois mois en session ordinaire. En outre, il se réunit soit à l'initiative de son président, soit à la demande de ses membres.

6. Le conseil d'administration établit le règlement intérieur du conseil exécutif.

7. Lorsque l'urgence le requiert, le conseil exécutif peut prendre certaines décisions provisoires au nom du conseil d'administration, en particulier sur des questions de gestion administrative, comme la suspension de la délégation des compétences dévolues à l'autorité investie du pouvoir de nomination, et sur des questions budgétaires. De telles décisions provisoires sont notifiées sans retard indu. Le conseil d'administration décide ensuite s'il approuve ou s'il rejette la décision provisoire trois mois au plus tard après cette prise de décision. Le conseil exécutif ne prend pas de décisions au nom du conseil d'administration qui doivent être approuvées par une majorité des deux tiers des membres du conseil d'administration sans droit de vote.

Section 3
Directeur exécutif

Article 31
Nomination, prolongation du mandat et révocation

1. Le directeur exécutif est nommé par le conseil d'administration sur la base de ses qualités et de ses compétences, à partir de la liste de candidats proposée par la Commission, à l'issue d'une procédure de sélection ouverte et transparente.

2. Avant d'être nommé, le candidat retenu par le conseil d'administration est invité à faire une déclaration devant la commission concernée du Parlement européen et à répondre aux questions des députés.

3. Le directeur exécutif est engagé en tant qu'agent temporaire de l'ENISA conformément à l'article 2, point a), du régime applicable aux autres agents.

4. Aux fins de la conclusion du contrat avec le directeur exécutif, l'ENISA est représentée par le président du conseil d'administration.

5. La durée du mandat du directeur exécutif est de cinq ans. En temps utile avant la fin de cette période, la Commission procède à un examen qui tient compte d'une évaluation du travail accompli par le directeur exécutif et des tâches et défis futurs de l'ENISA.

6. Le conseil d'administration, sur proposition de la Commission tenant compte de l'évaluation visée au paragraphe 5, peut prolonger une fois le mandat du directeur exécutif, pour une durée n'excédant pas cinq ans.

7. Un directeur exécutif dont le mandat a été prorogé ne peut participer à une autre procédure de sélection pour le même poste au terme de la prolongation de son mandat.

8. Le conseil d'administration informe le Parlement européen de son intention de proroger le mandat du directeur exécutif conformément au paragraphe 6. Dans les trois mois précédant cette prorogation, le directeur exécutif fait, s'il y est invité, une

déclaration devant la commission concernée du Parlement européen et répond aux questions des députés.

9. Le directeur exécutif ne peut être démis de ses fonctions que sur décision du conseil d'administration, statuant sur proposition de la Commission.

Article 32
Tâches et responsabilités du directeur exécutif

1. Le directeur exécutif gère l'ENISA et rend compte au conseil d'administration.
2. Le directeur exécutif est indépendant dans l'exécution de ses tâches et ne sollicite ni n'accepte aucune instruction d'aucune administration ni d'aucun autre organisme.
3. Le directeur exécutif fait rapport au Parlement européen sur l'exécution de ses tâches lorsqu'il y est invité. Le Conseil peut inviter le directeur exécutif à lui faire rapport sur l'exécution de ses tâches.
4. Le directeur exécutif est le représentant légal de l'ENISA.
5. Le directeur exécutif est chargé de la mise en œuvre des missions confiées à l'ENISA par le présent règlement. En particulier, le directeur exécutif est chargé:
   (a) d'assurer l'administration courante de l'ENISA;
   (b) de mettre en œuvre les décisions adoptées par le conseil d'administration;
   (c) de veiller au respect des règles financières de l'ENISA;
   (d) de préparer le projet de document unique de programmation et de le soumettre au conseil d'administration pour approbation, avant qu'il ne soit soumis pour avis à la Commission;
   (e) de mettre en œuvre le document unique de programmation et de rendre compte de sa mise en œuvre au conseil d'administration;
   (f) de préparer le rapport annuel consolidé sur les activités de l'ENISA, y compris la mise en œuvre du programme de travail annuel de l'ENISA, et de le présenter au conseil d'administration pour évaluation et adoption;
   (g) de préparer un plan d'action faisant suite aux conclusions des évaluations rétrospectives de l'ENISA visées à l'article 121 et de faire rapport tous les deux ans à la Commission sur les progrès accomplis;
   (h) d'élaborer un plan d'action donnant suite aux conclusions des rapports d'audit et évaluations internes ou externes et aux enquêtes effectuées par l'OLAF et par le Parquet européen, et de présenter des rapports semestriels à la Commission et des rapports réguliers au conseil d'administration sur les progrès accomplis;
   (i) de préparer le projet de règles financières applicables à l'ENISA visé à l'article 50;
   (j) de préparer le projet d'état prévisionnel des recettes et dépenses de l'ENISA et d'exécuter son budget;
   (k) de protéger les intérêts financiers de l'Union par l'application de mesures de prévention de la fraude, de la corruption et de toute autre activité illégale, sans préjudice des pouvoirs d'enquête de l'OLAF et du Parquet européen, par des contrôles efficaces ainsi que, si des irrégularités sont constatées, par le

recouvrement des montants indûment versés et, s'il y a lieu, par des sanctions administratives et financières, qui soient effectives, proportionnées et dissuasives;

(l) d'élaborer une stratégie antifraude, une stratégie visant à réaliser des gains d'efficacité et des synergies, une stratégie de coopération avec les pays tiers ou les organisations internationales, ainsi qu'une stratégie pour la gestion organisationnelle et les systèmes de contrôle interne, pour l'ENISA, et de les présenter au conseil d'administration pour approbation;

(m) d'établir et de maintenir le contact avec le secteur des entreprises et les organisations de consommateurs afin d'assurer un dialogue régulier avec les parties prenantes concernées;

(n) d'échanger régulièrement des points de vue et des informations avec les entités concernées de l'Union en ce qui concerne leurs activités liées à la cybersécurité afin de veiller à la cohérence dans la mise en œuvre de la politique de l'Union dans ce domaine;

(o) de promouvoir la diversité et l'équilibre entre les sexes en ce qui concerne le recrutement du personnel de l'ENISA;

(p) d'adopter des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, tels que visés à l'article 20, paragraphe 1;

(q) d'adopter des décisions à l'égard des demandeurs souhaitant devenir des fournisseurs d'attestation agréés ou renouveler leur agrément, conformément à l'article 22, paragraphe 3;

(r) d'exécuter les autres tâches qui sont assignées au directeur exécutif par le présent règlement.

6. En tant que de besoin et dans le cadre des objectifs et tâches de l'ENISA, le directeur exécutif peut créer des groupes de travail ad hoc composés d'experts, y compris des experts des autorités compétentes des États membres. Le directeur exécutif en informe le conseil d'administration au préalable. Les procédures concernant en particulier la composition des groupes de travail, la nomination par le directeur exécutif des experts qui composent les groupes de travail et le fonctionnement de ces groupes sont précisées dans les règles internes de fonctionnement de l'ENISA.

7. Lorsque cela s'avère nécessaire, à l'effet d'exécuter les tâches de l'ENISA de manière efficiente et efficace et sur la base d'une analyse coûts-bénéfices appropriée, le directeur exécutif peut décider d'établir un ou plusieurs bureaux locaux dans un ou plusieurs États membres. Avant de prendre une décision sur l'établissement d'un bureau local, le directeur exécutif demande l'avis des États membres concernés, notamment l'État membre dans lequel est situé le siège de l'ENISA, et obtient le consentement préalable de la Commission et du conseil d'administration. En cas de désaccord, au cours de la procédure de consultation, entre le directeur exécutif et les États membres concernés, la question est soumise au Conseil pour discussion. Les effectifs agrégés de l'ensemble des bureaux locaux sont maintenus au minimum et ne dépassent pas 40 % des effectifs totaux de l'ENISA en place dans l'État membre où se situe le siège de l'ENISA. Les effectifs de chaque bureau local ne dépassent pas 10 % des effectifs totaux de l'ENISA en place dans l'État membre où se situe le siège de l'ENISA.

8. La décision établissant un bureau local précise la portée des activités confiées à ce bureau local de manière à éviter des coûts inutiles et une duplication des fonctions administratives de l'ENISA.

Section 4
Directeur exécutif adjoint

Article 33
Directeur exécutif adjoint

1. Le conseil d'administration peut décider de créer une fonction de directeur exécutif adjoint pour assister le directeur exécutif.

2. Si le conseil d'administration décide de créer une fonction de directeur exécutif adjoint, les dispositions de l'article 31 s'appliquent au directeur exécutif adjoint en conséquence.

Article 34
Tâches et responsabilités du directeur exécutif adjoint

Le directeur exécutif adjoint assiste le directeur exécutif dans la gestion de l'ENISA et dans l'exécution des tâches visées à l'article 32. Si le directeur exécutif est absent ou empêché, ou si le poste est vacant, le directeur exécutif adjoint remplace le directeur exécutif pendant la durée de son absence ou jusqu'à ce que le poste soit pourvu.

Section 5
Groupe consultatif de l'ENISA

Article 35
Groupe consultatif de l'ENISA

1. Le conseil d'administration crée de manière transparente, sur proposition du directeur exécutif, le groupe consultatif de l'ENISA. Le groupe consultatif de l'ENISA est composé d'experts reconnus représentant les parties prenantes concernées, telles que le secteur de la cybersécurité, le secteur des TIC, les PME, les entités opérant dans les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555, les fabricants de produits comportant des éléments numériques et les intendants de logiciels ouverts au sens du règlement (UE) 2024/2847, les organismes d'évaluation de la conformité notifiés au titre du cadre européen de certification de cybersécurité visé à l'article 93 et du règlement (UE) 2024/2847, les entités opérant dans le domaine des moyens d'identification électronique, les groupes de consommateurs, les experts universitaires dans le domaine de la cybersécurité, les organisations européennes de normalisation, ainsi que les autorités répressives et de contrôle de la protection des données. Ces experts reconnus sont des ressortissants des États membres. Le conseil d'administration s'efforce d'assurer un équilibre approprié entre les hommes et les femmes et un équilibre géographique, ainsi qu'un équilibre entre les différents groupes de parties prenantes.

2. Les procédures applicables au groupe consultatif de l'ENISA, notamment en ce qui concerne sa composition, la proposition du directeur exécutif visée au paragraphe 1, le nombre de membres et leur nomination, ainsi que le fonctionnement du groupe

consultatif de l'ENISA sont précisées dans les règles internes de fonctionnement de l'ENISA et sont rendues publiques.

3. Le groupe consultatif de l'ENISA est présidé par le directeur exécutif ou par toute personne qu'il désigne à cet effet au cas par cas.

4. La durée du mandat des membres du groupe consultatif de l'ENISA est de deux ans et demi et le mandat est renouvelable une fois. Les membres du conseil d'administration ne peuvent pas être membres du groupe consultatif de l'ENISA. Des experts de la Commission et des États membres sont autorisés à assister aux réunions et à prendre part aux travaux du groupe consultatif de l'ENISA. Le directeur exécutif peut inviter des représentants d'autres organismes qui ne sont pas membres du groupe consultatif de l'ENISA à assister aux réunions du groupe consultatif de l'ENISA et à prendre part à ses travaux.

5. Le groupe consultatif de l'ENISA conseille l'ENISA en ce qui concerne l'exécution des tâches de celle-ci, excepté l'application des dispositions des titres III, IV et V du présent règlement. Il conseille en particulier le directeur exécutif pour ce qui est de l'élaboration d'une proposition de programme de travail annuel pour l'ENISA et de la communication à assurer avec les parties prenantes concernées sur les questions liées au programme de travail annuel.

6. Le groupe consultatif de l'ENISA informe régulièrement le conseil d'administration de ses activités.

7. L'ENISA fournit le soutien logistique nécessaire au conseil consultatif et assure le secrétariat de ses réunions.

Section 6
Commission de recours

Article 36
Création et composition de la commission de recours

1. L'ENISA établit une commission de recours par décision du conseil d'administration.

2. La commission de recours est composée d'un président et de trois autres membres. Chaque membre de la commission de recours a un suppléant. Les suppléants représentent les membres en leur absence.

3. Le conseil d'administration nomme le président, les autres membres ainsi que leurs suppléants à partir d'une liste de candidats qualifiés établie par la Commission. La liste des candidats qualifiés reste valable pour une durée de quatre ans. La validité de cette liste peut être prolongée par le conseil d'administration pour des périodes additionnelles de quatre ans, sur proposition de la Commission.

4. Lorsque la commission de recours considère que la nature du recours l'exige, elle peut demander au conseil d'administration de nommer deux membres supplémentaires et leurs suppléants à partir de la liste visée au paragraphe 3.

5. La commission de recours adopte son règlement intérieur et le rend public.

Article 37
Membres de la commission de recours

1. La durée du mandat des membres et des suppléants de la commission de recours est de quatre ans. Leur mandat peut être renouvelé par le conseil d'administration pour des périodes additionnelles de quatre ans, sur proposition de la Commission.

2. Les membres de la commission de recours sont indépendants et n'exercent pas d'autres fonctions au sein de l'ENISA. Lorsqu'ils prennent leurs décisions, ils ne sollicitent ni ne suivent les instructions d'aucun gouvernement ni d'aucun autre organisme ou entité du secteur privé.

3. Les membres de la commission de recours ne peuvent pas être démis de leurs fonctions ni retirés de la liste des candidats qualifiés au cours de leur mandat, sauf s'il existe des motifs graves pour ce faire et si le conseil d'administration, sur proposition de la Commission, prend une décision à cet effet.

Article 38
Exclusion et récusation

1. Les membres de la commission de recours ne prennent part à aucune procédure de recours s'ils ont un intérêt personnel dans celle-ci, s'ils ont déjà représenté une des parties à la procédure ou s'ils ont participé à l'adoption de la décision faisant l'objet du recours.

2. Si, pour une des raisons visées au paragraphe 1 ou pour toute autre raison, un membre d'une commission de recours estime qu'il ne peut prendre part à une procédure de recours, il en informe la commission de recours.

3. Une partie à la procédure de recours peut récuser un membre d'une commission de recours, quel qu'il soit, pour l'un des motifs visés au paragraphe 1, ou en cas de suspicion de partialité. Une telle récusation n'est pas recevable si, ayant connaissance d'un motif de récusation, la partie à la procédure de recours en cause a posé un acte de procédure. Aucune récusation ne peut être fondée sur la nationalité des membres de la commission de recours.

4. La commission de recours décide des mesures à prendre dans les cas visés aux paragraphes 2 et 3, sans la participation du membre concerné. Aux fins de cette décision, le membre concerné est remplacé à la commission de recours par son suppléant.

Article 39
Recours contre une décision et recours en carence

1. Les recours suivants peuvent être formés devant la commission de recours:

   (a) des recours contre les décisions adoptées par l'ENISA conformément à l'article 22, paragraphe 3;

   (b) des recours en carence lorsque l'ENISA s'abstient d'agir dans les délais applicables fixés à l'article 22, paragraphe 4.

2. Un recours formé en vertu du paragraphe 1 fait l'objet d'une révision préjudicielle conformément à l'article 41 avant d'être soumis à l'examen de la commission de recours.

3. Un recours introduit en application du paragraphe 1 n'a pas d'effet suspensif.

Article 40
Personnes admises à former un recours, délais et forme

1. Les demandeurs au sens de l'article 21, paragraphe 3, peuvent former

   (a) un recours contre une décision de l'ENISA qui leur est adressée, en application de l'article 22, paragraphe 3;

   (b) un recours en carence contre l'ENISA lorsque celle-ci s'est abstenue d'agir dans les délais applicables fixés à l'article 22, paragraphe 4, en ce qui concerne une demande qu'ils ont introduite auprès d'elle.

2. Dans le cas visé au paragraphe 1, point a), le recours est formé par écrit, avec indication de ses motifs, conformément au règlement intérieur visé à l'article 36, paragraphe 5, dans un délai de deux mois à compter de la notification de la décision au demandeur concerné ou, à défaut, du jour où celui-ci en a eu connaissance.

3. Dans le cas visé au paragraphe 1, point b), le recours est formé par écrit devant l'ENISA conformément au règlement intérieur visé à l'article 36, paragraphe 5, dans un délai de deux mois à compter de l'expiration du délai fixé à l'article 22, paragraphe 4.

Article 41
Réformation préjudicielle

1. Si l'ENISA estime que le recours est recevable et fondé, elle corrige sa décision ou son absence d'action visées à l'article 40, paragraphe 1.

2. Si l'ENISA ne corrige pas sa décision dans un délai d'un mois à compter de la réception du recours, elle décide aussitôt si elle suspend ou non l'application de sa décision et défère le recours à la commission de recours.

Article 42
Examen des décisions sur les recours

1. La commission de recours décide de faire droit ou non au recours dans un délai de trois mois à compter de sa présentation. Lorsqu'elle examine un recours, la commission de recours agit dans les délais fixés par son règlement intérieur. Elle invite aussi souvent qu'il est nécessaire les parties à la procédure de recours à présenter, dans un délai imparti, des observations sur les notifications qu'elle leur adresse ou sur les communications qui émanent des autres parties. Les parties à la procédure de recours sont autorisées à présenter oralement leurs observations.

2. Lorsque la commission de recours estime que le recours est fondé, elle renvoie l'affaire à l'ENISA. Celle-ci arrête sa décision définitive en conformité avec les conclusions de la commission de recours et motive ladite décision. L'ENISA informe les parties à la procédure de recours en conséquence.

Article 43
Recours devant la Cour de justice de l'Union européenne

1. Les recours en annulation des décisions de l'ENISA prises en application de l'article 22, paragraphe 3, ou pour absence d'action dans les délais applicables en vertu de l'article 22, paragraphe 4, peuvent être formés devant la Cour de justice de l'Union européenne après épuisement de la voie de recours interne de l'ENISA

prévue aux articles 39 à 42 ou en cas d'absence d'action dans les délais applicables en vertu de l'article 41, paragraphe 2.

2. L'ENISA prend toutes les mesures nécessaires pour se conformer à l'arrêt de la Cour de justice de l'Union européenne.

Section 7
Fonctionnement

Article 44
Document unique de programmation

1. L'ENISA opère conformément à un document unique de programmation qui décrit ses programmes de travail annuel et pluriannuel, et qui contient l'ensemble de ses activités planifiées.

2. Le directeur exécutif établit chaque année un projet de document unique de programmation, tel que mentionné au paragraphe 1, ainsi que la planification des ressources financières et humaines correspondantes, conformément à l'article 32 du règlement délégué (UE) 2019/715 de la Commission[74], en tenant compte des lignes directrices fixées par la Commission.

3. Au plus tard le 30 novembre de chaque année, le conseil d'administration adopte le document unique de programmation visé au paragraphe 1, en tenant compte de l'avis de la Commission visé à l'article 32, paragraphe 7, du règlement délégué (UE) 2019/715. Si le conseil d'administration décide de ne pas tenir compte de certains éléments de l'avis de la Commission, il fournit une justification détaillée de cette décision. Le conseil d'administration transmet le document unique de programmation au Parlement européen, au Conseil et à la Commission au plus tard le 31 janvier de l'année suivante, ainsi que toute version de ce document actualisée ultérieurement.

4. Le document unique de programmation devient définitif après l'adoption définitive du budget général de l'Union et il est adapté en tant que de besoin.

5. Le programme de travail annuel expose des objectifs détaillés et les résultats escomptés, notamment des indicateurs de performance. Il contient en outre une description des actions à financer et une indication des ressources financières et humaines allouées à chaque action, conformément aux principes d'établissement du budget par activités et de la gestion fondée sur les activités. Le programme de travail annuel s'inscrit dans la logique du programme de travail pluriannuel visé au paragraphe 7. Il indique clairement les tâches qui ont été ajoutées, modifiées ou supprimées par rapport à l'exercice précédent.

6. Le conseil d'administration modifie le programme de travail annuel adopté lorsqu'une nouvelle tâche est assignée à l'ENISA. Toute modification substantielle du programme de travail annuel est soumise à une procédure d'adoption identique à celle applicable au programme de travail annuel initial. Le conseil d'administration

[74] Règlement délégué (UE) 2019/715 de la Commission du 18 décembre 2018 portant règlement financier-cadre des organismes créés en vertu du traité sur le fonctionnement de l'Union européenne et du traité Euratom et visés à l'article 70 du règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil (JO L 122 du 10.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).

peut déléguer au directeur exécutif le pouvoir d'apporter des modifications non substantielles au programme de travail annuel.

7. Le programme de travail pluriannuel expose la programmation stratégique globale comprenant les objectifs, les résultats escomptés et les indicateurs de performance. Il définit également la programmation des ressources, notamment le budget pluriannuel et les effectifs.

8. La programmation des ressources est actualisée chaque année. La programmation stratégique est actualisée en tant que de besoin, notamment pour tenir compte, si nécessaire, des résultats de l'évaluation visée à l'article 120.

CHAPITRE IV
Établissement et structure du budget de l'ENISA

Article 45
Établissement du budget de l'ENISA

1. Chaque année, le directeur exécutif établit un avant-projet d'état prévisionnel des recettes et des dépenses de l'ENISA pour l'exercice suivant, comprenant le tableau des effectifs, et le transmet au conseil d'administration.

2. L'avant-projet d'état prévisionnel se fonde sur les objectifs et les résultats escomptés du programme de travail annuel et tient compte des ressources financières nécessaires pour atteindre ces objectifs et ces résultats escomptés, conformément au principe de bonne gestion financière et de performance.

3. Le conseil d'administration adopte, sur la base de l'avant-projet d'état prévisionnel, un projet d'état prévisionnel des recettes et dépenses de l'ENISA pour l'exercice suivant et le transmet à la Commission au plus tard le 31 janvier de chaque année.

4. La Commission transmet le projet d'état prévisionnel à l'autorité budgétaire en même temps que le projet de budget général de l'Union. Le projet d'état prévisionnel est également mis à la disposition de l'ENISA.

5. Sur la base du projet d'état prévisionnel, la Commission inscrit dans le projet de budget général de l'Union les prévisions qu'elle estime nécessaires pour le tableau des effectifs ainsi que le montant de la contribution à charge du budget général, et saisit l'autorité budgétaire conformément aux articles 313 et 314 du TFUE.

6. L'autorité budgétaire autorise les crédits au titre de la contribution du budget général de l'Union à l'ENISA.

7. L'autorité budgétaire arrête le tableau des effectifs de l'ENISA.

8. Le conseil d'administration adopte le budget de l'ENISA. Celui-ci devient définitif après l'adoption définitive du budget général de l'Union et, si nécessaire, est adapté en conséquence.

9. Le règlement délégué (UE) 2019/715 s'applique à tout projet immobilier susceptible d'avoir des incidences notables sur le budget de l'ENISA.

Article 46
Structure du budget de l'ENISA

1. Un état prévisionnel de toutes les recettes et dépenses de l'ENISA est préparé pour chaque exercice et est inscrit au budget de l'ENISA. L'exercice financier coïncide avec l'année civile.

2. Le budget de l'ENISA est équilibré en recettes et en dépenses.

3. Sans préjudice d'autres ressources, les recettes de l'ENISA sont constituées:

   (a) d'une contribution de l'Union inscrite au budget général de l'Union;

   (b) de recettes allouées à des postes de dépense spécifiques conformément à ses règles financières visées à l'article 50;

   (c) d'un financement de l'Union sous la forme de conventions de contribution ou de subventions ad hoc, conformément aux règles financières applicables à l'ENISA visées à l'article 50 et aux dispositions des instruments pertinents appuyant les politiques de l'Union;

   (d) des redevances perçues auprès des demandeurs pour les activités liées aux programmes d'attestation individuelle européenne des compétences en matière de cybersécurité visés à l'article 22, paragraphe 1;

   (e) des redevances perçues auprès des organismes d'évaluation de la conformité pour la participation à des certificats de cybersécurité européens et pour la délivrance de ces derniers dans le cadre d'un schéma européen de certification de cybersécurité, telles que visées à l'article 47, paragraphe 2;

   (f) des redevances perçues auprès des autorités publiques ou des organismes privés pour des outils de test, telles que visées à l'article 47, paragraphe 3;

   (g) de toute contribution de pays tiers participant aux travaux de l'ENISA en vertu de l'article 70, paragraphe 4;

   (h) de toute contribution volontaire des États membres en espèces ou en nature.

4. Les États membres qui apportent des contributions volontaires telles que visées au paragraphe 3, point g), ne peuvent prétendre à aucun droit ou service spécifique du fait de celles-ci.

5. Les dépenses de l'ENISA comprennent la rémunération du personnel, les dépenses administratives et d'infrastructure et les frais de fonctionnement.

Article 47
Redevances

1. En ce qui concerne chaque activité relative au programme d'attestation européenne visée à l'article 22, paragraphe 1, les redevances suivantes sont perçues auprès des demandeurs au sens de l'article 21, paragraphe 3, ou auprès des fournisseurs d'attestation agréés afin de contribuer à couvrir l'intégralité des coûts des activités menées par l'ENISA:

   (a) la délivrance d'agréments après un examen portant sur le respect des exigences énoncées à l'article 21, paragraphes 3 et 4, y compris la réalisation d'évaluations;

   (b) le maintien annuel de l'agrément;

(c) le renouvellement des agréments pour les fournisseurs d'attestations individuelles européennes des compétences en matière de cybersécurité, y compris la réalisation d'évaluations.

2. En ce qui concerne la certification, les redevances suivantes sont perçues auprès des organismes d'évaluation de la conformité pour la maintenance des schémas européens de certification de cybersécurité dans le cadre desquels des certificats de cybersécurité européens sont délivrés, en particulier:

(a) une redevance annuelle pour la participation à un schéma européen de certification de cybersécurité;

(b) une redevance pour la délivrance de certificats de cybersécurité européens dans le cadre de schémas européens de certification de cybersécurité.

Les redevances visées au point b) sont perçues lorsque l'organisme d'évaluation de la conformité soumet des certificats de cybersécurité européens à l'ENISA en vue de leur publication sur son site internet conformément à l'article 79.

3. Une redevance est perçue auprès de toute autorité publique ou de tout organisme privé pour l'utilisation des outils de test visés à l'article 15, paragraphe 1.

4. Les redevances sont exprimées et perçues en euros.

5. La Commission adopte des actes d'exécution établissant des règles détaillées relatives à la détermination des redevances à percevoir par l'ENISA, précisant notamment les coûts estimés imputables à chacune des activités pour lesquelles des redevances au titre des paragraphes 1, 2 et 3 sont exigibles, et les montants individuels des redevances exigibles, ainsi que les modalités et conditions de paiement. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2. La Commission consulte l'ENISA lors de l'élaboration de ces projets d'actes d'exécution.

6. Les redevances déterminées par les actes d'exécution visés au paragraphe 5 sont fixées à l'avance, sont proportionnées aux coûts estimés des activités réalisées ou des services fournis, de manière à respecter un rapport coût-efficacité satisfaisant, et sont suffisantes pour couvrir ces coûts. Les coûts à couvrir tiennent compte de toutes les dépenses de l'ENISA attribuées au personnel participant aux activités visées aux paragraphes 1, 2 et 3. Le montant des redevances est fixé de façon à éviter un déficit ou une accumulation importante d'excédents dans le budget de l'ENISA. Les excédents budgétaires générés par les redevances sont reportés pour financer les activités de l'ENISA, en particulier les activités futures liées aux redevances, ou compenser les pertes subies. Si un solde budgétaire positif significatif résultant d'activités couvertes par des redevances devient récurrent, ou si un solde négatif important résulte de la fourniture des services facturés, la Commission modifie les actes d'exécution visés au paragraphe 5 afin de réviser la méthode de calcul des redevances conformément à l'article 118, paragraphe 2.

Le montant des redevances facturées pour les tâches visées au paragraphe 1 est fixé à un niveau assurant des recettes suffisantes pour couvrir les coûts des activités liées au développement et à la maintenance des programmes d'attestation individuelle européenne, au traitement des demandes et à la délivrance et au renouvellement des agréments, ainsi que les activités de supervision nécessaires incombant à l'ENISA.

Le montant des redevances facturées pour les tâches visées au paragraphe 2 est fixé à un niveau assurant des recettes suffisantes pour couvrir la totalité des coûts des

activités liées à la maintenance des schémas européens de certification de cybersécurité, telle que décrite à l'article 75.

Le montant des redevances facturées pour les tâches visées au paragraphe 3 est fixé à un niveau assurant des recettes suffisantes pour couvrir les coûts des activités liées à la fourniture d'outils de test, telle que mentionnée à l'article 15, paragraphe1.

7. L'ENISA fournit un rapport sur les redevances perçues et leur incidence sur son budget dans le cadre de la procédure de reddition des comptes prévue à l'article 50.

8. L'ENISA met en place un ensemble d'indicateurs pour mesurer la charge de travail, l'efficacité et l'efficience en ce qui concerne les activités financées au moyen de redevances. L'ENISA adapte ses prévisions en termes d'effectifs et sa gestion des ressources liées aux redevances en conséquence afin d'être en mesure de répondre de manière adéquate à cette demande et à toute fluctuation des recettes tirées des redevances. L'ENISA communique le rapport à la Commission, qui peut l'utiliser aux fins de l'évaluation visée à l'article 120, paragraphe 1.

Article 48
Exécution du budget de l'ENISA

1. Le directeur exécutif est responsable de l'exécution du budget de l'ENISA et exerce les fonctions d'ordonnateur.

2. L'auditeur interne de la Commission exerce à l'égard de l'ENISA les mêmes pouvoirs que ceux qui lui sont attribués à l'égard des services de la Commission.

3. Le directeur exécutif transmet chaque année à l'autorité budgétaire toute information pertinente quant aux résultats des procédures d'évaluation.

Article 49
Présentation des comptes et décharge

1. Le comptable de l'ENISA transmet les comptes provisoires pour l'exercice (exercice N) au comptable de la Commission et à la Cour des comptes au plus tard le 1er mars de l'exercice suivant (exercice N + 1).

2. Le comptable de l'ENISA fournit également les informations comptables nécessaires à des fins de consolidation au comptable de la Commission, selon les modalités et le format définis par ce dernier au plus tard le 1er mars de l'exercice N + 1.

3. L'ENISA transmet le rapport sur la gestion budgétaire et financière pour l'exercice N au Parlement européen, au Conseil, à la Commission et à la Cour des comptes, au plus tard le 31 mars de l'exercice N + 1.

4. Dès réception des observations formulées par la Cour des comptes sur les comptes provisoires de l'ENISA pour l'exercice N, le comptable de l'ENISA établit, sous sa propre responsabilité, les comptes définitifs de l'ENISA. Le directeur exécutif les transmet pour avis au conseil d'administration.

5. Le conseil d'administration rend un avis sur les comptes définitifs de l'ENISA pour l'exercice N.

6. Le comptable de l'ENISA transmet, au plus tard le 1er juillet de l'exercice N + 1, au Parlement européen, au Conseil, à la Commission et à la Cour des comptes les comptes définitifs de l'exercice N, accompagnés de l'avis du conseil d'administration.

7. Un lien vers les pages web contenant les comptes définitifs de l'ENISA est publié au Journal officiel de l'Union européenne au plus tard le 15 novembre de l'exercice N + 1.

8. Le directeur exécutif adresse à la Cour des comptes, au plus tard le 30 septembre de l'exercice N + 1, une réponse aux observations formulées par celle-ci dans son rapport annuel. Le directeur exécutif adresse également cette réponse au conseil d'administration et à la Commission.

9. Le directeur exécutif soumet au Parlement européen, à la demande de celui-ci, toute information nécessaire au bon déroulement de la procédure de décharge pour l'exercice N, conformément à l'article 267, paragraphe 3, du règlement (UE, Euratom) 2024/2509 du Parlement européen et du Conseil.

10. Sur recommandation du Conseil statuant à la majorité qualifiée, le Parlement européen donne décharge au directeur exécutif sur l'exécution du budget de l'exercice N avant le 15 mai de l'exercice N + 2.

Article 50
Règles financières

1. Les règles financières applicables à l'ENISA sont arrêtées par le conseil d'administration, après consultation de la Commission. Elles ne peuvent s'écarter du règlement délégué (UE) 2019/715 que si le fonctionnement de l'ENISA le nécessite spécifiquement et moyennant l'accord préalable de la Commission.

2. L'ENISA établit et exécute son budget conformément à ses règles financières et au règlement (UE, Euratom) 2024/2509.

Article 51
Lutte contre la fraude

1. Aux fins de la lutte contre la fraude, la corruption et toute autre activité illégale, les dispositions du règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil[75] s'appliquent sans restriction aux activités de l'ENISA.

2. L'ENISA adhère à l'accord interinstitutionnel du 25 mai 1999 entre le Parlement européen, le Conseil de l'Union européenne et la Commission des Communautés européennes relatif aux enquêtes internes effectuées par l'Office européen de lutte antifraude (OLAF)[76] au plus tard six mois après le *[OP, veuillez insérer la date correcte prévue à l'article 127]* et arrête les dispositions appropriées, lesquelles s'appliquent à tout son personnel, au moyen du modèle figurant en annexe dudit accord.

3. La Cour des comptes dispose d'un pouvoir d'audit, sur pièces et sur place, à l'égard de tous les bénéficiaires de subventions, contractants et sous-traitants qui ont reçu des fonds de l'Union en provenance de l'ENISA.

---

75 Règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) et abrogeant le règlement (CE) nº 1073/1999 du Parlement européen et du Conseil et le règlement (Euratom) nº 1074/1999 du Conseil (JO L 248 du 18.9.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/883/oj).

76 JO L 136 du 31.5.1999, p. 15, ELI: http://data.europa.eu/eli/agree_interinstit/1999/531/oj.

4. L'OLAF peut mener des enquêtes, y compris des contrôles et vérifications sur place, en vue d'établir l'existence, le cas échéant, d'une fraude, d'un acte de corruption ou de toute autre activité illégale portant atteinte aux intérêts financiers de l'Union dans le cadre d'une subvention ou d'un marché financés par l'ENISA, conformément aux dispositions et procédures prévues par le règlement (UE, Euratom) nº 883/2013 et le règlement (Euratom, CE) nº 2185/96 du Conseil[77].

5. Sans préjudice des paragraphes 1 à 4, les accords de travail conclus avec des pays tiers et des organisations internationales, les contrats, les conventions de subvention et les décisions de subvention de l'ENISA contiennent des dispositions habilitant expressément la Cour des comptes et l'OLAF à procéder à ces audits et à ces enquêtes, conformément à leurs compétences respectives.

6. Conformément au règlement (UE) 2017/1939 du Conseil, le Parquet européen peut enquêter sur la fraude et les autres activités illégales portant atteinte aux intérêts financiers de l'Union et engager des poursuites contre les personnes impliquées, comme prévu par la directive (UE) 2017/1371 du Parlement européen et du Conseil[78].

Article 52
Déclaration d'intérêts

1. Les membres du conseil d'administration, le directeur exécutif, le directeur exécutif adjoint et les fonctionnaires détachés par les États membres à titre temporaire font chacun une déclaration d'engagements et une déclaration indiquant l'absence ou la présence de tout intérêt direct ou indirect qui pourrait être considéré comme préjudiciable à leur indépendance. Les déclarations sont exactes et complètes, faites par écrit sur une base annuelle et actualisées si nécessaire.

2. Les membres du conseil d'administration, le directeur exécutif, le directeur exécutif adjoint et les experts externes participant aux groupes de travail ad hoc déclarent chacun de manière exacte et complète, au plus tard au début de chaque réunion, les intérêts qui pourraient être considérés comme préjudiciables à leur indépendance eu égard aux points inscrits à l'ordre du jour, et s'abstiennent de prendre part aux discussions et de voter sur ces points.

3. L'ENISA fixe, dans ses règles internes de fonctionnement, les modalités pratiques concernant les règles relatives aux déclarations d'intérêt visées aux paragraphes 1 et 2.

Article 53
Transparence

1. L'ENISA exerce ses activités avec un niveau élevé de transparence et conformément à l'article 55.

---

77 Règlement (Euratom, CE) nº 2185/96 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités (JO L 292 du 15.11.1996, p. 2, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).

78 Directive (UE) 2017/1371 du Parlement européen et du Conseil du 5 juillet 2017 relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal (JO L 198 du 28.7.2017, p. 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).

2. L’ENISA veille à ce que le public et toute partie intéressée reçoivent une information appropriée, objective, fiable et facilement accessible, notamment en ce qui concerne le résultat de ses travaux. Elle rend également publiques les déclarations d’intérêt faites conformément à l’article 52.

3. Le conseil d’administration peut, sur proposition du directeur exécutif, autoriser des parties intéressées à participer en tant qu’observateurs à certaines activités de l’ENISA.

4. L’ENISA fixe, dans ses règles internes de fonctionnement, les modalités pratiques d’application des règles de transparence visées aux paragraphes 1 et 2.

Article 54
Confidentialité au sein de l’ENISA

1. Sans préjudice de l’article 55, l’ENISA ne divulgue pas à des tiers les informations qu’elle traite ou qu’elle reçoit et pour lesquelles une demande motivée de traitement confidentiel a été faite.

2. Les membres du conseil d’administration, le directeur exécutif, le directeur exécutif adjoint, les membres du groupe consultatif de l’ENISA, les experts externes participant aux groupes de travail ad hoc et les membres du personnel de l’ENISA, y compris les fonctionnaires détachés par les États membres à titre temporaire, respectent les obligations de confidentialité prévues à l’article 339 du traité sur le fonctionnement de l’Union européenne, même après la cessation de leurs fonctions.

3. L’ENISA fixe, dans ses règles internes de fonctionnement, les modalités pratiques d’application des règles de confidentialité visées aux paragraphes 1 et 2.

Article 55
Accès aux documents

1. Le règlement (CE) nº 1049/2001 s’applique aux documents détenus par l’ENISA.

2. Le conseil d’administration adopte les modalités d’application du règlement (CE) nº 1049/2001.

3. Les décisions prises par l’ENISA en application de l’article 8 du règlement (CE) nº 1049/2001 peuvent faire l’objet d’une plainte auprès du Médiateur européen au titre de l’article 228 du traité sur le fonctionnement de l’Union européenne, ou d’un recours devant la Cour de justice de l’Union européenne au titre de l’article 263 du traité sur le fonctionnement de l’Union européenne.

CHAPITRE V
Personnel et agents de liaison

Article 56
Dispositions générales

1. Le statut des fonctionnaires et le régime applicable aux autres agents, ainsi que les règles arrêtées d’un commun accord entre les institutions de l’Union visant à exécuter le statut des fonctionnaires et le régime applicable aux autres agents, s’appliquent au personnel de l’ENISA.

2. Le personnel de l'ENISA, les agents de liaison et les experts nationaux détachés auprès de l'ENISA font l'objet d'une procédure d'habilitation de sécurité appropriée.

Article 57
Privilèges et immunités

Le protocole nº 7 sur les privilèges et immunités de l'Union européenne annexé au TFUE s'applique à l'ENISA à son personnel.

Article 58
Agents de liaison

1. Chaque État membre désigne au moins deux agents de liaison issus d'une autorité nationale compétente désignée en vertu de l'article 8, paragraphe 1, de la directive (UE) 2022/2555 en tant qu'experts nationaux détachés auprès de l'ENISA pour travailler au siège de l'agence ou à son bureau local, conformément à l'article 59, paragraphe 2. La Commission peut également désigner un agent de liaison.

2. Les agents de liaison contribuent à l'exécution des tâches de l'ENISA, notamment en facilitant la coopération opérationnelle et l'échange d'informations tels que prévus à l'article 11. Les agents de liaison aident également l'ENISA à diffuser des informations sur ses activités, ses conclusions et ses recommandations auprès des parties prenantes concernées dans l'ensemble de l'Union. Ils agissent également en tant que points de contact nationaux en ce qui concerne les questions adressées par leur État membre et relatives à ce dernier, en répondant directement à ces questions ou en assurant la liaison avec leur administration nationale.

3. Les agents de liaison désignés par leurs États membres sont habilités à demander et à recevoir de leur État membre toutes les informations pertinentes, ainsi que le prévoit le présent règlement, dans le plein respect du droit national et des pratiques de leur État membre, notamment pour ce qui est de la protection des données et des règles de confidentialité.

Article 59
Experts nationaux détachés et autre personnel

1. L'ENISA peut avoir recours, dans tous ses domaines d'activité, à des experts nationaux détachés ou à d'autres personnes qu'elle n'emploie pas. Le statut des fonctionnaires et le régime applicable aux autres agents ne s'appliquent pas à ces membres du personnel.

2. Le conseil d'administration adopte une décision établissant le régime applicable aux experts nationaux détachés auprès de l'ENISA, y compris les agents de liaison.

CHAPITRE VI
Dispositions générales concernant l'ENISA

Article 60
Statut juridique de l'ENISA

1. L'ENISA est un organisme de l'Union doté de la personnalité juridique.

2. Dans chaque État membre, l'ENISA jouit de la capacité juridique la plus étendue reconnue aux personnes morales par le droit national de cet État membre. Elle peut notamment acquérir ou aliéner des biens mobiliers et immobiliers et ester en justice.

3. L'ENISA est représentée par le directeur exécutif.

Article 61
Siège

L'ENISA a son siège à Athènes (Grèce).

Article 62
Accord de siège et conditions de fonctionnement

1. Les dispositions requises pour l'implantation de l'ENISA dans l'État membre du siège et les prestations à fournir par cet État membre, ainsi que les règles particulières qui sont applicables dans ledit État membre au directeur exécutif, aux membres du conseil d'administration, au personnel de l'ENISA et aux membres de leurs familles sont arrêtées dans un accord de siège conclu entre l'ENISA et l'État membre du siège, après approbation par le conseil d'administration.

2. L'État membre du siège de l'ENISA offre les meilleures conditions possibles pour assurer le bon fonctionnement de l'ENISA, en tenant compte de l'accessibilité de l'emplacement, de l'existence de services d'éducation appropriés pour les enfants des membres du personnel et d'un accès adéquat au marché du travail, à la sécurité sociale et aux soins médicaux pour les enfants et les conjoints des membres du personnel.

Article 63
Contrôle administratif

Les activités de l'ENISA sont soumises au contrôle du Médiateur européen, conformément à l'article 228 du traité sur le fonctionnement de l'Union européenne.

Article 64
Responsabilité de l'ENISA

1. La responsabilité contractuelle de l'ENISA est régie par le droit applicable au contrat en question.

2. La Cour de justice de l'Union européenne est compétente pour statuer en vertu de toute clause compromissoire contenue dans un contrat conclu par l'ENISA.

3. En cas de responsabilité non contractuelle, l'ENISA répare tout dommage causé par ses services ou par son personnel dans l'exercice de leurs fonctions, conformément aux principes généraux communs aux législations des États membres.

4. La Cour de justice de l'Union européenne est compétente pour connaître des litiges concernant la réparation des dommages visés au paragraphe 3.

5. La responsabilité personnelle des membres du personnel de l'ENISA envers l'ENISA est régie par les dispositions du statut ou du régime applicable aux autres agents qui leur sont applicables.

Article 65
Régime linguistique

1. Le règlement nº 1 du Conseil[79] s'applique à l'ENISA. Les États membres et les autres organismes désignés par les États membres peuvent s'adresser à l'ENISA et recevoir une réponse dans la langue officielle des institutions de l'Union qu'ils choisissent.

2. Les services de traduction et tous les autres services linguistiques requis pour le fonctionnement de l'ENISA, à l'exception de l'interprétation, sont assurés par le Centre de traduction des organes de l'Union européenne.

Article 66
Protection des données à caractère personnel

1. Les opérations de traitement de données à caractère personnel effectuées par l'ENISA sont soumises au règlement (UE) 2018/1725.

2. Le conseil d'administration adopte les dispositions d'application visées à l'article 45, paragraphe 3, du règlement (UE) 2018/1725. Le conseil d'administration peut adopter des mesures supplémentaires nécessaires pour l'application du règlement (UE) 2018/1725 par l'ENISA.

Article 67
Règles de sécurité en matière de protection des informations sensibles non classifiées et des informations classifiées

En accord avec la Commission, l'ENISA adopte des règles de sécurité en appliquant les principes de sécurité énoncés dans les règles de sécurité de la Commission visant à protéger les informations sensibles non classifiées et les ICUE, énoncées dans les décisions (UE, Euratom) 2015/443[80] et (UE, Euratom) 2015/444[81]. Ces règles de sécurité comprennent des dispositions relatives à l'échange, au traitement et à l'archivage de ces informations.

Article 68
Coopération avec les entités de l'Union et les autorités nationales

1. Afin d'assurer la cohérence, de créer des synergies et de traiter les questions d'intérêt commun, l'ENISA coopère sur les questions liées à la cybersécurité avec le CERT-UE et les entités de l'Union concernées, y compris Europol, le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité établi en vertu du règlement (UE) 2021/887 et le comité européen de la protection des données institué en vertu de l'article 68, paragraphe 1, du règlement (UE) 2016/679.

2. La coopération visée au paragraphe 1 peut notamment prendre les formes suivantes:

---

79 Règlement nº 1 du Conseil portant fixation du régime linguistique de la Communauté économique européenne (JO 17 du 6.10.1958, p. 385, ELI: http://data.europa.eu/eli/reg/1958/1(1)/oj).

80 Décision (UE, Euratom) 2015/443 de la Commission du 13 mars 2015 relative à la sécurité au sein de la Commission (JO L 72 du 17.3.2015, p. 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj).

81 Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53, ELI: http://data.europa.eu/eli/dec/2015/444/oj).

(a) l’échange de savoir-faire et de meilleures pratiques;

(b) la fourniture de conseils et de lignes directrices sur des questions liées à la cybersécurité;

(c) l’établissement de modalités pratiques de l’exécution de tâches spécifiques, après consultation de la Commission.

3. L’ENISA pratique avec le CERT-UE une coopération structurée, en particulier sur les questions liées au renforcement des capacités, à la coopération opérationnelle et aux analyses stratégiques à long terme des cybermenaces.

4. L’ENISA coopère et échange des informations avec les autorités de surveillance du marché et de contrôle compétentes désignées en vertu de la législation de l’Union dans le domaine de la cybersécurité, y compris le règlement (UE) 2024/2847.

Article 69
Coopération avec les parties prenantes

1. Lorsque la réalisation des objectifs du présent règlement l'exige, l’ENISA coopère avec les parties prenantes concernées, telles que le secteur de la cybersécurité, le secteur des TIC, les PME, les entités opérant dans les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555, les fabricants, les importateurs ou les distributeurs de produits comportant des éléments numériques au sens du règlement (UE) 2024/2847, les organismes d’évaluation de la conformité notifiés au titre du cadre européen de certification de cybersécurité et du règlement (UE) 2024/2847, les entités opérant dans le domaine des moyens d’identification électronique, les groupes de consommateurs et les experts universitaires dans le domaine de la cybersécurité. À cette fin, l’ENISA peut établir des partenariats public-privé.

2. L’ENISA soutient, en consultation avec la Commission, la coopération entre les organismes d’évaluation de la conformité notifiés conformément à l’article 93. En particulier, elle peut créer un groupe d’organismes d’évaluation de la conformité notifiés pour partager les meilleures pratiques, en créant des synergies avec d’autres actes législatifs pertinents de l’Union, en particulier le règlement (UE) 2024/2847.

Article 70
Coopération avec des pays tiers et des organisations internationales

1. Dans la mesure nécessaire pour atteindre les objectifs du présent règlement, l’ENISA peut coopérer avec les autorités compétentes de pays tiers ou avec des organisations internationales, ou les deux, conformément aux priorités de l'Union. À cet effet, l’ENISA peut établir des arrangements de travail avec les autorités de pays tiers et des organisations internationales, sous réserve de l’accord préalable de la Commission. Ces arrangements de travail ne créent pas d’obligations juridiques à l’égard de l’Union ou de ses États membres.

2. Le conseil d’administration adopte une stratégie en ce qui concerne les relations avec les pays tiers et les organisations internationales sur les questions relevant de la compétence de l’ENISA, et conformément aux priorités visées au paragraphe 1. La Commission veille à ce que l’ENISA fonctionne dans les limites de son mandat et du cadre institutionnel existant en concluant des arrangements de travail appropriés avec le directeur exécutif.

3. Afin de soutenir la coopération avec les pays tiers, en particulier les pays candidats à l'adhésion à l'Union, l'ENISA peut apporter son expertise en matière de renforcement des capacités, notamment dans les domaines suivants:

   (a) l'évaluation du niveau de maturité des capacités et des ressources en matière de cybersécurité;

   (b) la croissance et le renforcement de la main-d'œuvre dans le domaine de la cybersécurité, notamment en promouvant l'ECSF et les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, et en proposant des activités d'apprentissage et de formation;

   (c) l'aide à la planification et à l'exécution d'exercices de cybersécurité.

4. Les travaux de l'ENISA sont ouverts à la participation de pays tiers qui ont conclu des accords en ce sens avec l'Union. Conformément aux dispositions pertinentes d'accords conclus entre des pays tiers et l'Union, des arrangements de travail sont élaborés, sous réserve de l'accord préalable de la Commission, pour préciser notamment la nature, l'étendue et les modalités de la participation de ces pays tiers aux travaux de l'ENISA, et contiennent des dispositions relatives à la participation aux initiatives prises par l'ENISA, aux contributions financières et au personnel. En ce qui concerne les questions relatives au personnel, lesdits arrangements de travail respectent en tout état de cause le statut et le régime applicable aux autres agents.

5. L'ENISA fait régulièrement rapport au Conseil et à la Commission sur la mise en œuvre des arrangements de travail visés aux paragraphes 1 et 4.

TITRE III

CADRE EUROPÉEN DE CERTIFICATION DE CYBERSÉCURITÉ

CHAPITRE I
Objet, champ d'application et procédures

Article 71

Objet et champ d'application du cadre européen de certification de cybersécurité

1. Le cadre européen de certification de cybersécurité est établi en vue de créer un marché unique numérique pour les produits TIC, services TIC, processus TIC, services de sécurité gérés et entités. À cette fin, il augmente le niveau de cybersécurité au sein de l'Union, permet une approche harmonisée des schémas européens de certification de cybersécurité et tire parti de la certification afin de faciliter le respect de la législation applicable de l'Union.

2. Le cadre européen de certification de cybersécurité prévoit un mécanisme permettant d'établir des schémas européens de certification de cybersécurité et d'attester:

   a) que les produits TIC, services TIC et processus TIC qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services qui sont offerts par lesdits produits, services et processus ou accessibles par leur intermédiaire tout au long de leur cycle de vie;

b) que les services de sécurité gérés qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité des données qui sont consultées, traitées, stockées ou transmises dans le cadre de la fourniture de ces services, et que ces services sont fournis en permanence avec la compétence, l'expertise et l'expérience requises par un personnel possédant un niveau suffisant et approprié de connaissances techniques pertinentes et d'intégrité professionnelle;

c) que la posture de cybersécurité d'une entité qui a été évaluée conformément à ces schémas est conforme aux exigences de cybersécurité spécifiées.

3. La certification de cybersécurité européenne est volontaire, sauf disposition contraire du droit de l'Union ou du droit national.

4. Les certificats de cybersécurité européen et les déclarations de conformité de l'UE délivrés au titre du cadre européen de certification de cybersécurité sont automatiquement reconnus dans tous les États membres.

Article 72
Information et consultation du public

1. Au moins une fois par an, la Commission organise, avec le soutien de l'ENISA, une assemblée européenne de la certification de cybersécurité, à laquelle elle invite les membres du GECC et d'autres experts compétents des États membres, les experts compétents des entités de l'Union et les parties prenantes concernées à débattre des priorités stratégiques en matière d'harmonisation dans le domaine de la certification de cybersécurité.

2. La Commission gère et met régulièrement à jour un site web spécifique fournissant des informations sur les aspects suivants:

a) les schémas européens de certification de cybersécurité dont la préparation est demandée conformément à l'article 73;

b) les priorités stratégiques pour l'harmonisation des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés, de la posture de cybersécurité des entités ou des exigences de sécurité de la législation de l'Union, y compris les domaines potentiels pour lesquels un schéma européen de certification de cybersécurité pourrait être demandé.

3. La Commission met à la disposition du public, sur le site internet visé au paragraphe 2 du présent article, les informations relatives à sa demande, adressée à l'ENISA, de préparer un schéma candidat tel que visé à l'article 73 et à sa décision d'accepter, de rejeter ou d'interrompre un schéma candidat transmis par l'ENISA conformément à l'article 74, paragraphe 7.

4. Au cours de la préparation d'un schéma candidat par l'ENISA, en vertu de l'article 74, le Parlement européen et le Conseil peuvent demander à la Commission, en sa qualité de président du GECC, et à l'ENISA, de présenter des informations pertinentes sur le projet de schéma candidat. À la demande du Parlement européen ou du Conseil, l'ENISA, en accord avec la Commission, et sans préjudice de l'article 54, peut mettre à la disposition du Parlement européen et du Conseil des parties pertinentes d'un projet de schéma candidat d'une manière adaptée au niveau de confidentialité requis et, le cas échéant, de manière restreinte.

5. Le Parlement européen et le Conseil peuvent inviter la Commission et l'ENISA à débattre de questions concernant la mise en œuvre de schémas européens de certification de cybersécurité pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités.

Article 73

Demandes de schéma européen de certification de cybersécurité

1. La Commission peut demander à l'ENISA de préparer un schéma européen de certification de cybersécurité candidat pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités.

2. Dans des cas dûment justifiés, le GECC peut suggérer à la Commission de présenter une demande visée au paragraphe 1.

3. La demande visée au paragraphe 1 précise l'objet, la portée et les modalités de la réalisation des objectifs et éléments de sécurité pertinents énoncés aux articles 80 et 81. La demande précise également le plan de préparation du schéma européen de certification de cybersécurité candidat et les spécifications techniques pertinentes à référencer ou à définir dans le schéma.

4. Lorsqu'elle prépare la demande visée au paragraphe 1, la Commission consulte dûment l'ENISA et le GECC et tient compte des avis de toutes les parties prenantes et autres entités de l'Union concernées, y compris, le cas échéant, celles qui sont pertinentes en vertu de la législation de l'Union dans laquelle un schéma européen de certification de cybersécurité démontre la conformité et fournit une présomption de conformité.

Article 74

Préparation et adoption des schémas européens de certification de cybersécurité

1. Au plus tard 12 mois après avoir reçu une demande de la Commission en vertu de l'article 73, sauf indication contraire dans la demande, l'ENISA prépare un schéma européen de certification de cybersécurité candidat qui satisfait aux exigences énoncées aux articles 80 et 81.

2. Pour la préparation de chaque schéma candidat, l'ENISA crée un groupe de travail ad hoc, conformément à l'article 32, paragraphe 6, afin qu'il lui fournisse des avis d'experts.

3. Lors de la préparation du schéma candidat, l'ENISA coopère étroitement avec le GECC. Celui-ci fournit aide et expertise à l'ENISA dans le cadre de la préparation du schéma candidat et, le cas échéant, des spécifications techniques d'appui.

4. Lors de la préparation du schéma candidat, y compris, le cas échéant, les spécifications techniques d'appui, l'ENISA consulte en temps utile les parties prenantes au moyen d'un processus de consultation formel, ouvert, transparent et inclusif. L'ENISA coopère également avec les autorités publiques compétentes des États membres et avec les entités de l'Union concernées afin de recueillir leurs avis d'experts en ce qui concerne la préparation du schéma candidat et, le cas échéant, les spécifications techniques d'appui. Lorsqu'elle transmet le schéma candidat à la Commission en vertu du paragraphe 6, l'ENISA décrit la manière dont elle s'est conformée au présent paragraphe.

5. Avant de transmettre à la Commission le schéma candidat et, le cas échéant, les spécifications techniques d'appui, l'ENISA demande aux membres du GECC de fournir des avis écrits sur le schéma candidat. Les avis sont fournis au plus tard 30 jours à compter de la date de la demande. L'ENISA tient le plus grand compte des avis des membres du GECC. L'absence de tels avis n'empêche pas l'ENISA de transmettre le schéma candidat à la Commission.

6. L'ENISA transmet le schéma candidat à la Commission au plus tard 60 jours à compter de la date de la demande visée au paragraphe 5.

7. Lorsqu'elle reçoit le schéma candidat, la Commission évalue si le schéma correspond à la demande formulée conformément à l'article 73. Dans les 30 jours suivant la date de transmission de ce schéma candidat, la Commission prend l'une des mesures suivantes:

   a) accepter le schéma candidat;

   b) renvoyer le schéma candidat à l'ENISA pour révision. Ce renvoi est assorti d'une justification et d'un délai ne dépassant pas 90 jours, dans lequel l'ENISA fournit un schéma candidat révisé;

   c) mettre fin au schéma candidat.

8. Lorsque la Commission renvoie un schéma candidat à l'ENISA pour révision conformément au paragraphe 7, point b), les paragraphes 4, 5 et 7 s'appliquent en conséquence.

9. La Commission, sur la base du schéma candidat accepté préparé par l'ENISA, est habilitée à adopter des actes d'exécution prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités, qui satisfait aux exigences énoncées aux articles 80 et 81. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.

10. La Commission peut faire référence aux spécifications techniques élaborées par l'ENISA dans les actes d'exécution visés au paragraphe 9 du présent article, conformément aux articles 18 et 77.

11. La Commission peut préciser les conditions de reconnaissance internationale des certificats de cybersécurité européens dans les actes d'exécution visés au paragraphe 9 du présent article, conformément à l'article 87.

Article 75

Maintenance des schémas européens de certification de cybersécurité

1. Une stratégie de maintenance est établie pour chaque schéma européen de certification de cybersécurité. La stratégie de maintenance doit définir les attentes en ce qui concerne les activités de maintenance, en particulier celles liées aux normes ou spécifications techniques référencées dans le système et à l'interaction avec les parties prenantes concernées.

2. L'ENISA, en coopération avec la Commission et avec le soutien du GECC et de son sous-groupe de maintenance concerné, assure la maintenance des schémas européens de certification de cybersécurité, y compris en vue d'un éventuel réexamen de ces schémas par la Commission. L'ENISA coopère et échange des informations avec les

entités et groupes de l'Union concernés en ce qui concerne les activités de maintenance.

3. L'ENISA peut organiser la participation du secteur privé à la maintenance d'un système sous la forme d'un groupe de travail ad hoc conformément à la stratégie de maintenance visée au paragraphe 1.

4. Les activités de maintenance des schémas européens de certification de cybersécurité comprennent les éléments suivants:

   a) l'élaboration, la mise à jour et l'approbation de spécifications techniques et de lignes directrices visant à soutenir le fonctionnement harmonisé et uniforme des schémas;

   b) l'identification de normes ou spécifications techniques pertinentes pour le schéma;

   c) les interactions et, le cas échéant, l'établissement de contacts avec les parties prenantes concernées, y compris les organisations européennes ou internationales de normalisation, notamment aux fins de fournir ou d'obtenir des contributions techniques;

   d) la publication de recommandations à la Commission sur les améliorations et les mises à jour nécessaires des schémas, y compris en vue d'un éventuel réexamen des schémas;

   e) l'échange d'informations relatives à la mise en œuvre pratique des schémas entre les États membres;

   f) les contributions aux mécanismes d'examen par les pairs et d'évaluation par les pairs et les analyses des résultats afin d'améliorer le fonctionnement des schémas et de soutenir leur éventuel réexamen.

5. Le GECC peut émettre un avis sur la maintenance des schémas européens de certification de cybersécurité.

Article 76

Évaluation, réexamen et retrait des schémas européens de certification de cybersécurité

1. Au moins tous les quatre ans après l'entrée en application d'un schéma européen de certification de cybersécurité, l'ENISA évalue l'incidence et l'efficacité de ce schéma, en coopération avec le sous-groupe «maintenance» concerné du GECC, et en tenant compte des retours d'information reçus des parties prenantes. L'ENISA procède à l'évaluation en effectuant l'analyse de marché conformément à l'article 8, paragraphe 1.

2. À la suite de l'évaluation visée au paragraphe 1, la Commission peut réexaminer ou retirer les actes d'exécution prévoyant un schéma européen de certification de cybersécurité conformément à l'article 74, paragraphe 9.

3. Lors du réexamen ou du retrait des schémas européens de certification de cybersécurité, la Commission consulte l'ENISA, le GECC et son sous-groupe de maintenance concerné, et tient compte des avis des parties prenantes concernées et d'autres entités de l'Union.

4. Le GECC peut émettre un avis sur le réexamen ou le retrait d'un schéma européen de certification de cybersécurité. La Commission en tient dûment compte lors du réexamen ou du retrait du schéma européen de certification de cybersécurité.

Article 77

Spécifications techniques des schémas européens de certification de cybersécurité

1. L'ENISA peut élaborer des spécifications techniques en vue d'un futur schéma européen de certification de cybersécurité ou à l'appui de la maintenance d'un schéma européen de certification de cybersécurité.

2. Les spécifications techniques visées au paragraphe 1 du présent article sont élaborées en temps utile, avec le soutien du GECC et de ses sous-groupes de maintenance et, le cas échéant, du groupe de travail ad hoc correspondant visé à l'article 75, paragraphe 3. À cette fin, l'ENISA sollicite également les contributions des groupes de parties prenantes concernés en tenant compte de la stratégie de maintenance visée à l'article 75, paragraphe 1.

3. Lorsque des spécifications techniques sont référencées dans un schéma européen de certification de cybersécurité conformément à l'article 74, paragraphe 10, elles sont mises à disposition sur le site internet visé à l'article 79.

4. Dans des cas dûment justifiés, en particulier lorsque les spécifications techniques contiennent des informations susceptibles de compromettre la sécurité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou de la posture de cybersécurité des entités, elles ne sont diffusées qu'aux parties prenantes concernées par les exigences du schéma. Ces spécifications techniques ne sont pas référencées dans les schémas européens de certification de cybersécurité conformément à l'article 74, paragraphe 10.

Article 78

Facilitation du respect de la législation de l'Union

1. Lorsqu'un acte juridique spécifique de l'Union le prévoit, un certificat délivré dans le cadre d'un schéma européen de certification de cybersécurité démontre le respect des exigences correspondantes énoncées dans cet acte juridique et établit la présomption de conformité.

2. Les activités d'évaluation menées dans le cadre d'un schéma européen de certification de cybersécurité sont compatibles avec l'acte juridique correspondant de l'Union établissant la démonstration du respect des exigences et la présomption de conformité. Lorsque ces activités d'évaluation ne sont pas spécifiées dans l'acte juridique correspondant de l'Union, le schéma les précise. Un organisme tiers procède à une évaluation de la conformité pour la certification conférant la présomption de conformité aux exigences énoncées dans la législation de l'Union.

3. En l'absence de législation de l'Union harmonisée, le droit national peut aussi prévoir qu'un schéma européen de certification de cybersécurité peut être utilisé pour démontrer le respect des exigences légales prévues dans le droit national et établir la présomption de conformité auxdites exigences.

Article 79

Adoption des schémas européens de certification de cybersécurité, site web de l'ENISA et publication des certificats

1. L'ENISA organise des activités visant à promouvoir l'adoption des schémas européens de certification de cybersécurité adoptés, y compris en gérant le site internet visé au paragraphe 2 du présent article.

2. L’ENISA gère et met régulièrement à jour un site web spécifique fournissant des informations publiques sur les aspects suivants:

a) les schémas européens de certification de cybersécurité;

b) les redevances liées à la maintenance de chaque schéma européen de certification de cybersécurité;

c) les spécifications techniques pertinentes de l’ENISA;

d) les certificats de cybersécurité européens et les déclarations de conformité de l’UE, y compris les informations relatives à ces certificats et déclarations qui ne sont plus valables ou qui sont suspendus ou retirés ou ont expiré;

e) les informations supplémentaires pertinentes en matière de cybersécurité fournies conformément à l’article 84;

f) les synthèses des examens par les pairs, conformément à l’article 89, paragraphe 7;

g) les spécifications techniques référencées dans les schémas européens de certification de cybersécurité en vertu de l’article 74, paragraphe 10.

3. Le cas échéant, le site internet visé au paragraphe 2 indique également les schémas nationaux de certification de cybersécurité qui ont été remplacés par un schéma européen de certification de cybersécurité.

CHAPITRE II
Contenu des schémas européens de certification de cybersécurité

Article 80
Objectifs de sécurité des schémas européens de certification de cybersécurité

1. Un schéma européen de certification de cybersécurité poursuit, selon le cas, les objectifs de sécurité suivants:

a) faire en sorte que les produits TIC, services TIC, processus TIC et services de sécurité gérés soient sécurisés par défaut et dès la conception;

b) protéger les données stockées, transmises ou traitées de toute autre façon contre le stockage, le traitement, l’accès ou la diffusion accidentels ou non autorisés à l’aide de moyens techniques appropriés, en tenant compte de l’ensemble du cycle de vie des produits TIC, services TIC ou processus TIC;

c) protéger l’intégrité des données, commandes, programmes et configurations stockés, transmis ou traités de toute autre façon, à caractère personnel ou autre, contre toute manipulation ou modification non autorisée par l’utilisateur, et signaler les corruptions, en tenant compte de l’ensemble du cycle de vie des produits TIC, services TIC ou processus TIC;

d) assurer la protection contre les accès non autorisés par des mécanismes de contrôle appropriés, y compris, mais sans s’y limiter, par des systèmes d’authentification, d’identité ou de gestion des accès et signaler tout accès non autorisé;

e) identifier et documenter les composants et les vulnérabilités, y compris, le cas échéant, en établissant une nomenclature des logiciels couvrant à tout le moins les dépendances de haut niveau;

f) fournir des informations relatives à la sécurité en enregistrant et en surveillant les activités internes pertinentes, y compris l'accès ou la modification des données, des services ou des fonctions, le cas échéant, tout en laissant à l'utilisateur la possibilité de désactiver le mécanisme;

g) vérifier que les produits TIC, services TIC et processus TIC ne contiennent pas de vulnérabilités exploitables connues;

h) protéger la disponibilité des fonctions essentielles et de base, notamment après un incident, y compris par des mesures de résilience et d'atténuation face aux attaques par déni de service;

i) réduire au minimum l'incidence négative sur la disponibilité des services fournis par d'autres réseaux et dispositifs en cas d'incident physique ou technique;

j) veiller à ce que les produits TIC, services TIC et processus TIC soient régulièrement testés et leur sécurité réexaminée;

k) veiller à ce que les vulnérabilités soient traitées et corrigées sans délai, y compris au moyen de mises à jour de sécurité, et à ce que les informations sur les vulnérabilités corrigées soient partagées et rendues publiques, à moins que les risques liés à la publication ne l'emportent sur les avantages en matière de sécurité;

l) veiller à ce qu'une politique de divulgation coordonnée des vulnérabilités soit en place;

m) faciliter le partage d'informations sur les vulnérabilités potentielles des produits TIC, services TIC et processus TIC;

n) veiller à ce que, lorsque des mises à jour de sécurité sont disponibles pour remédier à des problèmes de sécurité recensés, ces mises à jour de sécurité soient diffusées sans délai;

o) veiller à ce que les services de sécurité gérés soient fournis avec la compétence, l'expertise et l'expérience requises, notamment en s'assurant que le personnel chargé de fournir ces services possède un niveau de compétence et de connaissances techniques suffisant et approprié dans le domaine spécifique, une expérience suffisante et appropriée et la plus haute intégrité professionnelle;

p) veiller à ce que les produits TIC, services TIC et processus TIC déployés dans le cadre de la fourniture des services de sécurité gérés soient sécurisés dès la conception et par défaut et, le cas échéant, comprennent les dernières mises à jour de sécurité et ne contiennent pas de vulnérabilités notoires;

q) veiller à ce que l'entité certifiée ait mis en place des procédures internes appropriées pour garantir que les services sont fournis à un niveau de qualité suffisant et approprié;

r) veiller à ce que l'entité certifiée soit en mesure d'identifier les incidents, de se protéger contre ceux-ci, de les détecter, d'y réagir et de s'en rétablir;

s) veiller à ce que l’entité certifiée soit en mesure de gérer les risques qui menacent la sécurité des réseaux et des systèmes d’information que cette entité utilise dans le cadre de ses activités ou de la fourniture de ses services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de ses services et sur d’autres services;

t) veiller à ce que l’entité certifiée soit en mesure de développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant, directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, qu’elle a mis en place l’intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d’information qu’elle utilise, et qui sous-tendent la fourniture continue de services et leur qualité, y compris en cas de perturbations;

u) veiller à ce que l’entité certifiée soit en mesure de mettre en œuvre et de maintenir un système de gestion de la sécurité de l’information;

v) résister à tout événement susceptible de compromettre la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou traitées ou des services offerts ou accessibles par le réseau et le système d’information utilisés par l’entité, et assurer la continuité de la fourniture des services et leur qualité, y compris en cas de perturbations;

w) veiller à ce que l’entité soit en mesure d’assurer la sécurité du traitement des données à caractère personnel.

2. La Commission est habilitée à adopter des actes délégués conformément à l’article 119 en vue de modifier le paragraphe 1 du présent article en ajoutant ou en modifiant des objectifs de sécurité afin qu’ils reflètent les dernières évolutions technologiques et les nouvelles menaces connexes, ainsi que l’adoption d’une nouvelle législation de l’Union établissant la démonstration du respect des exigences et la présomption de conformité au moyen de la certification européenne de cybersécurité avec les exigences pertinentes de cette législation en matière de cybersécurité.

3. Un schéma européen de certification de cybersécurité portant sur des produits comportant des éléments numériques au sens de l’article 3, point 1), du règlement (UE) 2024/2847 est conçu conformément aux exigences essentielles de cybersécurité énoncées à l’annexe I dudit règlement et tient compte des normes harmonisées disponibles.

Article 81

Éléments des schémas européens de certification de cybersécurité

1. Un schéma européen de certification de cybersécurité comprend au moins les éléments suivants:

a) l’objet et le champ d’application du schéma de certification, notamment le type ou les catégories de produits TIC, services TIC, processus TIC ou services de sécurité gérés, ou les actifs, services et fonctions de l’entité relevant du champ d’application de la certification;

b) une description claire de la finalité du schéma et, le cas échéant, l’identification de la législation de l’Union fixant les exigences dont les certificats de

cybersécurité européens démontrent le respect et pour lesquelles ils confèrent une présomption de conformité;

c) la stratégie de maintenance précisant l'approche des activités de maintenance prévues à l'article 75;

d) les exigences, critères et méthodes spécifiques d'évaluation de la cybersécurité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou de la posture de cybersécurité des entités, et les références aux normes internationales, européennes ou nationales appliquées dans l'évaluation des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou de la posture de cybersécurité des entités ou, lorsque ces normes ne sont pas disponibles ou appropriées, aux spécifications techniques élaborées par l'ENISA conformément à l'article 77 ou, si ces spécifications ne sont pas disponibles, à d'autres spécifications techniques;

e) la durée maximale de validité des certificats de cybersécurité européens délivrés dans le cadre du schéma.

2. Un schéma européen de certification de cybersécurité comprend au moins des règles et conditions concernant les éléments suivants:

a) le contrôle du respect, par les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités, des exigences liées aux certificats de cybersécurité européens ou aux déclarations de conformité de l'UE, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité qui ont été définies;

b) la délivrance, la confirmation, le retrait et le renouvellement des certificats de cybersécurité européens, l'extension ou la réduction du champ d'application de la certification et la recertification;

c) les conséquences pour les produits TIC, services TIC, processus TIC, services de sécurité gérés ou entités qui ont été certifiés ou pour lesquels une déclaration de conformité de l'UE a été délivrée, mais qui ne respectent pas les exigences du schéma;

d) les modalités de signalement et de traitement des vulnérabilités de cybersécurité non détectées précédemment dans des produits TIC, services TIC et processus TIC;

e) le contenu et le format des certificats de cybersécurité européens et des déclarations de conformité de l'UE à délivrer;

f) la période de disponibilité de la déclaration de conformité de l'UE, de la documentation technique et de toutes les autres informations pertinentes qui doivent être mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés, ou par l'entité dont la posture de cybersécurité fait l'objet de la certification;

g) tout mécanisme d'évaluation par les pairs établi dans le cadre du schéma pour les autorités ou organismes délivrant des certificats de cybersécurité européens conformément à l'article 85, paragraphe 4, qui est sans préjudice de l'examen par les pairs prévu à l'article 90;

h) la confidentialité des informations et des données obtenues par toutes les parties dans l'exécution des tâches et activités liées à la mise en œuvre des dispositions du présent titre;

i) le format et les procédures que les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC doivent appliquer pour fournir et mettre à jour les informations supplémentaires en matière de cybersécurité conformément à l'article 84; et

j) la continuité des activités de certification dans des situations de crise extraordinaires, qui sont inévitables et entravent la possibilité d'appliquer les règles du schéma de certification.

3. Un schéma européen de certification de cybersécurité comprend également, le cas échéant, les éléments suivants:

a) un ou plusieurs niveaux d'assurance et les niveaux d'évaluation correspondants;

b) des profils de protection précisant les exigences de sécurité applicables à une catégorie donnée de produits TIC, services TIC, processus TIC ou services de sécurité gérés;

c) des profils d'extension pour définir des exigences de sécurité supplémentaires, y compris, le cas échéant, des exigences de sécurité énoncées dans les dispositions nationales transposant le droit de l'Union;

d) des précisions sur les activités d'évaluation de la conformité, y compris l'étalonnage, les essais, la certification et l'inspection, pour le niveau d'assurance «élevé» ou aux fins de démontrer le respect des exigences et d'accorder la présomption de conformité, qui sont autorisées en dehors de l'Espace économique européen (EEE);

e) l'identification des schémas nationaux ou internationaux de certification de cybersécurité couvrant le même type ou les mêmes catégories de produits TIC, services TIC, processus TIC, services de sécurité gérés ou posture de cybersécurité des entités;

f) des exigences supplémentaires ou spécifiques auxquelles sont soumis les organismes d'évaluation de la conformité aux fins de garantir qu'ils disposent des compétences techniques nécessaires pour évaluer les exigences de cybersécurité;

g) les informations nécessaires à la certification qu'un demandeur doit fournir ou mettre d'une autre manière à la disposition des organismes d'évaluation de la conformité;

h) les marques ou labels et les conditions dans lesquelles ces marques ou labels peuvent être utilisés;

i) les conditions de reconnaissance internationale des certificats de cybersécurité européens conformément à l'article 87.

4. Les exigences spécifiées du schéma européen de certification de cybersécurité sont conformes aux exigences de la législation de l'Union.

5. La Commission est habilitée à adopter des actes d'exécution établissant des principes communs et des dispositions types pour les éléments énoncés aux paragraphes 1, 2 et

3 dans l'ensemble des schémas européens de certification de cybersécurité. Le cas échéant, ces principes et dispositions types peuvent être référencés, s'ils sont disponibles, dans les schémas européens de certification de cybersécurité.

6. Les actes d'exécution visés au paragraphe 5 sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2. Lors de l'élaboration ou de la révision des principes communs et des dispositions types pour les éléments des schémas européens de certification de cybersécurité, la Commission consulte l'ENISA et tient compte, le cas échéant, des points de vue exprimés par le GECC, les parties prenantes concernées et les autres organismes concernés.

Article 82

Niveaux d'assurance et d'évaluation des schémas européens de certification de cybersécurité

1. Un schéma européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités: «élémentaire», «substantiel» ou «élevé». Ces niveaux d'assurance sont proportionnés au niveau de risque associé à l'utilisation prévue du produit TIC, service TIC, processus TIC, service de sécurité géré, ou à la nature des entités dont la posture de cybersécurité fait l'objet d'une certification, et à leur environnement opérationnel, en termes de probabilité et de conséquences d'un incident.

2. Les certificats de cybersécurité européens mentionnent tout niveau d'assurance précisé dans le schéma européen de certification de cybersécurité dans le cadre duquel lesdits certificats sont délivrés. Les déclarations de conformité de l'UE font référence au niveau d'assurance «élémentaire».

3. Les exigences de sécurité correspondant à chaque niveau d'assurance sont fournies dans le schéma européen de certification de cybersécurité concerné, y compris les contrôles de sécurité correspondants et l'évaluation correspondante à laquelle le produit TIC, le service TIC, le processus TIC, le service de sécurité géré ou la posture de cybersécurité des entités doivent être soumis.

4. Le certificat de cybersécurité européen ou la déclaration de conformité de l'UE fait référence aux spécifications techniques, aux normes et aux procédures connexes, y compris les contrôles techniques, l'objectif étant de réduire le risque d'incidents de cybersécurité ou de les prévenir.

5. Un certificat de cybersécurité européen ou une déclaration de conformité de l'UE qui se réfère au niveau d'assurance dit «élémentaire» offre l'assurance que les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités pour lesquels ce certificat ou cette déclaration de conformité de l'UE sont délivrés satisfont aux exigences de sécurité correspondantes, y compris les contrôles de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques élémentaires connus d'incidents et de cyberattaques. Les activités d'évaluation à entreprendre comprennent au moins un examen de la documentation technique. Lorsqu'un tel examen n'est pas approprié, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

6. Un certificat de cybersécurité européen qui se réfère au niveau d'assurance dit «substantiel» offre l'assurance que les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités pour lesquels ce certificat est délivré satisfont aux exigences de sécurité correspondantes,

y compris des contrôles de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques connus d'incidents et de cyberattaques et le risque d'incidents et de cyberattaques émanant d'acteurs aux aptitudes et aux ressources limitées. Les activités d'évaluation à entreprendre comprennent au moins: un examen visant à démontrer l'absence de vulnérabilités notoires et des vérifications tendant à démontrer que les produits TIC, services TIC, processus TIC, services de sécurité gérés ou entités mettent correctement en œuvre les contrôles de sécurité nécessaires. Lorsque de telles activités d'évaluation ne sont pas appropriées, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

7. Un certificat de cybersécurité européen qui se réfère au niveau d'assurance dit «élevé» offre l'assurance que les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités pour lesquels ce certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des contrôles de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques d'incidents et de cyberattaques de pointe émanant d'acteurs aux aptitudes solides et aux ressources importantes. Les activités d'évaluation à entreprendre comprennent au moins les éléments suivants:

   a) un examen visant à démontrer l'absence de vulnérabilités notoires;

   b) des tests visant à démontrer que les produits TIC, services TIC, processus TIC, services de sécurité gérés ou entités mettent correctement en œuvre les contrôles de sécurité correspondant à l'état de la technique;

   c) une évaluation de la résistance des produits TIC, services TIC, processus TIC, services de sécurité gérés ou entités aux attaques menées par des acteurs compétents, en utilisant, le cas échéant, des tests d'intrusion.

   Lorsque de telles activités d'évaluation ne sont pas appropriées, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises. Toutes les activités d'évaluation de la conformité, y compris l'étalonnage, les essais, la certification et l'inspection, pour le niveau d'assurance «élevé» sont menées dans l'Espace économique européen, sauf disposition contraire prévue dans un schéma européen de certification de cybersécurité.

8. Lorsqu'un schéma européen de certification de cybersécurité est conçu pour démontrer le respect des exigences et accorder une présomption de conformité avec un acte juridique spécifique de l'Union, il fournit l'assurance que les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités certifiés satisfont aux exigences de cybersécurité correspondantes de cet acte juridique. Toutes les activités d'évaluation de la conformité, y compris l'étalonnage, les essais, la certification et l'inspection, aux fins de la présomption de conformité, sont menées dans l'Espace économique européen, sauf disposition contraire prévue dans un schéma européen de certification de cybersécurité.

9. Un schéma européen de certification de cybersécurité peut préciser plusieurs niveaux d'évaluation pour un niveau d'assurance donné. Chacun des niveaux d'évaluation correspond à l'un des niveaux d'assurance.

Article 83
Autoévaluation de la conformité

1. Un schéma européen de certification de cybersécurité peut permettre la réalisation d'une autoévaluation de la conformité sous la seule responsabilité du fabricant ou du fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés ou de l'entité dont la posture de cybersécurité fait l'objet de la certification. L'autoévaluation de la conformité n'est autorisée que pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités qui présentent un risque faible correspondant au niveau d'assurance dit «élémentaire».

2. Le fabricant ou le fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés ou l'entité dont la posture de cybersécurité fait l'objet de la certification peut délivrer une déclaration de conformité de l'UE indiquant que le respect des exigences énoncées dans le schéma européen de certification de cybersécurité a été démontré. En délivrant une telle déclaration, ce fabricant, ce fournisseur ou cette entité assume la responsabilité du respect, par le produit TIC, le service TIC, le processus TIC, le service de sécurité géré ou la posture de cybersécurité, des exigences fixées dans ce schéma.

3. Le fabricant ou fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés ou l'entité dont la posture de cybersécurité fait l'objet de la certification garde à la disposition de l'autorité nationale de certification de cybersécurité désignée en vertu de l'article 89 la déclaration de conformité de l'UE, la documentation technique et toutes les autres informations pertinentes relatives à la conformité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou de la posture de cybersécurité avec le schéma européen de certification de cybersécurité pendant la durée prévue dans ledit schéma. Une copie de la déclaration de conformité de l'UE est transmise sans retard injustifié à l'autorité nationale de certification de cybersécurité et à l'ENISA.

Article 84
Informations supplémentaires en matière de cybersécurité pour les produits TIC, services TIC et processus TIC certifiés

1. Le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC pour lesquels une déclaration de conformité de l'UE ou un certificat de cybersécurité européen a été délivré met à la disposition de l'utilisateur les informations supplémentaires suivantes en matière de cybersécurité:

   a) la destination du produit TIC, service TIC ou processus TIC concerné, y compris l'environnement de sécurité fourni par le fabricant ou le fournisseur;

   b) des orientations et des recommandations pour aider les utilisateurs à assurer, de façon sécurisée, la configuration, l'installation, le déploiement, le fonctionnement et la maintenance des produits TIC ou services TIC;

   c) le type d'assistance technique en matière de sécurité proposé par le fabricant ou le fournisseur et la date de fin de la période d'assistance pendant laquelle les utilisateurs peuvent s'attendre à ce que les vulnérabilités soient traitées et à recevoir des mises à jour de sécurité;

d) lorsque le fabricant ou le fournisseur décide de mettre à la disposition de l'utilisateur une nomenclature de logiciels, des informations sur l'endroit où celle-ci peut être consultée.

2. Le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC pour lesquels une déclaration de conformité de l'UE ou un certificat de cybersécurité européen a été délivré met à la disposition du public les informations supplémentaires suivantes en matière de cybersécurité:

a) le point de contact unique où les informations sur les vulnérabilités du produit peuvent être signalées et reçues, et où peut être trouvée la politique du fabricant en matière de divulgation coordonnée des vulnérabilités;

b) des informations sur les vulnérabilités corrigées, y compris une description des vulnérabilités et des informations permettant aux utilisateurs d'identifier le produit comportant des éléments numériques concerné, les conséquences de ces vulnérabilités, leur gravité et des informations claires et accessibles aidant les utilisateurs à y remédier; dans des cas dûment justifiés, lorsque les fabricants considèrent que les risques pour la sécurité liés à la publication l'emportent sur les avantages en matière de sécurité, ils peuvent retarder la publication des informations relatives à une vulnérabilité corrigée jusqu'à ce que les utilisateurs aient eu la possibilité d'appliquer le correctif adapté.

3. Les informations visées aux paragraphes 1 et 2 sont disponibles sous forme électronique et restent disponibles et actualisées en tant que de besoin pendant la durée de validité et au moins pendant une période de cinq ans après l'expiration ou le retrait du certificat de cybersécurité européen ou de la déclaration de conformité de l'UE pertinent(e).

4. Les obligations énoncées aux paragraphes 1 et 2 ne s'appliquent pas lorsque la sécurité du produit TIC, service TIC ou processus TIC concerné pourrait être compromise si les informations sont rendues publiques.

CHAPITRE III
Gouvernance du cadre européen de certification de cybersécurité

Section 1
Règles générales et gestion des schémas européens de certification de cybersécurité

Article 85
Délivrance de certificats de cybersécurité européens

1. Les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités qui ont été certifiés dans le cadre d'un schéma européen de certification de cybersécurité sont présumés conformes aux exigences de ce schéma.

2. Les organismes d'évaluation de la conformité visés à l'article 91 délivrent des certificats de cybersécurité européens au titre du présent article sur la base des critères figurant dans le schéma européen de certification de cybersécurité adopté conformément à l'article 74.

3. Par dérogation au paragraphe 2, un schéma européen de certification de cybersécurité peut prévoir que seul un des organismes publics suivants peut délivrer des certificats de cybersécurité européens dans le cadre dudit schéma:

   a) une autorité nationale de certification de cybersécurité visée à l'article 88, accréditée en tant qu'organisme d'évaluation de la conformité conformément à l'article 91, paragraphe 1;

   b) un organisme public accrédité en tant qu'organisme d'évaluation de la conformité conformément à l'article 91, paragraphe 1.

4. Lorsqu'un schéma européen de certification de cybersécurité adopté en vertu de l'article 74 établit un niveau d'assurance «élevé», ou si ledit schéma en dispose autrement, le certificat de cybersécurité européen au titre de ce schéma doit être délivré uniquement par une autorité nationale de certification de cybersécurité, telle que visée à l'article 88, qui est accréditée en tant qu'organisme d'évaluation de la conformité conformément à l'article 91, paragraphe 1, ou, dans les cas suivants:

   a) par un organisme d'évaluation de la conformité sur la base d'un modèle d'approbation préalable; ou

   b) par un organisme d'évaluation de la conformité sur la base d'un modèle de délégation générale.

5. La Commission est habilitée à adopter des actes d'exécution précisant les procédures d'approbation préalable ou les modèles de délégation générale visés au paragraphe 4 du présent article. Dans le cadre de l'élaboration de ces actes d'exécution, la Commission consulte le GECC. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.

6. La personne physique ou morale qui soumet des produits TIC, services TIC, processus TIC ou services de sécurité gérés à la certification, ou l'entité qui demande la certification de sa posture de cybersécurité, met à la disposition de l'autorité nationale de certification de cybersécurité désignée en vertu de l'article 89, lorsque cette autorité est l'organisme délivrant le certificat de cybersécurité européen, ou de l'organisme d'évaluation de la conformité visé à l'article 91, toutes les informations nécessaires pour procéder à la certification.

7. Les organismes d'évaluation de la conformité et, le cas échéant, les autorités nationales de certification de cybersécurité informent l'ENISA dans les meilleurs délais de leurs décisions qui ont une incidence sur le statut des certificats de cybersécurité européens et des déclarations de conformité de l'UE conformément à l'article 94.

8. Le titulaire d'un certificat de cybersécurité européen informe l'organisme d'évaluation de la conformité et, le cas échéant, l'autorité nationale de certification de cybersécurité visée au paragraphe 7, de toute vulnérabilité ou non-conformité détectée ultérieurement concernant le produit TIC, le service TIC, le processus TIC, le service de sécurité géré certifié ou la posture de cybersécurité de l'entité, susceptible d'avoir une incidence sur sa conformité au certificat. Cet organisme transmet ces informations sans retard injustifié à l'autorité nationale de certification de cybersécurité concernée et évalue l'incidence sur le certificat conformément aux conditions du schéma énoncées à l'article 81, paragraphe 2, point d).

9. Les titulaires d'un certificat de cybersécurité européen n'utilisent pas, n'installent pas ou n'intègrent d'aucune autre manière des composants TIC ou des composants qui

incluent des composants TIC provenant de fournisseurs à haut risque dans leurs produits TIC, services TIC, processus TIC ou services de sécurité gérés certifiés qui ont été identifiés, en totalité ou en partie, en tant qu'actifs essentiels conformément à l'article 102.

10. Un certificat de cybersécurité européen est délivré pour la durée prévue par le schéma européen de certification de cybersécurité concerné et peut être renouvelé, pourvu que les exigences applicables continuent d'être satisfaites.

11. La Commission coopère avec les États membres pour garantir l'application des dispositions relatives à la délivrance de certificats de cybersécurité européens également en vue de l'application de l'article 100, paragraphe 4, point b). L'organisme d'évaluation de la conformité et, le cas échéant, l'autorité nationale de certification de cybersécurité fournissent à la Commission, sur demande et sans retard injustifié, toutes les informations relatives à la délivrance des certificats de cybersécurité européens ou des déclarations de conformité de l'UE pertinents.

Article 86
Schémas nationaux de certification de cybersécurité et certificats

1. Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités couverts par l'objet et le champ d'application d'un schéma européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte d'exécution adopté en application de l'article 74, paragraphe 9. Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités qui ne sont pas couverts par l'objet et le champ d'application d'un schéma européen de certification de cybersécurité peuvent continuent à exister.

2. Les États membres n'introduisent pas de nouveaux schémas nationaux de certification de cybersécurité ou de procédures connexes pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités déjà couverts par l'objet et le champ d'application d'un schéma européen de certification de cybersécurité.

3. Les certificats existants, qui ont été délivrés dans le cadre de schémas nationaux de certification de cybersécurité et qui sont couverts par l'objet et le champ d'application d'un schéma européen de certification de cybersécurité, restent valables jusqu'à leur date d'expiration.

4. Les États membres informent la Commission et le GECC avant d'adopter de nouveaux schémas nationaux de certification de cybersécurité pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités.

5. La Commission peut suggérer à un État membre de retirer un schéma national de certification de cybersécurité pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité d'entités, lorsque la préparation d'un schéma européen de certification de cybersécurité couvrant ces produits, ces services, ces processus ou cette posture de cybersécurité a déjà été demandée conformément à l'article 73, en tenant compte du plan de préparation de ce schéma.

Article 87

Reconnaissance internationale des certificats de cybersécurité européens

1. Les certificats de pays tiers de produits TIC, services TIC, processus TIC, services de sécurité gérés et posture de cybersécurité d'entités peuvent être reconnus, au moyen d'un acte d'exécution ou par la conclusion d'un accord entre l'Union et le pays tiers en question ou une organisation internationale, comme équivalents aux certificats de cybersécurité européens si les exigences du schéma du pays tiers ou de l'organisation internationale concernés sont considérées comme équivalentes à celles des schémas européens de certification de cybersécurité. La Commission est habilitée à adopter de tels actes d'exécution Les actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.

2. Les actes d'exécution et les accords visés au paragraphe 1 sont fondés sur les conditions de reconnaissance internationale des certificats de cybersécurité européens énoncées conformément à l'article 74, paragraphe 11.

3. Les accords sur la reconnaissance des certificats de pays tiers ou des certificats d'organisation internationale visés au paragraphe 1 ne sont conclus que s'ils reconnaissent également les certificats de cybersécurité européens comme équivalents aux certificats de pays tiers.

Article 88

Autorités nationales de certification de cybersécurité

1. Chaque État membre désigne une ou plusieurs autorités nationales de certification de cybersécurité sur son territoire ou, moyennant l'accord d'un autre État membre, désigne une ou plusieurs autorités nationales de certification de cybersécurité dans cet autre État membre comme responsables des tâches de supervision dans l'État membre qui procède à la désignation.

2. Chaque État membre informe la Commission de l'identité des autorités nationales de certification de cybersécurité désignées. Lorsqu'un État membre désigne plus d'une autorité, il communique en outre à la Commission des informations sur les tâches confiées à chacune de ces autorités.

3. Chaque autorité nationale de certification de cybersécurité est indépendante des entités qu'elle supervise en ce qui concerne son organisation, ses décisions de financement, sa structure juridique et sa prise de décision.

4. Les activités des autorités nationales de certification de cybersécurité liées à la délivrance de certificats de cybersécurité européens au titre du présent règlement sont strictement distinctes de leurs activités de supervision énoncées au présent article et à l'article 85, paragraphe 4, points a) et b), et sont exécutées indépendamment les unes des autres.

5. Les États membres veillent à ce que les autorités nationales de certification de cybersécurité disposent de ressources adéquates pour exercer leurs pouvoirs et exécuter leurs tâches de manière efficace et efficiente.

6. Les autorités nationales de certification de cybersécurité ont pour mission:

   a) de participer au GECC, conformément à l'article 90, paragraphe 2;

   b) de superviser et faire respecter les règles incluses dans les schémas européens de certification de cybersécurité conformément à l'article 81, paragraphe 2,

point a), afin de garantir la conformité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés et de la posture de cybersécurité des entités avec les exigences des certificats de cybersécurité européens qui ont été délivrés sur leurs territoires respectifs, en coopération avec les autorités de surveillance du marché ou de contrôle concernées, y compris les autorités compétentes au titre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[82] ou du règlement (UE) 2024/2847;

c) de contrôler, en coopération avec les autorités de surveillance du marché concernées, le respect des obligations qui incombent aux fabricants ou fournisseurs de produits TIC, services TIC, processus TIC et services de sécurité gérés ou aux entités dont la posture de cybersécurité est certifiée conformément au présent règlement, qui sont établis sur leurs territoires respectifs et qui procèdent à une autoévaluation de la conformité dans le cadre du schéma européen de certification de cybersécurité correspondant, et de faire respecter ces obligations;

d) sans préjudice de l'article 91, paragraphe 3, d'assister et de soutenir activement les organismes nationaux d'accréditation ou les autres autorités concernées dans le contrôle et la supervision des activités des organismes d'évaluation de la conformité aux fins du présent règlement;

e) de coopérer avec la Commission lorsque la compétence d'un organisme d'évaluation de la conformité est contestée en vertu de l'article 94;

f) de contrôler et superviser les activités des organismes publics visées à l'article 85, paragraphe 3;

g) le cas échéant, d'autoriser les organismes d'évaluation de la conformité conformément à l'article 93, à contrôler le respect des obligations qui incombent aux organismes d'évaluation de la conformité en ce qui concerne les exigences supplémentaires ou spécifiques énoncées dans les schémas européens de certification de cybersécurité conformément à l'article 81, paragraphe 3, point f), et à faire respecter ces obligations, ainsi qu'à restreindre, suspendre ou retirer l'autorisation existante lorsque les organismes d'évaluation de la conformité ne satisfont pas aux exigences du présent règlement;

h) de traiter les réclamations introduites par des personnes physiques ou morales en rapport avec les certificats de cybersécurité européens délivrés par des autorités nationales de certification de cybersécurité ou en rapport avec les certificats de cybersécurité européens délivrés par des organismes d'évaluation de la conformité conformément à l'article 85, paragraphe 4, ou en rapport avec les déclarations de conformité de l'Union européenne délivrées au titre de l'article 83, d'examiner l'objet de ces réclamations dans la mesure nécessaire et d'informer l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable;

---

82 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).

i) de présenter un rapport annuel sur ses principales activités à la Commission, à l'ENISA et au GECC au plus tard le 31 mars de chaque année à compter de [année d'entrée en vigueur + 12 mois], et de mettre ces rapports à la disposition de l'équipe chargée de l'examen par les pairs lorsque l'autorité nationale de certification de cybersécurité fait l'objet d'un examen par les pairs conformément à l'article 89;

j) de coopérer avec les autres autorités nationales de certification de cybersécurité, les autorités de surveillance du marché ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuel non-respect, par des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou la posture de cybersécurité d'entités, des exigences du présent règlement ou des exigences de schémas de certification de cybersécurité spécifiques;

k) de suivre les évolutions pertinentes dans le domaine de la certification de cybersécurité.

7. Chaque autorité nationale de certification de cybersécurité dispose au moins des pouvoirs suivants:

a) de demander aux organismes d'évaluation de la conformité, aux titulaires de certificats de cybersécurité européens et aux émetteurs de déclarations de conformité de l'Union européenne de lui communiquer toute information dont elle a besoin pour l'exécution de ses tâches;

b) d'effectuer des enquêtes, sous la forme d'audits, auprès des organismes d'évaluation de la conformité, des titulaires de certificats de cybersécurité européens et des émetteurs de déclarations de conformité de l'Union européenne afin de vérifier qu'ils respectent les exigences énoncées au présent titre;

c) de prendre les mesures appropriées, conformément au droit national, pour veiller à ce que les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne respectent le présent règlement ou un schéma européen de certification de cybersécurité;

d) d'obtenir l'accès aux locaux des organismes d'évaluation de la conformité ou des titulaires de certificats de cybersécurité européens afin d'effectuer des enquêtes conformément au droit de l'Union ou au droit procédural national;

e) de retirer, conformément au droit national, les certificats de cybersécurité européens délivrés par les autorités nationales de certification de cybersécurité ou les organismes d'évaluation de la conformité conformément à l'article 85, paragraphe 4, lorsque ces certificats ne respectent pas le présent règlement ou un schéma européen de certification de cybersécurité;

f) d'imposer des sanctions conformément au droit national, comme le prévoit l'article 97, et d'exiger la cessation immédiate des violations des obligations énoncées dans le présent règlement.

8. Les autorités nationales de certification de cybersécurité coopèrent entre elles et avec la Commission et échangent notamment des informations, expériences et bonnes pratiques en ce qui concerne la certification de cybersécurité et les questions

techniques relatives à la cybersécurité des produits TIC, services TIC, processus TIC, services de sécurité gérés et à la posture de cybersécurité des entités.

9. Au plus tard le [entrée en vigueur + 6 mois], l'ENISA élabore un modèle pour le rapport visé au paragraphe 6, point i), du présent article, en coopération avec la Commission et le GECC.

Article 89
Examen par les pairs

1. Les autorités nationales de certification de cybersécurité font l'objet d'un examen par les pairs.

2. L'examen par les pairs est effectué selon des critères et des procédures d'évaluation cohérents et transparents, en particulier en ce qui concerne les exigences structurelles et celles relatives aux ressources humaines et aux processus, ainsi que la confidentialité et les plaintes.

3. L'examen par les pairs évalue:

   a) lorsqu'il y a lieu, la question de savoir si les activités des autorités nationales de certification de cybersécurité liées à la délivrance de certificats de cybersécurité européens visées au présent règlement sont strictement distinctes des activités de supervision visées à l'article 88, et celle de savoir si ces activités sont exercées indépendamment l'une de l'autre;

   b) les procédures permettant de superviser et de faire respecter les règles relatives au contrôle du respect, par les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités, des certificats de cybersécurité européens, conformément à l'article 88, paragraphe 7, point a);

   c) les procédures permettant de contrôler et de faire respecter les obligations incombant aux fabricants et fournisseurs de produits TIC, services TIC, processus TIC ou services de sécurité gérés ou aux entités dont la posture de cybersécurité est certifiée, conformément à l'article 88, paragraphe 7, point b);

   d) les procédures permettant de contrôler, d'autoriser et de superviser les activités des organismes d'évaluation de la conformité.

4. L'examen par les pairs est effectué au moins une fois tous les cinq ans par au moins deux autorités nationales de certification de cybersécurité d'autres États membres et par la Commission. L'ENISA participe également à l'examen par les pairs en qualité d'observateur. L'équipe chargée de l'examen par les pairs établit le rapport final et la synthèse de l'examen par les pairs.

5. L'ENISA soutient l'organisation du mécanisme d'examen par les pairs et des examens par les pairs, y compris en élaborant des documents d'orientation et des modèles pertinents, en coopération avec la Commission et le GECC.

6. La Commission est habilitée à adopter des actes d'exécution établissant un plan pour l'examen par les pairs couvrant une période d'au moins cinq ans et définissant les critères concernant la composition de l'équipe chargée de l'examen par les pairs, la méthode utilisée pour mener cet examen, ainsi que le programme, la fréquence et les autres tâches liées à l'examen par les pairs. Dans le cadre de l'élaboration de ces actes d'exécution, la Commission consulte le GECC et l'ENISA. Ces actes

d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.

7. Le rapport final, y compris les éventuelles lignes directrices ou recommandations, et la synthèse de l'examen par les pairs sont examinés par le GECC, qui approuve la synthèse en vue de sa publication sur le site internet visé à l'article 79, paragraphe 2.

Article 90
Groupe européen de certification de cybersécurité

1. Le groupe européen de certification de cybersécurité (GECC) est institué.

2. Le GECC est composé de représentants d'autorités nationales de certification de cybersécurité ou de représentants d'autres autorités nationales compétentes. Un membre du GECC ne peut représenter plus de deux États membres.

3. Le GECC a pour mission:

a) de conseiller et d'assister la Commission dans ses travaux visant à garantir la mise en œuvre et l'application cohérentes des règles énoncées dans le présent titre ainsi que pour les aspects concernant les questions relatives à la politique de certification de cybersécurité et la coordination des approches stratégiques;

b) de conseiller et d'assister la Commission dans la préparation des demandes de schémas européens de certification de cybersécurité conformément à l'article 73;

c) d'assister et de conseiller l'ENISA et de coopérer avec elle en ce qui concerne la préparation d'un schéma candidat en vertu de l'article 74 et de spécifications techniques en vertu de l'article 77;

d) d'assister et de conseiller l'ENISA et la Commission et de coopérer avec elles en ce qui concerne les activités de maintenance conformément à l'article 75;

e) d'assister et de conseiller la Commission et de coopérer avec elle en ce qui concerne le réexamen ou le retrait de schémas européens de certification de cybersécurité existants conformément à l'article 76;

f) de suggérer qu'une demande soit soumise à la Commission en ce qui concerne la préparation d'un schéma européen de certification de cybersécurité candidat conformément à l'article 73, paragraphe 2;

g) d'adopter des avis adressés à la Commission concernant la maintenance, le réexamen et le retrait de schémas européens de certification de cybersécurité existants;

h) d'examiner les évolutions pertinentes dans le domaine de la certification de cybersécurité, y compris au niveau national conformément à l'article 86, et d'échanger des informations et de bonnes pratiques sur les schémas de certification de cybersécurité;

i) de faciliter la coopération entre les autorités nationales de certification de cybersécurité en vertu des règles énoncées dans le présent titre par le renforcement des capacités et l'échange d'informations, en particulier en ce qui concerne les questions relatives à la certification de cybersécurité;

j) de fournir un soutien à la mise en œuvre du mécanisme d'examen par les pairs conformément à l'article 89 et des mécanismes d'évaluation par les pairs

conformément aux règles fixées dans un schéma européen de certification de cybersécurité en vertu de l'article 81, paragraphe 2, point g);

k) de faciliter l'alignement des schémas européens de certification de cybersécurité sur les normes internationalement reconnues, y compris dans le cadre de la maintenance des schémas européens de certification de cybersécurité existants et, s'il y a lieu, de recommander à l'ENISA de nouer le dialogue avec les organisations européennes ou internationales de normalisation compétentes dans le but de remédier à des insuffisances ou à des lacunes affectant les normes en vigueur reconnues à l'échelon européen ou international.

4. Avec l'aide de l'ENISA, la Commission préside le GECC et en assure le secrétariat.

5. La Commission peut créer des sous-groupes du GECC aux fins suivantes:

a) examiner des questions spécifiques sur la base d'un mandat établi par la Commission;

b) tenir à jour et réexaminer les schémas européens de certification conformément au présent règlement et sur la base d'un mandat établi par la Commission.

6. Les sous-groupes font rapport au GECC.

7. Les sous-groupes sont coprésidés par la Commission et l'ENISA, et le secrétariat des sous-groupes est assuré par l'ENISA.

8. Le GECC et ses sous-groupes adoptent leur règlement intérieur à la majorité simple de leurs membres, sur la base d'une proposition de la Commission et en accord avec celle-ci.

Section 2
Organismes d'évaluation de la conformité

Article 91
Compétence des organismes d'évaluation de la conformité

1. Les organismes d'évaluation de la conformité sont accrédités par les organismes nationaux d'accréditation désignés conformément au règlement (CE) n° 765/2008. Cette accréditation n'est délivrée que lorsque l'organisme d'évaluation de la conformité satisfait aux exigences énoncées à l'annexe I du présent règlement.

2. Lorsqu'un certificat de cybersécurité européen est délivré par une autorité nationale de certification de cybersécurité en vertu du présent règlement, l'organisme de certification de l'autorité nationale de certification de cybersécurité est accrédité en tant qu'organisme d'évaluation de la conformité conformément au paragraphe 1.

3. L'accréditation visée au paragraphe 1 est délivrée aux organismes d'évaluation de la conformité pour une durée maximale de cinq ans et peut être renouvelée, pourvu que l'organisme d'évaluation de la conformité satisfasse aux exigences énoncées au présent article. Les organismes nationaux d'accréditation prennent, dans un délai raisonnable, toutes les mesures appropriées pour limiter, suspendre ou révoquer l'accréditation d'un organisme d'évaluation de la conformité délivrée en vertu du paragraphe 1 lorsque les conditions de l'accréditation ne sont pas ou plus remplies ou lorsque l'organisme d'évaluation de la conformité ne respecte pas le présent règlement.

4. Lors de l’établissement d’exigences d’accréditation supplémentaires ou spécifiques pour un schéma européen de certification de cybersécurité couvrant des produits TIC, conformément à l’article 92, des synergies sont recherchées, le cas échéant, avec les exigences relatives aux organismes notifiés au titre du règlement (UE) 2024/2847 et les exigences d’accréditation au titre des schémas de certification de cybersécurité qui ont déjà été adoptées.

5. Lorsqu’un organisme d’évaluation de la conformité est accrédité conformément au règlement (UE) 2024/2847, les autorités compétentes peuvent réutiliser les résultats du processus d’accréditation précédent en ce qui concerne tout chevauchement des exigences comme preuve au cours du processus d’accréditation au titre du présent règlement.

Article 92

Harmonisation supplémentaire de la compétence des organismes d’évaluation de la conformité

1. Lorsqu’un schéma européen de certification de cybersécurité définit des exigences supplémentaires ou spécifiques en vertu de l’article 81, paragraphe 3, point f), les organismes d’évaluation de la conformité sont autorisés par une autorité nationale de certification de cybersécurité désignée en vertu de l’article 88, paragraphe 1, à exécuter des tâches dans le cadre de ce schéma. Cette autorisation n’est délivrée que si l’organisme d’évaluation de la conformité a été accrédité et satisfait aux exigences supplémentaires ou spécifiques énoncées dans le cadre du schéma européen de certification de cybersécurité.

2. Lorsqu'un organisme d'évaluation de la conformité sollicite une autorisation au titre du présent article, il soumet sa demande à l’autorité nationale de certification de cybersécurité de l'État membre dans lequel il est établi ou à l’autorité nationale de certification de cybersécurité à laquelle l'État membre a recours conformément à l'article 88, paragraphe 1.

3. Un organisme d'évaluation de la conformité peut demander l'autorisation auprès d'une autorité nationale de certification de cybersécurité autre que celle visée au paragraphe 2 dans les cas suivants:

   a) lorsque l’autorité nationale de certification de cybersécurité visée au paragraphe 1 ne délivre pas d’autorisation pour les activités d’évaluation de la conformité pour lesquelles l’autorisation est demandée;

   b) lorsque l’autorité nationale de certification de cybersécurité visée au paragraphe 1 n’a pas fait l’objet d’un examen par les pairs conformément à l’article 89 pour les activités d’évaluation de la conformité pour lesquelles l’autorisation est demandée.

4. Lorsqu'une autorité nationale de certification de cybersécurité reçoit une demande en vertu du paragraphe 3, elle informe l'autorité nationale de certification de cybersécurité de l'État membre dans lequel l'organisme d'évaluation de la conformité demandeur est établi. Dans de tels cas, l’autorité nationale de certification de cybersécurité de cet État membre peut participer à l’autorisation en tant qu’observateur.

5. Une autorité nationale de certification de cybersécurité peut demander à une autre autorité nationale de certification de cybersécurité de réaliser une partie de l’activité

d’évaluation. Dans ce cas, le certificat d'autorisation est délivré par l'autorité requérante.

6. L’autorisation visée au paragraphe 1 est valable pour une durée n’excédant pas celle de l’accréditation et peut être renouvelée à condition que l’organisme d’évaluation de la conformité satisfasse aux exigences énoncées au paragraphe 1 et que son accréditation ait également été renouvelée.

7. Les autorités nationales de certification de cybersécurité prennent, dans un délai raisonnable, toutes les mesures appropriées pour limiter, suspendre ou révoquer l’autorisation d’un organisme d’évaluation de la conformité délivrée en vertu du paragraphe 1 lorsque les conditions de l’autorisation ne sont pas ou plus remplies ou lorsque l’organisme d’évaluation de la conformité ne respecte pas le présent règlement.

8. La Commission est habilitée à adopter des actes d’exécution pour établir les procédures d’autorisation des organismes d’évaluation de la conformité, y compris en ce qui concerne la coopération transfrontière. Dans le cadre de l'élaboration des actes d'exécution, la Commission consulte l’ENISA et le GECC. Ces actes d’exécution sont adoptés en conformité avec la procédure d’examen visée à l’article 118, paragraphe 2.

Article 93

Notification des organismes d’évaluation de la conformité

1. Pour chaque schéma européen de certification de cybersécurité, les autorités nationales de certification de cybersécurité d’un État membre notifient à la Commission et aux autres États membres les organismes d’évaluation de la conformité qui ont été accrédités et, le cas échéant, autorisés en vertu de l’article 92.

2. Les autorités nationales de certification de cybersécurité procèdent à la notification prévue au paragraphe 1 au moyen de l’outil de notification électronique mis au point et géré par la Commission.

3. La Commission est habilitée à adopter des actes d’exécution pour définir les circonstances, les formats et les procédures applicables aux notifications prévues au paragraphe 1 du présent article, y compris la procédure d’opposition par d’autres États membres au cours du processus de notification, l’identification unique des organismes d’évaluation de la conformité, ainsi que les circonstances de la restriction, de la suspension ou du retrait de la notification. Ces actes d’exécution sont adoptés en conformité avec la procédure d’examen visée à l’article 118, paragraphe 2.

Article 94

Contestation de la compétence des organismes d’évaluation de la conformité

1. La Commission enquête sur tous les cas dans lesquels elle émet des doutes ou est avertie de doutes quant à la compétence d’un organisme d’évaluation de la conformité de remplir ou de continuer à remplir les exigences qui lui sont applicables et de s’acquitter ou de continuer à s’acquitter des responsabilités qui lui incombent.

2. L’autorité nationale de certification de cybersécurité communique à la Commission, sur demande, toutes les informations relatives au fondement de la notification ou au maintien de la compétence de l’organisme d’évaluation de la conformité concerné.

3. La Commission veille à ce que toutes les informations sensibles obtenues au cours de ses enquêtes soient traitées de manière confidentielle.

4. Lorsque la Commission établit qu'un organisme d'évaluation de la conformité ne répond pas ou ne répond plus aux exigences relatives à sa notification, elle en informe l'autorité nationale de certification de cybersécurité et l'invite à prendre les mesures correctives qui s'imposent, y compris la dénotification si nécessaire.

5. Les États membres veillent à ce qu'il existe une procédure de recours contre les décisions des organismes notifiés.

Article 95
Obligation d'information et de conservation incombant aux organismes d'évaluation de la conformité

1. Les organismes d'évaluation de la conformité informent l'autorité nationale de certification de cybersécurité des éléments suivants:

   a) tout refus, restriction, suspension ou retrait d'un certificat;

   b) toute circonstance ayant une incidence sur la portée et les conditions de la notification visée à l'article 93, paragraphe 1;

   c) toute demande d'information reçue des autorités de surveillance du marché concernant des activités d'évaluation de la conformité;

   d) sur demande, toute activité d'évaluation de la conformité accomplie dans le cadre de leur notification et toute autre activité réalisée, y compris les activités et sous-traitances transfrontières.

2. Les organismes d'évaluation de la conformité fournissent également à l'ENISA les informations visées au paragraphe 1, point a), en vue de faciliter l'exécution de sa mission au titre de l'article 79.

3. Les organismes d'évaluation de la conformité fournissent dans les meilleurs délais, aux autres organismes d'évaluation de la conformité au sens du présent règlement, qui effectuent des activités similaires d'évaluation de la conformité couvrant les mêmes produits TIC, services TIC, processus TIC, services de sécurité gérés ou entités dont la posture de cybersécurité est certifiée, des informations pertinentes sur les questions relatives aux résultats négatifs et, sur demande, aux résultats positifs de l'évaluation de la conformité.

4. Les organismes d'évaluation de la conformité tiennent à jour un système de registre contenant tous les documents et éléments de preuve produits ou reçus dans le cadre de chaque évaluation et certification qu'ils effectuent. Le registre est stocké de manière sécurisée et accessible pendant la durée nécessaire à la certification et pendant au moins cinq ans après l'expiration ou le retrait du certificat de cybersécurité européen concerné.

Section 3
Autres dispositions

Article 96

Droit d'introduire une réclamation et droit à un recours juridictionnel effectif

1. Les personnes physiques et morales ont le droit d'introduire une réclamation auprès de l'émetteur d'un certificat de cybersécurité européen ou, lorsque la réclamation est en rapport avec un certificat de cybersécurité européen délivré par un organisme d'évaluation de la conformité agissant conformément à l'article 85, paragraphe 4, auprès de l'autorité nationale de certification de cybersécurité concernée.

2. L'autorité ou l'organisme auprès duquel la réclamation a été introduite informe l'auteur de la réclamation de l'état d'avancement de la procédure, de la décision prise, et de son droit à un recours juridictionnel effectif visé aux paragraphes 3 et 4.

3. Nonobstant tout recours administratif ou tout autre recours non juridictionnel, les personnes physiques ou morales disposent d'un droit de recours juridictionnel effectif en ce qui concerne:

   a) les décisions prises par l'autorité ou l'organisme visé au paragraphe 1, y compris, le cas échéant, en ce qui concerne la délivrance non justifiée, la non-délivrance ou la reconnaissance d'un certificat de cybersécurité européen détenu par ces personnes physiques ou morales;

   b) l'absence de réaction à une réclamation introduite auprès de l'autorité ou de l'organisme visé au paragraphe 1.

4. Les recours formés en vertu du présent article sont portés devant les juridictions de l'État membre dans lequel se trouve l'autorité ou l'organisme à l'encontre duquel le recours juridictionnel a été formé.

Article 97

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions du présent titre et aux violations des schémas européens de certification de cybersécurité et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission sans retard du régime ainsi déterminé et des mesures ainsi prises, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.

TITRE IV
SÉCURITÉ DES CHAÎNES D'APPROVISIONNEMENT DES TIC

CHAPITRE I
Un cadre digne de confiance pour la chaîne d'approvisionnement des TIC

Article 98

Champ d'application du cadre

1. Le cadre digne de confiance pour la chaîne d'approvisionnement des TIC prévoit un mécanisme de sécurité au niveau de l'Union pour faire face aux risques non techniques dans les secteurs hautement critiques et d'autres secteurs critiques visés dans la directive (UE) 2022/2555. Le mécanisme recense les actifs TIC essentiels

dans les chaînes d'approvisionnement critiques des TIC et définit des mesures d'atténuation appropriées et proportionnées pour les entités d'un des types visés aux annexes I et II de la directive (UE) 2022/2555.

2. Les obligations énoncées dans le présent titre sont sans préjudice des obligations énoncées à l'article 13 du règlement (UE) 2024/2847 et dans les dispositions nationales transposant l'article 21 de la directive (UE) 2022/2555.

3. Les dispositions établies au présent chapitre ne font pas obstacle à l'adoption ou au maintien par les États membres de dispositions assurant un niveau plus élevé de cybersécurité dans les chaînes d'approvisionnement des TIC, à condition que ces dispositions soient compatibles avec les obligations qui leur incombent en vertu du droit de l'Union.

Article 99
Évaluations des risques pour la sécurité

1. La Commission ou un groupe d'au moins trois États membres peut demander au groupe de coopération institué par l'article 14 de la directive (UE) 2022/2555 (ci-après dénommé «groupe de coopération SRI») de réaliser des évaluations coordonnées des risques pour la sécurité au niveau de l'Union conformément à l'article 22 de ladite directive. Lorsqu'une évaluation des risques pour la sécurité est effectuée à la suite d'une telle demande, elle comprend en particulier la proposition d'identification des actifs TIC essentiels de la chaîne d'approvisionnement des TIC concernée ainsi que des principaux acteurs de la menace, risques et vulnérabilités affectant ces actifs. Les évaluations coordonnées des risques pour la sécurité au niveau de l'Union contiennent des scénarios de risque et des propositions de mesures pour atténuer les risques recensés.

2. Les évaluations coordonnées des risques pour la sécurité au niveau de l'Union sont achevées dans un délai de six mois à compter de la demande visée au paragraphe 1. À la demande de la Commission, le groupe de coopération SRI peut convenir d'un délai plus court.

3. Lorsqu'elle a des raisons suffisantes de croire qu'il existe une cybermenace importante pour la sécurité de l'Union en ce qui concerne une chaîne d'approvisionnement des TIC et qu'une action est nécessaire pour préserver le bon fonctionnement du marché intérieur, la Commission:

   a) consulte sans délai les États membres sur la nécessité de prendre une ou plusieurs des mesures d'atténuation visées à l'article 103; et

   b) réalise sans délai une évaluation des risques pour la sécurité, en tenant compte de la consultation des États membres. L'évaluation des risques pour la sécurité comprend la proposition d'identification des actifs TIC essentiels ainsi que des principaux acteurs de la menace, risques et vulnérabilités affectant ces actifs. Elle contient des scénarios de risque et des propositions de mesures pour atténuer les risques recensés.

Article 100
Désignation des pays tiers suscitant des préoccupations en matière de cybersécurité

1. Lorsque, à la suite de l'évaluation des risques pour la sécurité visée à l'article 99, ou sur la base d'autres sources, telles qu'une déclaration publique au nom de l'Union ou

d'un État membre, il apparaît qu'un pays tiers présente un risque non technique grave et structurel pour les chaînes d'approvisionnement des TIC, la Commission vérifie le risque présenté par ce pays, en tenant compte des éléments suivants:

a) l'existence, dans le pays tiers, de lois qui imposent aux entités relevant de leur juridiction de communiquer des informations sur les vulnérabilités logicielles ou matérielles aux autorités de ce pays tiers avant que l'exploitation de ces vulnérabilités ne soit avérée;

b) l'existence, dans le pays tiers, de pratiques, démontrées par des sources indépendantes, qui imposent aux entités relevant de la juridiction du pays tiers de communiquer des informations sur les vulnérabilités logicielles ou matérielles aux autorités de ce pays tiers avant que l'exploitation de ces vulnérabilités ne soit avérée;

c) l'absence de recours juridictionnels effectifs et de mécanismes de contrôle indépendants et démocratiques susceptibles de remédier aux préoccupations recensées en matière de sécurité, y compris en ce qui concerne les pratiques existantes visées au point b);

d) des informations étayées sur un ou plusieurs incidents impliquant des acteurs de la menace contrôlés depuis ce pays et opérant en dehors du territoire de ce dernier, qui mènent des cyberactivités ou des cybercampagnes malveillantes, et le manque de capacité ou de volonté du pays tiers de coopérer avec la Commission ou les États membres pour faire face au risque découlant des agissements de ces acteurs de la menace;

e) les informations pertinentes provenant d'évaluations coordonnées des risques de sécurité au niveau de l'Union ou de rapports établis par les États membres ou des organisations internationales.

2. Lorsque la Commission, à la suite de la vérification prévue au paragraphe 1, conclut qu'un pays tiers présente des risques non techniques graves et structurels pour les chaînes d'approvisionnement des TIC, elle peut, au moyen d'un acte d'exécution, désigner ce pays tiers comme un pays suscitant des préoccupations en matière de cybersécurité pour les chaînes d'approvisionnement des TIC. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.

3. La Commission réexamine régulièrement les actes d'exécution adoptés conformément au paragraphe 2.

4. Les fournisseurs à haut risque n'ont pas le droit:

a) de participer à l'élaboration et à l'évaluation des normes européennes et des publications en matière de normalisation européenne visées à l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012 et des spécifications communes visées à l'article 27 du règlement (UE) 2024/2847 dans le domaine de la cybersécurité, ni de participer aux consultations et aux décisions les concernant;

b) de demander un certificat de cybersécurité européen conformément au titre III ni d'en être titulaires;

c) de devenir un organisme d'évaluation de la conformité accrédité conformément au titre III;

d) de demander à devenir un fournisseur agréé de toute attestation individuelle européenne des compétences en matière de cybersécurité conformément au titre II, section 4;

e) de participer à des procédures de passation de marchés publics organisées conformément à la législation transposant la directive 2014/24/UE et la directive 2014/25/UE en ce qui concerne la fourniture de composants TIC ou de composants qui incluent des composants TIC destinés à être utilisés dans des actifs TIC essentiels recensés conformément à l'article 102;

f) de participer à toute activité relevant des programmes et instruments de financement de l'Union mis en œuvre en gestion directe et indirecte conformément à l'article 136 du règlement (UE, Euratom) 2024/2509 et à la réglementation sectorielle de l'Union, ainsi qu'à toute activité de financement de l'Union mise en œuvre en gestion partagée en ce qui concerne la fourniture de composants TIC ou de composants qui incluent des composants TIC destinés à être utilisés dans des actifs TIC essentiels recensés conformément à l'article 102.

Les autorités chargées des procédures visées aux points a) à f) réalisent les évaluations nécessaires aux fins du présent paragraphe. Les autorités peuvent également se fonder à cette fin sur la liste visée à l'article 104.

5. Lorsqu'un fournisseur à haut risque a déjà obtenu un certificat de cybersécurité européen en vertu du titre III, l'autorité compétente le retire sans retard injustifié.

Article 101
Mécanisme général de sécurité de la chaîne d'approvisionnement des TIC

Lorsque le groupe de coopération SRI a réalisé une évaluation coordonnée des risques pour la sécurité au niveau de l'Union conformément à l'article 99, paragraphe 1, du présent règlement, ou après l'achèvement de la procédure en cas de cybermenace importante au titre de l'article 99, paragraphe 3, pour une chaîne d'approvisionnement des TIC, la Commission peut prendre les mesures prévues à l'article 102 et à l'article 103, paragraphes 1 et 2.

Article 102
Recensement des actifs TIC essentiels

1. Lorsque l'évaluation des risques effectuée conformément à l'article 99, paragraphe 1 ou 3, indique des risques de cybersécurité importants liés à une chaîne d'approvisionnement des TIC, la Commission est habilitée à adopter des actes d'exécution recensant les actifs TIC essentiels utilisés pour la fabrication de produits ou la fourniture de services par des entités d'un des types visés aux annexes I et II de la directive (UE) 2022/2555. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2, du présent règlement.

2. Lorsqu'elle recense les actifs TIC essentiels visés au paragraphe 1, la Commission prend en considération les éléments suivants:

a) la question de savoir si ces actifs ont des fonctions essentielles et sensibles pour le fonctionnement de produits fabriqués ou de services fournis par l'entité d'un des types visés aux annexes I et II de la directive (UE) 2022/2555;

b) la question de savoir si les incidents, y compris ceux causés par des vulnérabilités exploitées concernant ces actifs, peuvent entraîner de graves

perturbations des chaînes d'approvisionnement des TIC dans l'ensemble du marché intérieur ou conduire à l'exfiltration de données;

c) la question de savoir s'il existe une dépendance à l'égard d'un nombre limité de fournisseurs de ces actifs;

d) les résultats des évaluations visées à l'article 99.

Article 103

Mesures d'atténuation dans la chaîne d'approvisionnement des TIC

1. La Commission est habilitée à adopter des actes d'exécution interdisant, lorsque cela est nécessaire pour garantir un niveau élevé de cybersécurité, de cyberrésilience et de confiance au sein de l'Union, à un type spécifique d'entités visées aux annexes I et II de la directive (UE) 2022/2555 d'utiliser, d'installer ou d'intégrer sous quelque forme que ce soit des composants TIC ou des composants TIC qui incluent des composants TIC provenant de fournisseurs à haut risque recensés conformément à l'article 104 dans des actifs TIC essentiels recensés conformément à l'article 102. Ces actes d'exécution prévoient des périodes de transition appropriées, au cours desquelles la Commission publie la liste des fournisseurs à haut risque visée à l'article 104, ainsi que des délais supplémentaires pour l'élimination progressive des composants TIC et des composants qui incluent des composants TIC concernés. Ces actes d'exécution peuvent également préciser ces composants TIC ou composants qui incluent des composants TIC.

2. La Commission est habilitée à adopter des actes d'exécution disposant, lorsque cela est nécessaire pour garantir un niveau élevé de cybersécurité, de cyberrésilience et de confiance au sein de l'Union, qu'un type spécifique d'entités visées aux annexes I et II de la directive (UE) 2022/2555 fait l'objet d'une ou plusieurs des mesures d'atténuation suivantes en ce qui concerne leur chaîne d'approvisionnement des TIC et en particulier les actifs TIC essentiels recensés conformément à l'article 102, afin d'atténuer les risques recensés lors des évaluations des risques de sécurité réalisées conformément à l'article 99:

a) l'application d'exigences de transparence concernant la fourniture à l'autorité compétente d'informations sur les fournisseurs de la chaîne d'approvisionnement des TIC pour les actifs TIC essentiels désignés conformément à l'article 102;

b) l'interdiction relative aux transferts de données vers des pays tiers et au traitement de données à distance depuis un pays tiers;

c) des mesures techniques devant faire l'objet d'un audit par un tiers, notamment:

i) le recours au traitement embarqué;

ii) la segmentation spécifique des systèmes de réseau;

iii) le blocage de tout accès physique ou à distance à des actifs TIC essentiels;

iv) la désactivation de fonctionnalités non essentielles;

v) la surveillance opérationnelle du réseau;

vi) les essais du matériel et des logiciels.

d) les restrictions liées au contrôle opérationnel, y compris l'externalisation de fonctions organisationnelles à des prestataires de services gérés;

e) les restrictions liées aux relations contractuelles de l'entité avec ses fournisseurs;

f) l'obligation que le service soit exploité, géré, entretenu ou soutenu par du personnel agréé par les autorités nationales compétentes concernées;

g) la diversification de l'offre de composants TIC ou de composants inclus dans des composants TIC.

3. Lorsqu'elle introduit les mesures visées au paragraphe 2, la Commission peut fixer des exigences techniques et méthodologiques applicables à ces mesures.

4. Avant d'adopter les actes d'exécution visés aux paragraphes 1 et 2, la Commission évalue les risques et dépendances potentiels et, en particulier:

a) le cas échéant, le niveau de risque associé à l'utilisation, à l'installation ou à l'intégration, sous quelque forme que ce soit, de composants TIC ou de composants qui incluent des composants TIC provenant de fournisseurs à haut risque dans des actifs TIC essentiels;

b) les incidences économiques et sociétales potentielles que l'obligation peut avoir sur les entités d'un des types visés aux annexes I et II de la directive (UE) 2022/2555;

c) la disponibilité d'autres fournisseurs que ceux à haut risque;

d) la perturbation potentielle des activités économiques et sociétales transfrontières causée par un incident affectant la chaîne d'approvisionnement des TIC d'une entité.

5. Les actes d'exécution visés aux paragraphes 1 et 2 du présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2 et font l'objet d'un réexamen au moins tous les 36 mois.

6. Dans des circonstances exceptionnelles, qui justifient une intervention visant à préserver le bon fonctionnement du marché intérieur et lorsque la Commission a des raisons suffisantes de considérer que l'utilisation, l'installation ou l'intégration de composants TIC ou de composants qui incluent des composants TIC provenant d'une entité spécifique établie dans un pays tiers ou contrôlée par un pays tiers, par des entités d'un pays tiers, ou par un ressortissant d'un pays tiers, représente un risque de cybersécurité non technique important pour les activités économiques ou sociétales d'au moins trois États membres, la Commission consulte sans délai les États membres sur la nécessité de prendre des mesures au niveau de l'Union.

7. La Commission est habilitée à adopter des actes d'exécution afin d'interdire à un type spécifique d'entités visées aux annexes I et II de la directive (UE) 2022/2555 d'utiliser, d'installer ou d'intégrer des composants TIC ou des composants qui incluent des composants TIC provenant d'une entité visée au paragraphe 6. À cette fin, elle consulte les entités des types visés aux annexes I et II de la directive (UE) 2022/2555 potentiellement concernées par l'interdiction. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2. Le cas échéant, ils prévoient des périodes appropriées pour la suppression progressive de ces composants TIC ou composants qui incluent des composants TIC. Ces actes d'exécution peuvent également préciser les composants TIC ou composants qui incluent des composants TIC auxquels s'applique l'interdiction. Cette interdiction concerne également les composants TIC, ou les composants qui incluent

des composants TIC, de toutes les entités contrôlées par l'entité spécifique visée au paragraphe 6.

8. Les actes d'exécution visés aux paragraphes 1, 2 et 7 peuvent également préciser que les mesures d'atténuation ne s'appliquent qu'aux types d'entités visés aux annexes I et II de la directive (UE) 2022/2555 d'une taille spécifique.

9. L'article 100, paragraphe 4, s'applique à l'entité spécifique établie dans un pays tiers ou contrôlée par un pays tiers, par une entité d'un pays tiers, ou par un ressortissant d'un pays tiers, visée au paragraphe 7.

10. Les actes d'exécution adoptés conformément aux paragraphes 1, 2 et 7 qui sont applicables aux types d'entités visés à l'annexe I, point 10, de la directive (UE) 2022/2555 s'appliquent mutatis mutandis à l'institution, aux organes et aux organismes de l'Union.

Article 104
Identification des fournisseurs à haut risque

1. Par voie d'actes d'exécution, la Commission établit des listes des fournisseurs à haut risque concernés par les interdictions énoncées dans les actes d'exécution adoptés conformément à l'article 103, paragraphes 1 et 7, ou par l'interdiction visée à l'article 111, paragraphe 1.

2. À cette fin, la Commission inventorie les fournisseurs des composants TIC et des composants qui incluent des composants TIC concernés par l'interdiction visée au paragraphe 1.

   Sur cette base, la Commission procède à une évaluation initiale afin de déterminer lesquels des fournisseurs inventoriés sont potentiellement établis dans un pays tiers désigné conformément à l'article 100 ou contrôlés par un tel pays tiers, par une entité établie dans un tel pays tiers ou par un ressortissant d'un tel pays tiers. La Commission procède également à un premier inventaire des fournisseurs potentiellement contrôlés par l'entité visée à l'article 103, paragraphe 6.

3. La Commission évalue le lieu d'établissement ainsi que la structure de propriété et de contrôle des fournisseurs initialement identifiés conformément au paragraphe 2, deuxième alinéa.

4. Aux fins de l'évaluation visée au paragraphe 3, la Commission est habilitée à demander aux fournisseurs les informations nécessaires. Si le fournisseur ne communique pas les informations nécessaires dans le délai fixé, la Commission peut conclure qu'il est établi dans un pays tiers désigné conformément à l'article 100 ou contrôlé parce pays tiers, par des entités de ce pays tiers ou par des ressortissants de ce pays tiers. Lorsque la Commission réalise une évaluation aux fins de l'article 103, paragraphe 7, et que le fournisseur ne communique pas les informations nécessaires dans le délai fixé, la Commission peut conclure que le fournisseur est contrôlé par une entité désignée conformément audit article. Les autorités compétentes visées à l'article 112 partagent également, sur demande, les informations pertinentes avec la Commission.

5. La Commission partage avec le fournisseur concerné les constatations préliminaires concernant l'évaluation de l'établissement, du contrôle et de la propriété. La Commission donne au fournisseur la possibilité d'être entendu sur ces constatations préliminaires.

6. La Commission peut demander à une autorité compétente de réaliser l'évaluation initiale de l'établissement, de la propriété et du contrôle d'un fournisseur, lorsque les caractéristiques du fonctionnement de ce fournisseur le justifient. Une autorité compétente peut proposer de procéder à cette évaluation initiale. La Commission vérifie ces constatations initiales afin de décider si le fournisseur doit être inclus dans la liste des fournisseurs à haut risque.

7. La Commission met régulièrement à jour la liste des fournisseurs à haut risque en vue de supprimer ou d'ajouter des fournisseurs à haut risque. Les fournisseurs à haut risque figurant sur la liste peuvent demander à la Commission de réévaluer leur établissement et leur structure de contrôle et de propriété s'ils apportent la preuve que des changements pertinents ont eu lieu.

8. Lorsqu'une autorité compétente constate, y compris sur la base d'informations fournies par une entité d'un des types visés aux annexes I et II de la directive (UE) 2022/2555, qu'un fournisseur est susceptible d'être inscrit sur une liste de fournisseurs à haut risque, elle en informe la Commission dans les meilleurs délais.

Article 105

Exemption pour les entités établies dans un pays tiers ou contrôlées par des entités d'un pays tiers suscitant des préoccupations en matière de cybersécurité

1. Une entité établie dans un pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlée par des entités d'un tel pays tiers désigné conformément à l'article 100 peut adresser à la Commission une demande motivée en vue d'être exemptée:

   a) de l'interdiction imposée aux entités d'un des types visés aux annexes I et II de la directive (UE) 2022/2555 d'utiliser, d'installer ou d'intégrer sous quelque forme que ce soit ses composants TIC ou composants qui incluent ses composants TIC dans les actifs TIC essentiels de ces entités, par dérogation à l'article 111 ou aux actes d'exécution adoptés en vertu de l'article 103, paragraphe 1;

   b) de l'interdiction de participer à des procédures de passation de marchés publics organisées conformément à la législation transposant la directive 2014/24/UE et la directive 2014/25/UE en ce qui concerne la fourniture de composants TIC ou de composants qui incluent des composants TIC destinés à être utilisés dans des actifs TIC essentiels définis conformément à l'article 102, par dérogation à l'article 100, paragraphe 4.

2. La demande visée au paragraphe 1:

   a) précise l'intérêt de l'entité établie dans un pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlée par des entités d'un tel pays tiers désigné conformément à l'article 100 à se voir accorder l'exemption visée au paragraphe 1 du présent article; et

   b) démontre clairement que des mesures d'atténuation efficaces seront mises en place pour faire face aux risques non techniques et garantir l'absence de toute éventuelle ingérence indue par le pays tiers désigné conformément à l'article 100 en ce qui concerne la fourniture de composants TIC ou de composants qui incluent des composants TIC pour l'utilisation, l'installation ou l'intégration dans des actifs TIC essentiels d'une entité d'un des types visés aux annexes I et II de la directive (UE) 2022/2555.

3. La Commission est habilitée à adopter des actes d'exécution pour préciser davantage les conditions visées au paragraphe 2, point b), et à établir des règles détaillées en ce qui concerne les procédures visées au présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.

4. La Commission évalue la demande visée au paragraphe 1 dans le cadre d'une procédure équitable et transparente, en tenant compte:

   a) des circonstances et des éléments supplémentaires visés à l'article 100, paragraphes 1 et 2, en ce qui concerne le pays désigné qui suscite des préoccupations en matière de cybersécurité pour les chaînes d'approvisionnement des TIC, dans lequel l'entité est établie ou à partir duquel elle est contrôlée;

   b) de l'efficacité des mesures d'atténuation visées au paragraphe 2, point b);

   c) de la question de savoir si l'exemption accordée à l'entité établie dans un pays tiers suscitant des préoccupations en matière de cybersécurité pour les chaînes d'approvisionnement des TIC ou contrôlée par des entités de ce pays tiers ne porterait pas atteinte aux intérêts de l'Union.

5. Lorsque la Commission conclut, à la suite de l'évaluation visée au paragraphe 3, qu'il est justifié d'accorder une exemption, elle le fait par voie de décision, qu'elle notifie au demandeur dans un délai de 9 mois à compter de la réception de la demande.

6. Lorsqu'elle adopte une décision visée au paragraphe 4, la Commission peut limiter l'exemption à une période donnée et la soumettre à des conditions pour l'entité, notamment:

   a) un calendrier de mise en œuvre des mesures d'atténuation visées au paragraphe 2, point b);

   b) des audits réguliers réalisés par des tiers afin de garantir la mise en œuvre effective des mesures d'atténuation;

   c) des obligations en matière d'établissement de rapports concernant le respect des règles.

7. Lorsque la Commission conclut, à la suite de l'évaluation visée au paragraphe 3, qu'il n'est pas justifié d'accorder une exemption, elle le fait par voie de décision, qu'elle notifie au demandeur dans un délai de 9 mois à compter de la réception de la demande.

8. La Commission peut, de sa propre initiative, retirer ou modifier la décision visée au paragraphe 4 dans une ou plusieurs des situations suivantes:

   a) l'un des faits sur lesquels la décision repose subit un changement important;

   b) l'entité qui a demandé l'exemption agit contrairement à ses engagements;

   c) l'exemption était fondée sur des informations incomplètes, inexactes ou trompeuses fournies par l'entité à l'origine de la demande.

Article 106
Droits de la défense

La Commission veille à ce que, avant l'adoption d'un acte d'exécution en vertu de l'article 103, paragraphe 7, ou d'une décision refusant l'octroi d'une exemption en vertu de l'article 105, paragraphe 7, sur la base d'éléments qui n'ont pas été présentés par le demandeur, ou avant le retrait d'une décision en vertu de l'article 105, paragraphe 8, l'entité concernée ait la possibilité d'être entendue, compte tenu de la nécessité, dans certains cas, d'une procédure d'urgence.

Article 107
Registre

La Commission tient un registre, accessible au public, contenant ses décisions visées à l'article 105, paragraphe 5. Ce registre indique le nom des entités qui ont fait l'objet de telles décisions. La Commission met régulièrement à jour ce registre.

Article 108
Confidentialité

Les informations recueillies par la Commission en application des articles 105 et 106 ne peuvent être utilisées qu'aux fins auxquelles elles ont été recueillies.

Article 109
Redevances

1. La Commission perçoit des redevances pour les demandes présentées conformément à l'article 105, paragraphe 1.
2. Les redevances sont exprimées et perçues en euros.
3. Les redevances sont proportionnées aux coûts liés au traitement des demandes visées à l'article 105, paragraphe 1, à l'évaluation des critères et des informations visés à l'article 105, paragraphe 2, ainsi qu'à la mise en place, à la tenue et au fonctionnement du registre visé à l'article 107. Toutes les dépenses de la Commission imputées au personnel participant à ces activités sont incluses dans ces coûts.
4. La Commission adopte des actes d'exécution établissant des règles détaillées relatives aux redevances et précisant leur montant et leurs modalités de paiement. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.

CHAPITRE II
Chaînes d'approvisionnement des TIC dans les réseaux de communications électroniques

Article 110
Actifs TIC essentiels pour les réseaux de communications électroniques mobiles, fixes et par satellite

1. Les actifs TIC essentiels pour les réseaux de communications électroniques mobiles, fixes et par satellite sont définis à l'annexe II.

2. Les composants TIC ou composants qui incluent des composants TIC fournis par des fournisseurs à haut risque sont progressivement retirés des actifs TIC essentiels des réseaux de communications électroniques mobiles, fixes et par satellite.

3. Le délai de suppression des composants TIC ou composants qui incluent des composants TIC fournis par des fournisseurs à haut risque en ce qui concerne les réseaux de communications électroniques mobiles ne dépasse pas 36 mois à compter de la publication de la liste des fournisseurs à haut risque visée à l'article 104 qui sont pertinents pour les réseaux de communications électroniques mobiles.

4. La Commission est habilitée à adopter des actes d'exécution conformément à l'article 118, paragraphe 2, afin de préciser les délais de suppression des composants TIC ou composants qui incluent des composants TIC fournis par des fournisseurs à haut risque en ce qui concerne les réseaux de communications électroniques fixes et par satellite.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 119 pour modifier l'annexe II du présent règlement afin de l'adapter aux évolutions technologiques en tenant compte des éléments visés à l'article 103, paragraphe 4.

Article 111

Interdictions applicables aux réseaux de communications électroniques mobiles, fixes et par satellite

1. Les fournisseurs de réseaux de communications électroniques mobiles, fixes et par satellite n'utilisent, n'installent ni n'intègrent, sous quelque forme que ce soit, de composants TIC ou composants qui incluent des composants TIC provenant de fournisseurs à haut risque dans le cadre de l'exploitation des actifs TIC essentiels visés à l'annexe II.

2. Dans les cas où l'autorité compétente désignée en vertu du présent règlement dans un État membre diffère de l'autorité compétente désignée en vertu du règlement (UE) XX/XXXX [proposition de règlement sur les réseaux numériques], l'autorité compétente désignée en vertu du présent règlement informe sans tarder l'autorité compétente désignée en vertu du règlement (UE) XX/XXXX [proposition de règlement sur les réseaux numériques] des mesures imposées aux fournisseurs de réseaux de communications électroniques mobiles, fixes et par satellite conformément à l'article 114. Les autorités coopèrent étroitement aux fins d'une surveillance et d'une exécution efficaces de ces mesures.

CHAPITRE III

Autorités compétentes, surveillance et exécution, compétence, droits de la défense

Article 112

Autorités compétentes

1. Chaque État membre désigne les autorités compétentes visées à l'article 8 de la directive (UE) 2022/2555 comme autorités chargées de prendre les mesures de surveillance et d'exécution visées à l'article 114.

2. Les autorités compétentes sont, sur les plans structurel et fonctionnel, totalement impartiales et libres de toute influence extérieure, directe ou indirecte; en particulier,

elles ne sollicitent ni n'acceptent d'instructions d'aucune autre autorité publique ni d'aucune partie privée.

3. Les États membres veillent à ce que leurs autorités compétentes disposent des pouvoirs appropriés, des ressources humaines et techniques suffisantes et de l'expertise nécessaire pour mettre en œuvre efficacement les mesures de surveillance et d'exécution visées à l'article 114.

4. Chaque État membre notifie dans les meilleurs délais à la Commission les noms des autorités compétentes désignées conformément au paragraphe 1, les tâches respectives de ces autorités et toute modification ultérieure les concernant. Chaque État membre rend également publics les noms des autorités compétentes désignées conformément au paragraphe 1.

Article 113
Réseau de coopération et services de soutien de la Commission

En vue d'une surveillance efficace, la Commission met en place un réseau de coopération entre les autorités compétentes des États membres visées à l'article 112 et la Commission afin de servir de plateforme de coopération et d'échange d'informations, en particulier aux fins de l'évaluation de l'établissement, du contrôle et de la propriété visée à l'article 104. La Commission apporte le soutien administratif nécessaire au réseau.

Article 114
Mesures de surveillance et d'exécution

1. Les autorités compétentes visées à l'article 112 sont habilitées à prendre des mesures de surveillance et d'exécution à l'égard des entités d'un des types visés aux annexes I et II de la directive (UE) 2022/2555. Les États membres veillent à ce que les mesures susmentionnées soient effectives, proportionnées et dissuasives, compte tenu des circonstances propres à chaque cas d'espèce. Les États membres notifient à la Commission les règles adoptées à cet effet et leurs modifications ultérieures.

2. Lorsqu'elles exercent leurs missions de surveillance à l'égard des entités visées aux annexes I et II de la directive (UE) 2022/2555, les autorités compétentes sont habilitées à:

   a) exiger de ces entités une liste détaillée et à jour de leurs fournisseurs et prestataires de services concernés;

   b) demander à ces entités l'accès aux données, documents et informations nécessaires pour vérifier le respect du présent règlement;

   c) soumettre ces entités à des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés;

   d) interroger ces entités sur la composition des produits matériels ou logiciels installés ou intégrés sous quelque forme que ce soit dans le réseau ou le système, y compris les composants et les dépendances transitoires, dans un format couramment utilisé et lisible par machine.

3. Lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard des entités d'un des types visés aux annexes I et II de la directive (UE) 2022/2555, les autorités compétentes sont habilitées à:

a) émettre des avertissements sur les violations du présent règlement commises par les entités concernées, en exposant les faits et considérations juridiques pertinents;

b) adopter des décisions exigeant des entités concernées qu'elles remédient à la violation du présent règlement ou aux manquements constatés dans la mise en œuvre des mesures d'atténuation;

c) ordonner aux entités concernées de cesser les activités qui enfreignent le présent règlement et de ne pas les réitérer; et

d) infliger des sanctions, conformément aux règles relatives au montant prévu à l'article 115, ou demander que ces sanctions soient infligées par les instances, juridictions ou tribunaux compétents, conformément au droit national.

4. Lorsqu'elles prennent l'une des mesures d'exécution visées au paragraphe précédent, les autorités compétentes tiennent dûment compte des circonstances propres à chaque cas et des facteurs suivants:

a) la gravité de la violation et l'importance des dispositions enfreintes;

b) la durée de la violation;

c) le chiffre d'affaires pertinent de l'entité concernée;

d) toute violation antérieure pertinente commise par l'entité concernée;

e) le cas échéant, les dommages matériels, corporels ou moraux causés par la violation, y compris les pertes financières ou économiques, les effets sur d'autres entités et le nombre d'utilisateurs touchés;

f) le fait que l'entité concernée a agi délibérément ou par négligence;

g) les mesures prises par l'entité pour prévenir ou atténuer les dommages matériels, corporels ou moraux;

h) le degré de coopération avec les autorités compétentes des personnes physiques ou morales tenues pour responsables.

Aux fins du premier alinéa, point a), sont considérés comme violations graves:

i) les infractions répétées;

j) le fait de ne pas notifier des incidents importants ou de ne pas y remédier;

k) le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes des autorités compétentes.

5. Les autorités compétentes informent les entités concernées de leurs conclusions préliminaires avant de prendre des mesures d'exécution. Les entités concernées disposent d'un délai raisonnable pour présenter leurs observations sur les constatations préliminaires. Les autorités compétentes exposent en détail les motifs de leurs mesures d'exécution.

6. Les autorités compétentes respectent les principes de confidentialité et de secret professionnel et commercial.

7. Les autorités compétentes coopèrent entre elles et avec la Commission aux fins de la surveillance et de l'exécution en vertu du présent titre conformément à l'article 116.

Article 115
Sanctions

1. Les États membres déterminent le régime des sanctions applicables aux violations du présent règlement et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions.

2. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.

3. Les sanctions sont imposées en complément de l'une ou l'autre des mesures visées à l'article 114, paragraphe 3, points a) à c).

4. Au moment de décider s'il y a lieu d'imposer une sanction et de décider de son montant, dans chaque cas d'espèce, il est dûment tenu compte, au minimum, des facteurs visés à l'article 114, paragraphe 4, premier alinéa.

5. Les violations de l'article 103, paragraphe 2, point a), sont passibles, conformément au paragraphe 3 du présent article, de sanctions représentant au maximum 1 % du chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent par l'entreprise à laquelle l'entité appartient.

6. Les violations de l'article 103, paragraphe 2, points b) à g), sont passibles, conformément au paragraphe 3 du présent article, de sanctions représentant au maximum 2 % du chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent par l'entreprise à laquelle l'entité appartient.

7. Les violations de l'article 103, paragraphe 1, et à l'article 111, sont passibles, conformément au paragraphe 3 du présent article, de sanctions représentant au maximum 7 % du chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent par l'entreprise à laquelle l'entité appartient.

Article 116
Assistance mutuelle

1. Lorsqu'une entité d'un des types visés aux annexes I ou II de la directive (UE) 2022/2555 fournit des services dans plus d'un État membre, ou fournit des services dans un ou plusieurs États membres et que ses actifs TIC essentiels sont situés dans un ou plusieurs autres États membres, les autorités compétentes des États membres concernés et la Commission coopèrent et se prêtent mutuellement assistance en vue de garantir l'application effective et efficace du règlement. À cette fin, les règles suivantes s'appliquent au minimum:

   a) les autorités compétentes appliquant des mesures de supervision ou d'exécution dans un État membre informent et consultent les autorités compétentes des autres États membres concernés en ce qui concerne les mesures de supervision et d'exécution prises;

   b) une autorité compétente d'un État membre peut demander à une autre autorité compétente d'un autre État membre de prendre des mesures de supervision ou d'exécution;

   c) une autorité compétente d'un État membre, dès réception d'une demande motivée d'une autre autorité compétente d'un autre État membre, fournit à

cette autre autorité compétente, dans toute la mesure du possible, une assistance mutuelle afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente.

2. L'assistance mutuelle visée au paragraphe 1, point c), peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés. Une autorité compétente à laquelle une demande d'assistance est adressée ne peut refuser cette demande que s'il est établi que l'autorité n'est pas compétente pour fournir l'assistance demandée, que l'assistance demandée n'est pas proportionnée aux tâches de supervision de l'autorité compétente ou que la demande concerne des informations ou implique des activités dont la divulgation ou l'exercice seraient contraires aux intérêts essentiels de la sécurité nationale, la sécurité publique ou la défense de cet État membre. Avant de refuser une telle demande, l'autorité compétente consulte les autres autorités compétentes concernées ainsi que, à la demande de l'un des États membres concernés, la Commission.

3. Le cas échéant et d'un commun accord, les autorités compétentes de différents États membres peuvent mener à bien des actions communes de supervision.

4. Compte tenu de l'obligation de respecter les principes de confidentialité et de secret professionnel et commercial visés à l'article 114, paragraphe 6, toute information échangée dans le cadre d'une demande d'assistance et fournie en vertu du présent article n'est utilisée qu'aux fins pour lesquelles elle a été demandée.

Article 117
Compétence et territorialité

1. Les entités d'un type visé aux annexes I et II de la directive (UE) 2022/2555 relevant du champ d'application du présent règlement sont considérées comme relevant de la compétence de l'État membre dans lequel elles sont établies, à l'exception des cas suivants:

   a) les fournisseurs de réseaux de communications électroniques publics ou les fournisseurs de services de communications électroniques accessibles au public, qui sont considérés comme relevant de la compétence de l'État membre dans lequel ils fournissent leurs services;

   b) les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux, qui sont considérés comme relevant de la compétence de l'État membre dans lequel ils ont leur établissement principal dans l'Union en application du paragraphe 2;

   c) les entités de l'administration publique, qui sont considérées comme relevant de la compétence de l'État membre auxquelles elles appartiennent;

   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) nº 1008/2008 du Parlement européen et du Conseil[83] ou, lorsque la licence d'exploitation ou l'équivalent n'a pas été délivré conformément audit règlement, qui sont considérés comme relevant de la compétence de l'État membre dans lequel ils ont leur établissement principal dans l'Union en vertu du paragraphe 2.

2. Aux fins du présent règlement, une entité visée au paragraphe 1, point b), est réputée avoir son établissement principal dans l'Union dans l'État membre où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Si un tel État membre ne peut être déterminé ou si ces décisions ne sont pas prises dans l'Union, l'établissement principal est réputé se trouver dans l'État membre où la plupart des opérations de cybersécurité sont effectuées. Si un tel État membre ne peut être déterminé, l'établissement principal est réputé se trouver dans l'État membre où l'entité concernée possède l'établissement comptant le plus grand nombre de salariés dans l'Union.

3. Si une entité d'un type visé aux annexes I et II de la directive (UE) 2022/2555 n'est pas établie dans l'Union mais offre des services dans l'Union, elle désigne un représentant dans l'Union. Le représentant est établi dans l'un des États membres dans lesquels les services sont fournis. Une telle entité est réputée relever 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 réputée relever 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 du présent règlement.

4. La désignation d'un représentant par une entité visée au paragraphe 1, point b), est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même.

5. Les États membres qui ont reçu une demande d'assistance mutuelle en lien avec une entité visée au paragraphe 1, point b), peuvent, dans les limites de cette demande, prendre des mesures de supervision et d'exécution appropriées à l'égard de l'entité concernée lorsque celle-ci fournit des services ou dispose d'un réseau et d'un système d'information sur leur territoire.

TITRE VI
DISPOSITIONS FINALES

Article 118
Procédure de comité

1. La Commission est assistée par un comité. Ce comité existe en deux configurations. En ce qui concerne les titres II et III, la Commission est assistée par ce comité dans sa première configuration, tandis qu'en ce qui concerne le titre IV, la Commission est

[83] 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: https://eur-lex.europa.eu/eli/reg/2008/1008/oj/eng).

assistée par ce comité dans sa seconde configuration. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nºº182/2011 s'applique.

Article 119
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter les actes délégués conformément à l'article 80, paragraphe 2, et à l'article 110, paragraphe 5, est conféré à la Commission pour une durée indéterminée à partir de la date d'entrée en vigueur du présent règlement.

3. La délégation de pouvoir visée à l'article 80, paragraphe 2, et à l'article 110, paragraphe 5, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 80, paragraphe 2, et de l'article 110, paragraphe 5, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 120
Évaluation et réexamen

1. Au plus tard le [JJ MM AAAA], et tous les cinq ans par la suite, la Commission commande une évaluation qui est menée conformément à ses lignes directrices.

2. L'évaluation visée au paragraphe 1 porte notamment sur les éléments suivants:

   a) les performances de l'ENISA au regard de ses objectifs, de son mandat, de sa mission, de ses tâches, de sa gouvernance et de sa localisation;

   b) l'efficacité, l'efficience et la valeur ajoutée européenne des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité prévus au titre II, chapitre II, section 4, du présent règlement;

   c) les effets, l'efficacité et l'efficience des dispositions du titre III du présent règlement au regard des objectifs consistant à garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC, services de

sécurité gérés et entités dans l'Union et à améliorer le fonctionnement du marché intérieur;

d) l'incidence, l'efficacité et l'efficience des dispositions du titre IV du présent règlement en ce qui concerne les objectifs du cadre digne de confiance pour la chaîne d'approvisionnement des TIC.

3. L'évaluation visée au paragraphe 1, point a), examine, en particulier, la nécessité éventuelle de modifier le mandat de l'ENISA et les conséquences financières d'une telle modification.

4. Une fois sur deux, dans le cadre de l'évaluation visée au paragraphe 1, point a), la Commission apprécie les résultats obtenus par l'ENISA en tenant compte des objectifs, du mandat, de la mission, de la gouvernance et des tâches de celle-ci, et détermine si le maintien de l'Agence est toujours justifié au regard de ces objectifs, de ce mandat, de cette mission, de cette gouvernance et de ces tâches.

5. La Commission fait rapport des conclusions de l'évaluation au Parlement européen, au Conseil et au conseil d'administration. Les résultats de l'évaluation sont rendus publics.

Article 121
Abrogation et poursuite des activités

1. Le règlement (UE) 2019/881 du Parlement européen et du Conseil est abrogé avec effet au JJMMAAAA.

2. Les références au règlement (UE) 2019/881, à l'ENISA et aux schémas européens de certification de cybersécurité établis par ledit règlement s'entendent comme faites au présent règlement et sont à lire selon le tableau de correspondance figurant à l'annexe III du présent règlement.

3. En vertu du présent règlement, l'ENISA poursuit les opérations et les activités de l'ENISA instituée par le règlement (UE) 2019/881 en ce qui concerne tous les droits de propriété, accords, obligations légales, contrats de travail, engagements financiers et responsabilités. Toutes les décisions du conseil d'administration et du conseil exécutif adoptées conformément au règlement (UE) 2019/881 restent valables, pour autant qu'elles respectent le présent règlement.

4. Le directeur exécutif nommé en vertu de l'article 15, paragraphe 1, point n), du règlement (UE) 2019/881 reste en fonction et assume les tâches et responsabilités du directeur exécutif visées à l'article 32 du présent règlement pour la durée restante de son mandat. Les autres conditions de son contrat demeurent inchangées.

5. Les schémas candidats dont la préparation a été demandée conformément à l'article 49 du règlement (UE) 2019/881 sont réputés avoir été demandés conformément aux dispositions correspondantes du présent règlement. Les dispositions du titre III du présent règlement s'appliquent à ces systèmes candidats en conséquence.

6. Les membres du conseil d'administration nommés par la Commission et leurs suppléants nommés en application de l'article 14 du règlement (UE) 2019/881 restent en fonction et exercent les fonctions du conseil d'administration visées à l'article 27 du présent règlement pour la durée restante de leur mandat. Les membres du conseil d'administration nommés par les États membres en application de l'article 14 du règlement (UE) 2019/881 restent en fonction et exercent les fonctions du conseil

d’administration visées à l’article 27 du présent règlement pour autant qu’ils exercent les fonctions visées à l’article 24, paragraphe 3, du présent règlement.

Article 122
Entrée en vigueur

Le présent règlement entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l’Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*

FICHE FINANCIÈRE ET NUMÉRIQUE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

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)

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

Titre abrégé: Règlement sur la cybersécurité (CSA2)

et

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

1.2. Domaine(s) politique(s) concerné(s)

Domaine(s) politique(s): 09 – Réseaux de communication, contenu et technologies

Activité(s): 09.02 Marché unique numérique

1.3. Objectif(s)

1.3.1. Objectif général / objectifs généraux

Les principaux objectifs de l'intervention sont les suivants:

(1) Renforcer les capacités et la résilience en matière de cybersécurité

Contribuer à renforcer la gouvernance de l'Union en matière de cybersécurité et à faire en sorte que les institutions, autorités et autres parties prenantes concernées soient mieux préparées à prévenir et à détecter les menaces en matière de cybersécurité et à y réagir de manière coordonnée et efficace.

(2) Prévenir la fragmentation au sein du marché intérieur:

en soutenant l'élaboration, la mise en œuvre et l'adoption d'instruments communs de l'Union en matière de cybersécurité, tels que les schémas de certification, et en fournissant des cadres harmonisés qui renforcent la confiance et l'interopérabilité entre les États membres.

Ces objectifs généraux répondent aux principaux défis recensés dans la définition du problème figurant dans l'analyse d'impact de l'initiative proposée. Ils reflètent l'objectif stratégique global consistant à renforcer la gouvernance de la cybersécurité dans l'Union et à soutenir le développement d'un marché unique numérique sûr, résilient et compétitif.

1.3.2. Objectif(s) spécifique(s)

Remédier au décalage entre le cadre d'action de l'Union en matière de cybersécurité et les besoins des parties prenantes:

Objectif spécifique nº 1: créer les capacités nécessaires pour mettre en œuvre efficacement les politiques de cybersécurité de l'Union et une coopération opérationnelle continue qui permettra une coopération plus structurée entre les États membres.

Objectif spécifique nº 2: élaborer et mettre en œuvre des moyens et des mécanismes permettant de soutenir et de répondre efficacement aux besoins des États membres, de l'industrie et des autres parties prenantes.

Remédier à l'adoption et à l'efficacité limitées du cadre européen de certification de cybersécurité (ECCF):

Objectif spécifique nº 3: créer les conditions préalables à une mise en œuvre plus rapide des schémas de certification de cybersécurité en fonction des besoins du marché, en élargissant le champ d'application de l'ECCF, en garantissant une maintenance efficace et des procédures souples et en renforçant la transparence.

Remédier à la fragmentation du paysage de la conformité et à la complexité des cadres horizontaux et sectoriels:

Objectif spécifique nº 4: créer des mécanismes et des conditions pour faciliter le respect des exigences en matière de cybersécurité, en rendant ainsi leur mise en œuvre plus cohérente et plus efficace.

Faire face aux risques de cybersécurité dans la chaîne d'approvisionnement:

Objectif spécifique nº 5: réduire les risques pour les chaînes d'approvisionnement critiques des TIC posés par les entités établies dans des pays ou contrôlées par des entités de pays qui suscitent des préoccupations en matière de cybersécurité (fournisseurs à haut risque) et réduire les dépendances critiques en élaborant un cadre cohérent et efficace au niveau de l'Union pour faire face aux risques liés à la sécurité des chaînes d'approvisionnement des TIC.

1.3.3. Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

Les résultats attendus sont les suivants:

(1) Réforme fonctionnelle de l'ENISA

(2) Réforme de l'ECCF – extension du champ d'application, nouvelle procédure et gouvernance révisée

(3) Poursuite de la simplification du respect du cadre législatif applicable de l'Union en matière de cybersécurité

(4) Cadre global et horizontal pour faire face aux risques de cybersécurité dans les chaînes d'approvisionnement des TIC

Impact global

La proposition aura une incidence considérable sur la cybersécurité dans l'Union, car elle envisage de nombreux aspects tels que le nécessaire renforcement de l'Agence de l'Union européenne pour la cybersécurité, renforce le soutien à la mise en œuvre du droit de l'Union, introduit des réformes en vue d'une mise en œuvre harmonieuse du cadre européen de certification, favorise la compréhension commune par l'Union des cybermenaces et aborde l'atténuation des risques de cybersécurité sous l'angle de la réalité géopolitique. La mise en œuvre des dispositions proposées garantira des niveaux élevés d'efficacité et de cohérence et évitera une charge réglementaire excessive. Le train de mesures est conçu pour être résilient face aux difficultés de mise en œuvre et pour favoriser la cohérence des politiques à long terme dans l'ensemble de l'écosystème numérique et de cybersécurité. Il améliore la clarté, supprime les inefficacités et aligne les procédures de différents cadres juridiques,

tout en contribuant à atteindre un niveau élevé de cybersécurité dans l'ensemble de l'Union. L'un des grands objectifs prioritaires de la Commission européenne est que les efforts de simplification envisagés génèrent des avantages économiques considérables pour les entreprises, y compris les PME (plus de 14,63 milliards d'euros), et pour les pouvoirs publics (7,5 millions d'euros).

Les résultats spécifiques comprennent:

- une sensibilisation accrue et une meilleure coordination opérationnelle, ce qui pourrait permettre aux entreprises, aux pouvoirs publics et aux citoyens de réaliser des économies considérables grâce à une détection plus précoce des incidents et une réponse plus rapide;
- une clarification du champ d'application et du mandat de l'ENISA, tout en assurant la hiérarchisation nécessaire de ses tâches principales;
- la réception par les parties prenantes d'un soutien adéquat pour la mise en œuvre des politiques, les activités opérationnelles et la coordination générale;
- un soutien apporté à la conscience situationnelle commune de l'Union;
- une coopération renforcée avec EU-CyCLONe, le réseau des CSIRT, la Commission, Europol, le CERT-UE et les entités concernées de l'Union dans le but de mettre au point des répertoires de renseignements vérifiés et fiables sur les cybermenaces;
- un soutien des efforts visant à atténuer les attaques par rançongiciel;
- une coordination renforcée avec le secteur privé sur les sujets ayant trait à la cybersécurité;
- la diffusion d'informations en temps utile au moyen d'alertes précoces sur un incident important ou majeur, ou une cybermenace de nature transfrontière, concernant des secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555;
- la promotion de synergies efficaces avec d'autres organes et agences de l'Union;
- la réduction du prix des certifications de compétences, notamment en augmentant l'offre sur le marché grâce à la mise en place des programmes d'attestation européenne des compétences;
- la fourniture d'un soutien visant à combler le déficit de compétences en Europe au moyen d'attestations individuelles européennes des compétences en matière de cybersécurité et à aider les États membres et l'industrie à renforcer leur main-d'œuvre;
- la remédiation au manque de clarté et d'incidence du cadre de l'ECCF, grâce à l'élargissement de son champ d'application et à l'amélioration de son modèle de gouvernance;
- l'amélioration de la réputation des schémas adoptés grâce à la mise en place d'une structure de maintenance et à l'introduction d'un processus d'élaboration transparent et en temps utile;
- la mise en place d'un mécanisme de redevances en rapport avec les coûts liés à l'élaboration et à la maintenance des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, au traitement des

demandes et à l'octroi d'agréments aux fournisseurs, ainsi qu'à la maintenance des schémas adoptés dans le cadre de l'ECCF, ce qui contribuera à la stabilité financière de l'Agence et permettra de réaliser des économies au titre du budget de l'Union;

- l'alignement des schémas européens de certification sur le cadre législatif existant, qui permettra de mieux soutenir les efforts de mise en œuvre et les besoins des entreprises en matière de conformité;
- l'adoption de schémas actuellement bloqués;
- une compétitivité accrue des entreprises européennes, grâce aux efforts visant à encourager l'alignement des normes internationales et européennes;
- une fragmentation réduite des mesures et des exigences en matière de cybersécurité;
- de la clarté juridique et une charge administrative considérablement réduite, sans entraîner d'insécurité juridique importante parmi les parties prenantes qui sont en train de s'adapter aux cadres juridiques récemment adoptés;
- une mise en conformité facilitée pour les entités relevant de la directive SRI 2, qui contribuerait également à un meilleur taux de conformité global et à la mise en place de mesures de cybersécurité plus significatives, tout en rendant le processus de surveillance plus efficace du côté des autorités;

Autres

- L'initiative aurait de nombreux effets positifs sur les PME, compte tenu de l'amélioration de la compétitivité sur le marché de la cybersécurité de l'Union, ainsi que de la réduction des coûts et de la charge administrative:

1. *Rôle positif pour les PME, qui bénéficieraient d'une cyberrésilience accrue grâce au renforcement du rôle de l'ENISA et aux orientations techniques fournies par l'Agence.*
2. *Les PME, en tant que fournisseurs d'attestations agréés dans le cadre du schéma européen d'attestation des compétences, gagneront en visibilité et en réputation et se feront de nouveaux clients. En outre, les attestations individuelles européennes de compétences en matière de cybersécurité aideront les PME à repérer les candidats possédant les compétences adéquates.*
3. *Des schémas européens de certification efficaces peuvent faciliter le choix de technologies TIC fiables pour les PME et contribuer à renforcer leur cyberrésilience globale.*
4. *En tant que fournisseurs de DNS, les PME bénéficieront de mesures liées à la mise en œuvre de la directive SRI 2 en raison de l'exclusion des fournisseurs de DNS du champ d'application.*
5 *Les clarifications du champ d'application qui limiteraient l'application des obligations à certaines entités dans certains secteurs énumérés dans la directive SRI 2 seraient bénéfiques pour les PME.*
6. *En ce qui concerne les mesures de sécurité de la chaîne d'approvisionnement des TIC, l'utilisation de technologies fiables serait bénéfique aux PME en général. En tant que fournisseurs actifs dans les secteurs soumis à des restrictions, les PME seraient plus lourdement touchées que les grandes entreprises par les coûts de substitution et de transaction. Toutefois, en tant que fournisseurs de confiance, elles bénéficieront de nouveaux débouchés commerciaux.*

- Aucun des objectifs ne devrait entraîner d'incidence environnementale significative;

- En ce qui concerne le budget de l'UE, le renforcement de la coopération et de la coordination des activités entre les institutions, organes et organismes de l'UE devrait se traduire par des gains d'efficacité. Des économies sont attendues à long terme grâce à l'introduction de mécanismes de redevances.

1.3.4. Indicateurs de performance

Préciser les indicateurs permettant de suivre l'avancement et les réalisations.

Objectif: créer les capacités nécessaires pour mettre en œuvre efficacement les politiques de cybersécurité de l'Union et une coopération opérationnelle régulière/continue qui permettra une coopération plus structurée entre les États membres.

– Nombre de contributions pertinentes de l'ENISA à la mise en œuvre des politiques et initiatives législatives nationales et de l'Union

– Retour d'information positif des parties prenantes concernant les contributions pertinentes de l'ENISA

– Augmentation de 25 % par rapport au niveau de référence de 2023, comme indiqué dans le rapport annuel d'activité de l'ENISA (pour le nombre de contributions pertinentes) et dans l'enquête annuelle de satisfaction de l'ENISA (pour les retours d'information positifs)

– Statistiques d'utilisation de la base de données européenne des vulnérabilités

– Augmentation de 25 % du nombre d'utilisateurs par rapport à 2025

– Disponibilité, sécurité et fonctionnement de la plateforme du règlement sur la cyberrésilience

– Diminution de 25 % des temps d'arrêt de la plateforme et du nombre d'incidents par rapport aux statistiques de 2025 sur les temps d'arrêt et les incidents sur la plateforme

Objectif: élaborer et déployer des moyens et des mécanismes permettant de soutenir et de répondre efficacement aux besoins des États membres, de l'industrie et des autres parties prenantes.

– Nombre de parties prenantes soutenues par l'ENISA et qualité du soutien apporté.

– Nombre de mesures déployées pour soutenir les parties prenantes.

– Augmentation de 10 % du nombre de parties prenantes soutenues et augmentation de 10 % du niveau de satisfaction des parties prenantes soutenues par rapport à 2025

Objectif: créer les conditions préalables à une mise en œuvre plus rapide des schémas de certification de cybersécurité en fonction des besoins du marché en élargissant le champ d'application de l'ECCF, en garantissant une maintenance efficace et des procédures souples et en améliorant la transparence.

– Nombre de schémas adoptés

– Réduction de 50 % du temps nécessaire à l'élaboration d'un schéma par rapport à 2025

– Nombre de certificats valables délivrés chaque année

– Augmentation de 25 % par rapport au niveau de référence de 2025

– Retours d'information positifs des parties prenantes en ce qui concerne leur participation à l'élaboration des schémas et à la transparence de l'ECCF

– Augmentation de 25 % par rapport au scénario de référence dans l'enquête annuelle de satisfaction de l'ENISA par rapport à 2027

Objectif: mettre en place des mécanismes et des conditions pour faciliter le respect des exigences en matière de cybersécurité et rendre ainsi leur mise en œuvre plus cohérente et plus efficace.

– Pourcentage des coûts supportés par les PME pour se conformer à la directive SRI 2 et aux règles de cybersécurité, par rapport à l'ensemble des coûts de mise en conformité

– > 70 % de PME faisant état d'une réduction de leurs coûts de mise en conformité en matière de cybersécurité par rapport à 2025

– Nombre d'attaques par rançongiciel et montant des dommages en euros

– Réduction du nombre d'attaques par rançongiciel de plus de 1 % par rapport à 2027

– Pourcentage d'incidents transfrontières pendant ou après lesquels les autorités des États membres ont eu recours à des mécanismes d'assistance mutuelle

– Augmentation de plus de 20 points de pourcentage par rapport à 2025 de la proportion de cas dans lesquels l'assistance mutuelle a été utilisée

Objectif: réduire les dépendances critiques en élaborant un cadre cohérent et efficace au niveau de l'Union pour faire face aux risques liés à la sécurité des chaînes d'approvisionnement des TIC.

– Nombre de mesures adoptées

– Augmentation de 25 % du nombre de mesures adoptées et d'actifs essentiels recensés par rapport à la date d'adoption + 6 mois

– Diminution de 25 %, par rapport à 2025, de la dépendance à l'égard de fournisseurs d'actifs de TIC essentiels à haut risque

1.4. La proposition/l'initiative porte sur:

☒ Une nouvelle action (titre IV Chaîne d'approvisionnement, titre V Simplification)

☐ une action nouvelle suite à un projet pilote/une action préparatoire[84]

[84] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

☒ La prolongation d'une action existante (*titre II Mandat de l'ENISA et titre III Certification*)

☐ une fusion ou une réorientation d'une ou de plusieurs actions vers une autre action/une action nouvelle

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

En juillet 2024, dans ses orientations politiques[85], la présidente de la Commission européenne, Ursula von der Leyen, a appelé à simplifier, consolider et codifier la législation de l'Union afin d'éliminer les éventuels chevauchements et contradictions, tout en maintenant des normes élevées. La lettre de mission de la vice-présidente exécutive Henna Virkkunen[86] mentionne en particulier l'amélioration du processus d'adoption des schémas européens de certification de cybersécurité et la nécessité de protéger nos industries, nos citoyens et nos administrations publiques contre les menaces internes et externes. En outre, le rapport Niinistö de 2024[87] appelle à réduire les risques de dépendances indésirables à l'égard de la chaîne d'approvisionnement dans les technologies critiques. Les rapports commandés par la présidente de la Commission européenne, à savoir les rapports Draghi[88] et Letta[89] tournaient en grande partie autour de la nécessité de maintenir la compétitivité du marché unique grâce à la simplification et de garantir les niveaux les plus élevés de sécurité et d'autonomie stratégique. Sur cette base, la révision du règlement sur la cybersécurité représente une pierre angulaire des travaux de la Commission sur la sécurité et constitue le déploiement d'une révision ambitieuse de l'écosystème réglementaire européen en matière de cybersécurité. La proposition de règlement sur la cybersécurité 2 introduit des mécanismes visant à faire face aux risques de cybersécurité dans la chaîne d'approvisionnement ainsi que des mécanismes visant à réduire la fragmentation du paysage de la conformité et la complexité des cadres horizontaux et sectoriels. L'ENISA devrait également être un vecteur de simplification accrue des obligations de notification grâce à l'intégration d'un point d'entrée unique.

En outre, compte tenu du nombre de dispositions sectorielles introduites après l'adoption du règlement sur la cybersécurité en 2019, ainsi que de l'évolution rapide du paysage des menaces de cybersécurité, le mandat de l'ENISA doit être revu afin de définir un ensemble de tâches renouvelé et plus ciblé, en vue de soutenir de manière efficace et efficiente les efforts déployés par les États membres, les institutions de l'Union et les autres parties prenantes afin de garantir un cyberespace sûr dans l'Union européenne. Grâce au renforcement du cadre européen de certification de cybersécurité (ECCF), la proposition garantit que l'Union dispose d'un système de certification léger, moderne et adaptable qui servira les objectifs des actions relatives à la chaîne d'approvisionnement et favorisera la mise en œuvre rapide du règlement sur la cyberrésilience. En conclusion, le champ d'application proposé pour le mandat est délimité, en renforçant les domaines dans lesquels

85 Orientations politiques 2024.
86 Lettre de mission de la vice-présidente exécutive Henna Virkkunen.
87 Rapport de Sauli Niinistö
88 Rapport Draghi sur la compétitivité de l'UE
89 Enrico Letta - Much more than a market (avril 2024)

l'Agence a apporté une valeur ajoutée manifeste et en ajoutant les nouveaux domaines dans lesquels un soutien est nécessaire compte tenu des nouvelles priorités et des nouveaux instruments stratégiques et pour renforcer l'ECCF.

La révision du règlement sur la cybersécurité est donc conçue comme un changement radical majeur dans la posture de cybersécurité de l'Union et dans la sécurité, la préparation et la résilience globales de l'Union européenne.

1.5.2. Valeur ajoutée de l'intervention de l'UE (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins de la présente section, on entend par «valeur ajoutée de l'intervention de l'UE» la valeur découlant de l'intervention de l'UE qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

Le règlement sur la cybersécurité a été adopté en 2019 avec comme base juridique l'article 114 TFUE, qui habilite le législateur de l'Union à adopter des mesures d'harmonisation des dispositions législatives et réglementaires nationales qui ont pour objet l'établissement et le fonctionnement du marché intérieur.

La proposition révisée de règlement sur la cybersécurité vise à rationaliser la législation en matière de cybersécurité au niveau de l'Union, en complétant et en révisant l'actuel règlement sur la cybersécurité, en vigueur depuis 2019 (règlement sur la cybersécurité 1). Les objectifs du règlement sur la cybersécurité 1 consistant à conférer un mandat permanent à l'Agence de l'Union européenne pour la cybersécurité, afin de soutenir le niveau élevé commun de cybersécurité dans l'ensemble de l'Union ainsi qu'à éviter la fragmentation du marché intérieur en ce qui concerne les schémas de certification de cybersécurité, sont maintenus dans le cadre de la révision entreprise. Ces objectifs, tels qu'ils ont déjà été dûment analysés dans le cadre de la proposition de règlement sur la cybersécurité en 2017, ne peuvent pas être atteints de manière suffisante par les États membres, mais peuvent uniquement l'être au niveau de l'Union, conformément à l'article 5 du traité sur l'Union européenne.

La proposition de révision du règlement sur la cybersécurité met clairement l'accent sur la rationalisation, la hiérarchisation et la codification des tâches dans l'ensemble des actes législatifs en rapport avec le cyberespace, des objectifs qui ne pourraient être réalisés qu'au niveau de l'Union, et aucune initiative de ce type n'existe actuellement. La nouvelle proposition renforce encore la sécurité de la chaîne d'approvisionnement et le secteur de la cybersécurité au sein de l'Union et améliore la préparation et la résilience des États membres et de l'industrie. Les dépendances à l'égard d'entités établies dans des pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlées par des entités établies dans ces pays tiers (fournisseurs à haut risque) affectent des entités de toute l'Union, tandis que les incidents de cybersécurité importants dans la chaîne d'approvisionnement se propagent souvent au-delà des frontières nationales. Une action au seul niveau national ne sera probablement pas efficace.

Les nouvelles tâches confiées à l'ENISA revêtent une importance capitale pour atteindre des niveaux élevés de cybersécurité dans l'ensemble de l'Union. Bien que l'Agence travaille en coordination avec d'autres organismes de l'Union actifs dans le domaine de la sécurité, tels qu'Europol, ainsi que le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité (CECC),

qui est responsable de la mise en œuvre du financement, la mission et les tâches de l'Agence sont uniques et il n'existe actuellement aucun autre organe assumant ce type de responsabilités. Dans l'écosystème de la cybersécurité de l'Union, toutes les entités concernées travaillent dans le cadre de synergies étroites et de mandats clairs. Par conséquent, la proposition de règlement sur la cybersécurité 2 ne renforce que les parties présentant une valeur ajoutée manifeste, en veillant à ce qu'il n'y ait aucune ambiguïté en ce qui concerne la duplication des tâches, sur le fond mais aussi en ce qui concerne le financement avec d'autres organismes de l'écosystème de la cybersécurité.

Plus en détail

Le mandat actuel de l'ENISA a été élargi par des actes législatifs ultérieurs sans que ses responsabilités essentielles et ses ressources ne soient réexaminées en profondeur, ce qui a créé des chevauchements, des inefficacités et une priorisation insuffisante des principales tâches destinées à soutenir les États membres.

Plusieurs États membres ont mis en œuvre leurs propres schémas nationaux de certification de cybersécurité, dont le champ d'application et les procédures d'évaluation de la conformité diffèrent considérablement, ce qui crée une fragmentation du marché et des charges redondantes pour les opérateurs et les PME, qui souhaitent être certifiés une seule fois et exercer leurs activités dans l'ensemble de l'Union. L'ECCF a été créé dans le règlement sur la cybersécurité pour remédier à la fragmentation du marché, mais sa mise en œuvre a été lente et inégale.

De même, plusieurs actes juridiques horizontaux et sectoriels définissent des mesures de cybersécurité ayant des finalités et des objectifs différents, ce qui entraîne également des différences dans les méthodes de contrôle de la conformité et de surveillance définies par les États membres. En conséquence, les entités, en particulier les PME ou les entreprises opérant dans plusieurs États membres, sont confrontées à une charge supplémentaire en matière de conformité, ce qui nuit à leur compétitivité.

La diversité des approches en matière de sécurité de la chaîne d'approvisionnement des TIC et les différentes mesures prises par les États membres entraînent une fragmentation du marché et des exigences de conformité différentes pour les entités. En particulier, compte tenu de la nature transfrontière des chaînes d'approvisionnement des TIC, la fragmentation des exigences de conformité au sein du marché intérieur compromettrait la sécurité juridique pour les entités. Des cadres nationaux différents pour l'établissement de restrictions concernant les fournisseurs à haut risque pourraient créer des obstacles à la circulation transfrontalière des biens et des services au sein du marché intérieur. Enfin, étant donné que les chaînes d'approvisionnement des TIC peuvent impliquer des entités et des infrastructures critiques, quel que soit le lieu où ces fournisseurs sont établis, la fragmentation et les lacunes dans les mesures de cybersécurité engendrent des risques de sécurité supplémentaires pour ces entités.

En outre, les propositions de programmes du cadre financier pluriannuel (CFP) comprennent une disposition horizontale qui impose l'exclusion des fournisseurs à haut risque recensés en vertu du droit de l'Union, afin de protéger l'intégrité du budget de l'Union et de veiller à ce que les dépenses de l'Union ne soient pas contraires aux intérêts essentiels de l'Union en matière de sécurité. Le cadre établi dans le règlement sur la cybersécurité concernant les chaînes d'approvisionnement serait le mécanisme qui permettrait cette détection dans le domaine des chaînes

d'approvisionnement des TIC et il ne peut donc être mis en œuvre qu'au niveau de l'Union.

Par défaut, les cyberattaques sont de nature transfrontière, compte tenu notamment des effets d'entraînement qui pourraient survenir à partir d'un seul point d'entrée touché. Les menaces et les risques pour la cybersécurité ont une incidence sur l'ensemble de l'Union européenne et, par conséquent, disposer d'une conscience situationnelle collective pourrait améliorer considérablement les niveaux de cybersécurité des entités au sein de l'Union européenne. Les propositions formulées dans le cadre du mandat révisé de l'ENISA abordent cette question dans le but d'accroître considérablement la cyberrésilience de l'UE.

En conclusion, l'intervention de l'Union est essentielle étant donné que les menaces en matière de cybersécurité et les défis qui y sont liés s'étendent au-delà des différents États membres. Les solutions nationales fragmentées se sont révélées insuffisantes pour assurer la confiance et la coordination à l'échelle du marché. Un cadre juridique révisé de l'Union est nécessaire pour supprimer les obstacles, assurer une mise en œuvre cohérente et soutenir les États membres dans un environnement réglementaire et de menaces de plus en plus complexe.

1.5.3. Leçons tirées d'expériences similaires

L'ENISA a été créée en 2004 avec un mandat à durée déterminée. En 2019, le règlement sur la cybersécurité est entré en vigueur, dont les dispositions ont conféré à l'ENISA un mandat permanent et lui ont donné pour objectif de devenir le centre d'expertise en matière de cybersécurité en Europe. Aujourd'hui, l'ENISA est une marque reconnue et un partenaire de confiance parmi les parties prenantes de l'Union. Les compétences de l'Agence ont été progressivement construites sur une période de 25 ans, en reflétant l'évolution de l'écosystème de la cybersécurité.

Conformément à l'article 67 du règlement sur la cybersécurité, la Commission évalue tous les cinq ans l'incidence, l'efficacité et l'efficience de l'ENISA et de ses méthodes de travail, la nécessité éventuelle d'apporter des modifications et les conséquences financières de telles modifications. Cette évaluation porte également sur l'incidence, l'efficacité et l'efficience des dispositions relatives au cadre européen de certification.

Conformément à ces dispositions, la Commission a procédé à une évaluation de l'Agence et du cadre européen de certification de cybersécurité, qui comprenait une consultation publique et une étude indépendante. Conformément aux pratiques en matière d'amélioration de la réglementation, la Commission a également lancé une consultation publique portant spécifiquement sur la révision du règlement sur la cybersécurité, ainsi qu'un appel à contributions visant à recueillir des données auprès des groupes de parties prenantes. L'évaluation est parvenue à la conclusion que l'ENISA avait rempli son mandat en produisant la quasi-totalité des réalisations prévues. Les objectifs de l'Agence demeurent pertinents aujourd'hui et les parties prenantes reconnaissent particulièrement la valeur de ses réalisations lors des périodes difficiles telles que la pandémie de COVID-19 et la guerre d'agression menée par la Russie contre l'Ukraine. Malgré les retours d'information généralement positifs des parties prenantes quant aux réalisations de l'ENISA, il est également apparu qu'il existait une marge d'amélioration importante pour répondre de manière cohérente aux attentes des parties prenantes.

Les enseignements tirés ont montré que, pour accroître son niveau d'efficacité, l'ENISA aurait besoin d'une orientation plus stratégique, d'une hiérarchisation des tâches et d'un renforcement de sa capacité à fournir en temps utile des informations sur les menaces émergentes et des outils stratégiques pour y répondre. En outre, comme l'ont indiqué un certain nombre de parties prenantes, l'ENISA pourrait mettre en place des méthodes plus structurées et transparentes pour dialoguer avec les entités privées, en mettant l'accent sur le soutien aux PME. Lors de toutes les consultations externes, l'importance d'accroître le financement, les effectifs et les capacités opérationnelles de l'ENISA afin de lui permettre de répondre aux exigences croissantes du paysage de la cybersécurité de l'Union a été soulignée. Dans leur rapport d'évaluation, à la suite de l'étude, les services de la Commission ont conclu qu'il était manifestement nécessaire de disposer d'une législation à l'épreuve du temps, capable de s'adapter à la complexité et à l'évolution rapide de la situation en ce qui concerne les cybermenaces et, dans ce cadre, de renforcer l'Agence en lui fournissant les ressources nécessaires pour soutenir les niveaux les plus élevés de cybersécurité en Europe. Sur la base des données recueillies et de l'expérience tirée de la mise en œuvre du règlement sur la cybersécurité, il a été conclu que la coordination avec d'autres organismes devrait être rationalisée et qu'une attention particulière devrait être accordée au soutien que l'ENISA apporte à la mise en œuvre du droit de l'Union et au soutien qu'elle apporte à la Commission, à sa demande, pour l'élaboration de la législation relative à la cybersécurité. La proposition examine les synergies avec les priorités géopolitiques de la Commission afin de faire face à des risques tels que la dépendance croissante, en Europe, à l'égard d'entités établies dans des pays suscitant des préoccupations en matière de cybersécurité (fournisseurs à haut risque) ou contrôlées par de tels pays. En tant que centre d'expertise, l'ENISA joue actuellement aussi le rôle essentiel de répertoire d'informations, qui est capital pour parvenir à une compréhension commune des menaces et des risques qui pèsent sur les entités de l'Union. Par conséquent, le cadre proposé s'appuie sur l'expérience tirée du premier règlement sur la cybersécurité et mobilise la coordination des flux d'informations en vue de parvenir à une conscience situationnelle globale.

L'évaluation de l'ECCF fait apparaître plusieurs recommandations stratégiques. Malgré le rôle central de l'ENISA dans la promotion de la coopération et de la cohésion opérationnelle entre les États membres et les autres parties prenantes, les contraintes pesant sur l'efficience et l'efficacité de l'ECCF ont été évidentes, principalement en raison de la complexité des processus d'adoption des schémas. Ces problèmes ont mis en évidence la nécessité d'une révision substantielle des structures de gouvernance afin de renforcer la clarté opérationnelle et la responsabilité à tous les niveaux, ce que vise à faire la proposition de révision du règlement sur la cybersécurité. L'expérience du fonctionnement de l'ECCF actuel a prouvé la nécessité de moderniser et de clarifier le cadre de certification et d'introduire une procédure de maintenance des schémas de certification afin de leur permettre de s'adapter aux besoins du marché et au paysage des menaces. Enfin, le cadre initial n'a pas anticipé les risques non techniques, qui peuvent être considérés comme l'une des raisons du blocage de la mise en œuvre de l'ECCF en ce qui concerne les schémas relatifs à la 5G et à l'informatique en nuage.

La complexité de l'écosystème de la cybersécurité de l'Union a augmenté en même temps que les cybermenaces ont évolué. Dans les observations écrites des parties prenantes, un large consensus s'est dégagé quant à la nécessité de réduire la charge administrative, en particulier pour les PME, et les parties prenantes ont demandé une

simplification des procédures de mise en conformité. Si le principal effort de simplification passera par l'initiative «omnibus numérique», la proposition tient compte des besoins des parties prenantes en apportant des modifications à la directive SRI 2 afin de faciliter le processus de mise en œuvre.

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

Le règlement sur la cybersécurité 2 apporte les révisions nécessaires pour doter l'Union d'outils et de mécanismes permettant de réagir face à la situation en matière de cybersécurité et de répondre aux objectifs stratégiques. Le règlement proposé renforcera encore l'ENISA en la dotant des capacités nécessaires pour aider les États membres à mettre en œuvre le droit de l'Union et à lutter contre les cyberrisques. Compte tenu des rapports Draghi et Letta susmentionnés, la proposition de cadre financier pluriannuel (CFP) 2028-2034 place la compétitivité, la sécurité et l'autonomie stratégique au centre de ses préoccupations.

En conséquence, les propositions du train de mesures horizontales au titre du CFP 2028-2034, notamment les propositions relatives au Fonds européen pour la compétitivité et à Horizon Europe, introduisent de nouveaux critères d'éligibilité fondés sur le principe d'exclusion des «fournisseurs à haut risque» du bénéfice des fonds de l'Union. Le règlement sur la cybersécurité 2 est pleinement aligné sur ce principe et constitue en outre un outil permettant la mise en œuvre des nouvelles exigences relatives aux «fournisseurs à haut risque», en offrant un cadre procédural pour désigner les pays qui suscitent des préoccupations en matière de cybersécurité au niveau de l'Union. À cet égard, le règlement sur la cybersécurité 2 est une proposition stratégique, conforme aux priorités de la Commission pour parvenir à la souveraineté technologique et stimuler la compétitivité en Europe.

Il sera remédié à la fragmentation existante grâce à une harmonisation accrue sur le marché de la certification de l'Union, qui rendra le processus de certification européen plus efficace et plus durable.

Les propositions relatives au CFP pour la période 2028-2034 font de l'effort de simplification une priorité dans l'ensemble du cadre. Le nombre de lignes budgétaires est réduit à quatre au lieu de sept, tandis que le nombre de programmes de financement horizontaux a été abaissé de manière significative, passant de 52 à 16, ce qui offre de la souplesse et une capacité d'adaptation aux besoins existants. L'analyse d'impact de la révision du règlement sur la cybersécurité a précisément mis l'accent sur ces objectifs, à savoir la nécessité de simplifier les exigences en matière de cybersécurité dans plusieurs cadres législatifs et de codifier et de concentrer les tâches de l'ENISA sur les domaines qui permettront le mieux d'améliorer la résilience de l'écosystème de la cybersécurité de l'Union. À la suite de ces constatations, les dispositions proposées stimulent la compétitivité grâce à la simplification, garantissent des niveaux élevés de sécurité en renforçant la coordination et l'analyse des risques et des vulnérabilités et favorisent des niveaux d'harmonisation accrus en surmontant la fragmentation due au nombre de schémas nationaux. En outre, l'ENISA est conçue pour être le principal vecteur des efforts de simplification numérique, car elle comprendra le point d'entrée unique pour les notifications, comme indiqué dans l'initiative «omnibus numériques»[90].

[90] À ajouter après publication.

Un élément essentiel du train de mesures du CFP 2028-2034 est la proposition relative à un nouveau Fonds pour la compétitivité (FEC), qui regroupe plus de 16 programmes de financement tels que le programme pour une Europe numérique, le programme EU4Health, le Fonds européen de la défense, etc. Horizon Europe restera un programme autonome, étroitement lié au FEC. Ce nouveau cadre de programmation nécessite une coordination et un financement solides correspondant aux priorités actuelles. Dans cette optique, les dispositions proposées dans le règlement sur la cybersécurité 2 constituent le fondement de l'approfondissement de la coordination entre l'ENISA et le CECC, responsable de la mise en œuvre du programme des parties du programme pour une Europe numérique et d'Horizon Europe en rapport avec la cybersécurité. Les dispositions proposées garantissent la cohérence et mettent l'accent sur les synergies entre l'ENISA et le CECC. La même approche a été adoptée en ce qui concerne la coopération avec d'autres agences et organes, tels qu'Europol.

Un autre aspect de l'alignement entre la proposition de règlement sur la cybersécurité 2 et le CFP 2028-2034 réside dans le principe de flexibilité. Avec cette révision, la Commission propose un mécanisme de «redevances», qui offrira à l'ENISA un moyen souple de financer en partie ses activités, plus particulièrement en ce qui concerne le développement et la maintenance des programmes d'attestation européenne des compétences en matière de cybersécurité, le traitement et la délivrance d'agréments aux fournisseurs et la maintenance des schémas européens de certification de cybersécurité. Grâce à ce changement, l'Agence disposera de la flexibilité et de la modularité nécessaires pour répondre aux besoins des parties prenantes et assurer la durabilité de ses dépenses grâce au refinancement de ses services.

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

Depuis la dernière révision du mandat de l'ENISA en 2019, la tendance observée est une croissance exponentielle des contributions attendues de l'Agence au soutien à la mise en œuvre du droit de l'Union, menant à des demandes de budgets annuels et de renforcement des effectifs au-delà des niveaux initialement programmés. La révision proposée introduit de nouvelles tâches importantes et intègre des tâches relevant du mandat de l'ENISA qui ont été imposées par d'autres actes législatifs après l'adoption du règlement sur la cybersécurité 1, en élargissant ainsi les capacités de l'ENISA, ce qui nécessite des renforts financiers et humains supplémentaires. Animée par l'objectif de faire de la sécurité numérique un avantage concurrentiel de l'Europe, la proposition appelle à produire un impact concret au sein de l'écosystème de la cybersécurité, ce qui n'est pas possible en l'absence d'investissements importants correspondant à l'effet souhaité et, surtout, aux besoins des États membres et des autres parties prenantes. Les nouvelles tâches nécessitent du personnel technique et spécialisé, ainsi que des investissements financiers (par exemple, pour les outils et les plateformes), qui ne pourraient être assurés que par une dotation financière supplémentaire provenant du budget de l'Union.

Afin d'accroître la flexibilité tout en garantissant la pérennité du budget de l'Agence, la révision propose un mécanisme de redevances qui financera partiellement les services fournis pour la maintenance du cadre de certification de cybersécurité et en ce qui concerne l'élaboration et la maintenance des programmes d'attestation

individuelle européenne des compétences en matière de cybersécurité ainsi que le traitement et la délivrance d'agréments aux fournisseurs.

Toutes les estimations de ressources supplémentaires figurant dans la révision du règlement sur la cybersécurité sont effectuées en prenant pour point de départ le budget de base de l'ENISA en 2025 (coûts opérationnels et ETP). La Commission a procédé à une analyse approfondie des possibilités de redéploiement au sein de l'Agence afin de tenir compte des nouvelles tâches envisagées dans le mandat révisé. Le fait que l'Agence fonctionne à capacité maximale, sans aucune possibilité de réduction des tâches, et que le conseil d'administration ait déjà supprimé une priorité en 2023 amène de toute évidence à conclure qu'aucune nouvelle tâche ne peut être prise en charge dans le cadre de la structure actuelle sans un renforcement du budget et des ressources humaines. En outre, bon nombre des tâches actuelles sont couvertes par des conventions de contribution conclues entre l'ENISA et la Commission. La proposition vise par conséquent à ajouter ces tâches au mandat de l'ENISA et à obtenir un budget stable pour les années à venir.

Sans préjudice des négociations sur le prochain CFP, les crédits alloués à l'Agence à partir de 2028 seront compensés par des redéploiements de programmes au titre du CFP 2028-2034. Si une réduction compensatoire est nécessaire, les ressources allouées à l'Agence ainsi que leurs sources et flux de financement pourraient devoir être révisés. Les mesures mises en place dans le cadre du règlement sur la cybersécurité 2 proposé impliquent également la prise en charge de tâches supplémentaires pour la DG partenaire de l'ENISA (direction générale des réseaux de communication, du contenu et des technologies, ou DG CNECT). Il convient en particulier de noter que le cadre pour la chaîne d'approvisionnement des TIC sera entièrement mis en œuvre au niveau de la Commission, y compris l'analyse de marché accompagnant les évaluations des risques et la préparation des actes d'exécution. En outre, un ensemble supplémentaire d'actes d'exécution devront être élaborés et adoptés par la Commission en ce qui concerne les modalités des mécanismes de redevance. Une surveillance et une assistance supplémentaires au niveau de la Commission seront nécessaires pour l'application du cadre européen de certification de cybersécurité, l'élaboration de dispositions types, la maintenance des schémas de cybersécurité, les accords de reconnaissance mutuelle avec les pays tiers et la supervision de l'ENISA.

1.6. Durée de la proposition/de l'initiative et de son incidence financière

☐ **durée limitée**

– ☐ En vigueur à partir de/du [JJ/MM]AAAA jusqu'en/au [JJ/MM]AAAA

– ☐ Incidence financière de AAAA jusqu'en AAAA pour les crédits d'engagement et de AAAA jusqu'en AAAA pour les crédits de paiement.

☒ **durée illimitée**

– Mise en œuvre avec une période de montée en puissance de AAAA jusqu'en AAAA,

– puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) d'exécution budgétaire prévu(s)

☐ **Gestion directe** par la Commission

– ☐ dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives.

☐ **Gestion partagée** avec les États membres

☒ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

– ☐ à des pays tiers ou des organismes qu'ils ont désignés

– ☐ à des organisations internationales et à leurs agences (à préciser)

– ☐ à la Banque européenne d'investissement et au Fonds européen d'investissement

– ☒ aux organismes visés aux articles 70 et 71 du règlement financier

– ☐ à des établissements de droit public

– ☐ à des entités de droit privé investies d'une mission de service public, pour autant qu'elles soient dotées de garanties financières suffisantes

– ☐ à des entités de droit privé d'un État membre qui sont chargées de la mise en œuvre d'un partenariat public-privé et dotées de garanties financières suffisantes

– ☐ à des organismes ou des personnes chargés de l'exécution d'actions spécifiques relevant de la politique étrangère et de sécurité commune, en vertu du titre V du traité sur l'Union européenne, identifiés dans l'acte de base concerné

– ☐ à des entités établies dans un État membre, régies par le droit privé d'un État membre ou par le droit de l'Union et qui peuvent se voir confier, conformément à la réglementation sectorielle, l'exécution des fonds de l'Union ou des garanties budgétaires, dans la mesure où ces entités sont contrôlées par des établissements de droit public ou par des entités de droit privé investies d'une mission de service public et disposent des garanties financières appropriées sous la forme d'une responsabilité solidaire des entités de contrôle ou des garanties financières équivalentes et qui peuvent être, pour chaque action, limitées au montant maximal du soutien de l'Union.

Remarques

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Le contrôle et les rapports respecteront les principes énoncés dans l'actuel règlement sur la cybersécurité[91] et le règlement financier[92] et seront conformes à l'approche commune sur les agences décentralisées[93].

Conformément à l'article 40 du règlement financier, l'ENISA doit envoyer chaque année à la Commission, au Parlement européen et au Conseil un document unique de programmation incluant les programmes de travail annuel et pluriannuel ainsi que la programmation des ressources. En outre, la proposition de la Commission visant à modifier le mandat de l'ENISA introduit l'obligation pour la Commission, en tant que membre du conseil d'administration, d'exprimer un vote favorable à l'adoption par le conseil d'administration de l'ENISA du document unique de programmation pour les questions liées aux ressources humaines et au budget. La Commission émettra également un avis sur le projet de document unique de programmation avant la procédure de vote au sein du conseil d'administration; cet avis devrait être mis en œuvre avant l'adoption du document unique de programmation[94].

L'ENISA doit transmettre un rapport d'activité annuel consolidé au conseil d'administration. Ce rapport comprend notamment des informations sur la réalisation des objectifs et sur l'obtention des résultats énoncés dans le document unique de programmation. Le rapport doit également être envoyé à la Commission, au Parlement européen et au Conseil. Le directeur exécutif de l'ENISA devrait présenter tous les deux ans au conseil d'administration une évaluation ex post des activités de l'ENISA. L'Agence devrait également élaborer un plan d'action de suivi relatif aux conclusions des évaluations rétrospectives et présenter des rapports à la Commission deux fois par an sur les progrès accomplis. Le conseil d'administration devrait surveiller le suivi adéquat de ces conclusions.

Les cas présumés de mauvaise administration dans les activités de l'Agence peuvent faire l'objet d'enquêtes du Médiateur européen conformément aux dispositions de l'article 228 du traité.

Les principales sources de données pour le suivi prévu seraient l'ENISA, le Groupe européen de certification de cybersécurité, le groupe de coopération SRI, le réseau des CSIRT et les autorités des États membres. Outre les données issues des rapports (y compris les rapports d'activité annuels) de l'ENISA, des outils de collecte de données spécifiques du Groupe européen de certification de cybersécurité, du groupe de coopération SRI, du réseau des CSIRT et de la Commission seront utilisés en cas de besoin (par exemple, des enquêtes auprès des autorités nationales, des sondages Eurobaromètre, des études spécifiques ainsi que les rapports découlant des exercices paneuropéens).

La proposition de la Commission relative au règlement sur la cybersécurité 2 poursuit la pratique établie de l'Agence en matière d'examen et d'évaluation.

91 Le règlement de l'UE sur la cybersécurité EUR-Lex

92 Règlement financier relatif aux règles applicables au budget général de l'Union (refonte) - Office des publications de l'Union européenne

93 https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf

94 Règlement délégué – 2019/715 – FR – EUR-Lex.

Comme indiqué à l'article 119 de la proposition relative au règlement sur la cybersécurité 2, la Commission doit commander une évaluation de l'ENISA au plus tard le [JJ MM AAAA] et tous les cinq ans par la suite. Cette évaluation examinera, en particulier, la nécessité éventuelle de modifier le mandat de l'ENISA, ainsi que les conséquences financières d'une telle modification. Une évaluation sur deux donne lieu à une appréciation des résultats obtenus par l'ENISA, en tenant compte des objectifs, du mandat, de la mission, de la gouvernance et des tâches de celle-ci, y compris une appréciation de la question de savoir si le maintien de l'ENISA est toujours justifié au regard de ces objectifs, de ce mandat, de cette mission, de cette gouvernance et de ces tâches.

L'évaluation porte également sur les effets, l'efficacité et l'efficience des dispositions du titre III du règlement au regard des objectifs du cadre européen de certification de cybersécurité consistant à garantir un niveau adéquat de cybersécurité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés et des entités dans l'Union et à améliorer le fonctionnement du marché intérieur.

Cette évaluation porte également sur l'incidence, l'efficacité et l'efficience des dispositions du titre IV du règlement relatives aux objectifs du cadre de sécurité de la chaîne d'approvisionnement des TIC.

La Commission rend compte au Parlement européen et au Conseil de tous les résultats de l'évaluation et au conseil d'administration des résultats relatifs au titre II du règlement. Les résultats de l'évaluation sont rendus publics.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) d'exécution budgétaire, du (des) mécanisme(s) de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposée

La proposition ayant une incidence sur la contribution annuelle de l'UE à l'ENISA, le budget de l'UE sera mis en œuvre par gestion indirecte.

Dans le respect du principe de bonne gestion financière, le budget de l'ENISA est exécuté selon le principe d'un contrôle interne efficace et efficient. L'ENISA est donc tenue de mettre en œuvre une stratégie appropriée de contrôle, coordonnée entre les acteurs compétents de la chaîne de contrôle.

En ce qui concerne les contrôles ex post, l'ENISA, en tant qu'agence décentralisée, est notamment soumise aux contrôles suivants:

- audit interne du service d'audit interne de la Commission;
- rapports annuels de la Cour des comptes européenne, qui fournit une déclaration d'assurance concernant la fiabilité des comptes ainsi que la légalité et la régularité des opérations sous-jacentes;
- décharge annuelle par le Parlement européen;
- d'éventuelles enquêtes menées par l'OLAF, notamment pour s'assurer du bon usage des ressources allouées aux agences.
- En tant que DG partenaire de l'ENISA, la DG CNECT mettra en œuvre sa stratégie de contrôle des agences décentralisées pour veiller à des comptes rendus fiables dans le cadre de son rapport d'activité annuel (RAA). Si les agences décentralisées sont entièrement responsables de l'exécution de leur

budget, la DG CNECT est responsable du paiement régulier des contributions annuelles fixées par l'autorité budgétaire.

- Enfin, le Médiateur européen apporte un niveau supplémentaire de contrôle et de responsabilité à l'ENISA.

Sur la base de l'évaluation de l'Agence et de l'analyse d'impact qui a été réalisée en vue de la présentation de la proposition de règlement sur la cybersécurité 2, il a été jugé de la plus haute importance de garantir des ressources financières suffisantes pour que l'ENISA puisse s'acquitter des tâches qui lui sont confiées par le nouveau mandat. Une nouveauté importante pour le mandat révisé de l'Agence sera l'introduction d'un mécanisme de redevances envisagé pour financer les coûts de maintenance des schémas européens de certification de cybersécurité, adoptés dans le cadre de l'ECCF. L'ECCF révisé formalisera la procédure de maintenance. L'activité de maintenance sera dirigée par l'ENISA et partiellement financée par des redevances afin de tenir compte de son caractère modulable (la maintenance d'un plus grand nombre de schémas nécessitant davantage de personnel). L'Agence sera également dotée de la capacité de fournir des outils de tests pour faciliter la mise en œuvre des procédures d'évaluation de la conformité tant dans le cadre de l'ECCF que dans le cadre d'autres actes législatifs pertinents de l'Union en matière de cybersécurité. Les modalités relatives aux redevances seront fixées dans un acte d'exécution adopté par la Commission. La révision envisage par ailleurs l'élaboration et la maintenance de programmes d'attestation individuelle européenne et l'adoption de décisions autorisant les fournisseurs à délivrer des attestations individuelles européennes de compétences en matière de cybersécurité.

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

La proposition de règlement sur la cybersécurité 2 vise, en elle-même, à atténuer les risques recensés dans le cadre du mandat de l'ENISA et de l'ECCF, y compris au moyen de dispositions relatives au cadre de sécurité de la chaîne d'approvisionnement des TIC et à la simplification. Plus précisément, l'ENISA est une agence de l'Union européenne déjà existante et, dans le cadre de la révision, son mandat est délimité plus en détail, en renforçant les domaines dans lesquels l'Agence a apporté une valeur ajoutée manifeste et en ajoutant les nouveaux domaines dans lesquels un soutien est nécessaire compte tenu des nouvelles priorités et des nouveaux instruments stratégiques, tels que la simplification grâce à l'intégration d'un point d'entrée unique pour les notifications, la facilitation de l'établissement d'une conscience situationnelle commune à l'échelle de l'Union et d'une coopération opérationnelle et le renforcement et la rationalisation du cadre européen de certification de cybersécurité.

Un autre risque recensé, et abordé dans la proposition, est le nombre de conventions de contribution conclues par la Commission et l'Agence ces dernières années. En raison de la situation géopolitique actuelle et de l'évolution rapide du paysage des menaces de cybersécurité, la Commission a conclu des conventions de contribution avec l'Agence pour un montant total de plus de 75 millions d'euros depuis 2019. Étant donné que les tâches confiées à l'ENISA dans ces accords ont désormais un caractère permanent, l'instabilité des flux budgétaires passant par des conventions de contribution présente un risque pour les résultats à long terme des activités de l'ENISA.

Par conséquent, la présente proposition vise, entre autres, à renforcer les capacités en ressources de l'Agence, à redéfinir ses tâches et à réaliser des gains d'efficacité. En particulier, la possibilité de percevoir des redevances contribuera à long terme à un circuit financier durable de l'Agence grâce à un refinancement des coûts liés à la maintenance des schémas européens de certification, adoptés dans le cadre de l'ECCF, à l'expérimentation d'outils et à l'élaboration, à la maintenance et à la mise en œuvre de programmes d'attestation individuelle européenne des compétences en matière de cybersécurité. À long terme, elle devrait permettre de réaliser des économies pour le budget de l'Union qui atteindront 18,5 millions d'euros par an. La Commission dirigera les efforts de définition des modalités des redevances et de leur composition, en adoptant des actes d'exécution.

L'augmentation des tâches opérationnelles de l'Agence ne représente pas un risque réel. Ces tâches viendraient compléter l'action des États membres et soutenir ces derniers, à leur demande. Elles seront également limitées à des services prédéfinis, par analogie avec le règlement (UE) 2019/881 sur la cybersécurité[95]. Les nouveaux éléments/tâches figurant dans la proposition apporteront une valeur ajoutée aux parties prenantes européennes, qui profiteront du rôle joué par l'ENISA en tant que pôle d'information contribuant au partage d'informations et fournissant des notifications d'alerte à leurs membres.

En outre, le modèle proposé pour l'Agence est aligné sur l'approche commune de la Commission à l'égard des agences décentralisées, ce qui garantit un contrôle suffisant pour s'assurer que l'ENISA œuvre à la réalisation de ses objectifs. Les risques opérationnels et financiers des modifications proposées semblent limités, étant donné que les dispositions sont élaborées de manière à atténuer les risques actuels. Néanmoins, certains aspects négatifs pourraient être attendus à long terme, sous la forme:

– d'une limitation des ressources opérationnelles due aux besoins opérationnels croissants des États membres et à l'évolution constante des cyberrisques et des cybermenaces dans le domaine de la cybersécurité;

– d'une augmentation rapide du budget, avec des attentes quant à une mise en œuvre rapide.

- insuffisance des ressources humaines et financières par rapport aux besoins opérationnels.

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport entre les coûts du contrôle et la valeur des fonds gérés concernés), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

Le coût supporté par la DG CNECT pour le contrôle et la supervision des entités chargées de l'exécution, y compris l'ENISA, s'élève à environ 5,25 millions d'euros, comme indiqué dans le rapport annuel d'activité pour 2024[96]. Ce montant comprend principalement les coûts de personnel et représente 0,50 % des paiements opérationnels effectués en faveur de ces entités au cours de l'année 2024. Le taux

95 https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

96 CNECT_AAR_2024_final

global du coût des contrôles a légèrement augmenté, passant de 0,50 % en 2024 à 0,46 % en 2023, mais reste relativement stable par rapport aux années précédentes.

Plus précisément, en ce qui concerne l'ENISA, les coûts des contrôles en 2024 s'élèvent à 0,32 million d'euros, soit 0,70 % des coûts des contrôles en 2024, contre 0,69 % en 2023 et 1,22 % en 2022. L'analyse montre que l'augmentation des coûts des contrôles est principalement liée à la préparation et au suivi des conventions de contribution entre la Commission et l'Agence (principalement des coûts de ressources humaines); étant donné que ces coûts devraient être considérablement réduits pendant le nouveau mandat, on s'attend à ce que les niveaux de gains d'efficacité soient plus élevés. En ce qui concerne les coûts globaux supportés par la DG CNECT par rapport aux autres entités chargées de l'exécution, l'ENISA se situe dans la moyenne, par rapport à 11 autres entités.

La proposition de règlement sur la cybersécurité 2 prévoit d'augmenter le personnel de la DG CNECT de 50 ETP, dont un ETP supplémentaire sera spécifiquement affecté aux tâches liées au rôle de la DG CNECT en tant que DG partenaire de l'Agence. Cette personne soutiendra l'élaboration de l'avis de la Commission sur le document unique de programmation de l'ENISA et surveillera la mise en œuvre de ce dernier, aidera à superviser la préparation du budget de l'Agence et à assurer le suivi de son exécution et aidera l'Agence à développer ses activités conformément aux politiques de l'Union, y compris en participant aux réunions pertinentes. Cette action est justifiée par l'augmentation des tâches de surveillances confiées à la DG CNECT, parmi lesquelles figure l'expression d'un vote favorable de la Commission sur les questions ayant trait au budget et aux ressources humaines. Il convient d'observer que la mise en œuvre des dispositions relatives à la désignation des pays présentant des risques stratégiques en matière de cybersécurité pour des actifs essentiels spécifiques (fournisseurs à haut risque) sera un processus entièrement piloté par la Commission. Le personnel nécessaire aux évaluations des risques effectuées dans le cadre des activités susmentionnées est estimé à 25 ETP. L'action est justifiée par le volume de travail que requiert la mise en œuvre du cadre stratégique, en particulier le soutien des évaluations coordonnées des risques de l'Union, l'analyse économique réalisée pour chaque produit/service TIC, la préparation des actes d'exécution respectifs et le suivi de la mise en œuvre du cadre et la réalisation des évaluations de la propriété et du contrôle. Le coût pour la Commission des contrôles relatifs à la mise en œuvre du cadre pour le fonctionnement de la chaîne d'approvisionnement devrait être spécifiquement influencé par le nombre d'évaluations du contrôle de la propriété (ECP) que la Commission réalisera. Les résultats de cette tâche contribueront toutefois grandement à permettre aux États membres de réaliser des économies lorsqu'ils superviseront la mise en œuvre des mesures et obligations d'atténuation imposées par le cadre aux entités relevant de la directive SRI 2. Les États membres seront en mesure de tirer directement parti des résultats des ECP, plutôt que de dépenser chacun individuellement des ressources pour répondre aux mêmes besoins d'évaluation. Le renforcement du cadre européen de certification de cybersécurité, la normalisation et la mise en œuvre des activités connexes, la mise en œuvre de la directive SRI 2 (y compris les besoins de mise en œuvre connexes, les actes d'exécution relatifs aux redevances et le soutien à la maintenance des schémas de certification et des programmes d'attestation des compétences) devrait nécessiter 19 ETP, tandis que les politiques de coopération opérationnelle et de conscience situationnelle nécessitent cinq ETP supplémentaires. La description complète des tâches se trouve à la section 3.2.4.

Dans son rapport annuel d'activité consolidé 2023[97], l'ENISA a formulé une conclusion positive concernant l'évaluation de ses systèmes de contrôle interne et a fourni une déclaration d'assurance vierge. Dans son rapport annuel sur les agences de l'UE relatif à l'exercice 2023, la Cour des comptes a émis une opinion d'audit favorable sur les comptes et une opinion avec réserve sur la légalité et la régularité des paiements sous-jacents aux comptes (également mentionnée au point 2.2.2). La DG CNECT a pris note de ce rapport, mais a conclu qu'il n'avait pas d'incidence sur l'efficacité de sa supervision. L'ENISA rend également régulièrement compte des mesures prises pour éviter de nouvelles constatations et, pour l'instant, rien n'indique que le taux d'erreur s'aggravera/dépassera les 2 % dans les années à venir.

Par ailleurs, l'article 80, paragraphe 2, du règlement financier de l'ENISA[98] prévoit la possibilité pour l'Agence de partager une structure d'audit interne avec d'autres organismes de l'Union œuvrant dans le même domaine d'activité si la structure d'audit interne d'un organisme de l'Union ne présente pas un bon rapport coût/efficacité.

En conclusion, étant donné qu'il est proposé d'augmenter la taille de l'Agence de plus de 100 % alors que l'augmentation des coûts des contrôles a été relativement faible, l'analyse montre un rapport coût-efficacité satisfaisant. Compte tenu de toutes les données disponibles, rien n'indique que le taux d'erreur escompté pourrait être supérieur à 2 %.

2.3. Mesures de prévention des fraudes et irrégularités

L'Agence de l'Union européenne pour la cybersécurité appliquera les normes les plus élevées applicables à la prévention de la fraude et des irrégularités.

Le contrôle du paiement de tout service ou étude nécessaire est effectué par le personnel de l'Agence avant le paiement, compte tenu de toute obligation contractuelle, des principes économiques et des bonnes pratiques financières ou de gestion. Des dispositions antifraude (surveillance, exigences en matière de rapports) seront introduites dans tous les accords et contrats conclus entre l'Agence et les bénéficiaires de tous paiements.

Aux fins de la lutte contre la fraude, la corruption et toute autre activité illégale, les dispositions du règlement (UE, Euratom) no 883/2013 du Parlement européen et du Conseil s'appliquent sans restriction.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

- Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre	Ligne budgétaire	Nature de la dépense	Participation

97 enisa.europa.eu/sites/default/files/2024-11/2023 Consolidated Annual Activity Report_1.pdf.

98 MB Decision 2019_8 Financial rules_adopted.pdf

financier pluriannuel	Numéro	CD/CND[99].	de pays AELE[100]	de pays candidats et pays candidats potentiels [101]	d'autres pays tiers	autres recettes affectées
	[XX.YY.YY.YY]	CND	OUI	NON	NON	OUI/NON
	[XX.YY.YY.YY]	CD/CND	OUI/NON	OUI/NON	OUI/NON	OUI/NON
	[XX.YY.YY.YY]	CD/CND	OUI/NON	OUI/NON	OUI/NON	OUI/NON

- Nouvelles lignes budgétaires, dont la création est demandée

<u>Dans l'ordre</u> des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro	CD/CND	de pays AELE	de pays candidats et pays candidats potentiels	d'autres pays tiers	autres recettes affectées
	[XX.YY.YY.YY]	CD/CND	OUI/NON	OUI/NON	OUI/NON	OUI/NON
	[XX.YY.YY.YY]	CD/CND	OUI/NON	OUI/NON	OUI/NON	OUI/NON
	[XX.YY.YY.YY]	CD/CND	OUI/NON	OUI/NON	OUI/NON	OUI/NON

99 CD = crédits dissociés / CND = crédits non dissociés.

100 AELE: Association européenne de libre-échange.

101 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☒ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

3.2.1.1. Crédits issus du budget voté

En Mio EUR (à la 3e décimale)

Agence: ENISA	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**	**TOTAL CFP 2028-2034**
Ligne budgétaire: <…….> / Contribution supplémentaire du budget de l'UE à l'Agence	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006

Les crédits/la contribution du budget de l'UE à l'agence seront compensés par une réduction de l'enveloppe du programme suivant <….> / ligne budgétaire: <….> / durant l'année/les années: <…….> .

			Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**	**TOTAL CFP 2028-2034**	
TOTAL des crédits opérationnels	Engagements	(4)	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006	
	Paiements	(5)	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006	
TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		(6)	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**	
TOTAL des crédits pour la	Engagements		=4+6	22,265	21,959	26,808	28,586	28,901	28,716	28,926	186,161

RUBRIQUE 2										
du cadre financier pluriannuel	Paiements	=5+6	22,265	20,890	24,851	26,254	26,254	25,754	25,754	186,161

DG: CNECT	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**	**TOTAL CFP 2028-2034**
• Ressources humaines	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**
• Autres dépenses administratives	0	0	0	0	0	0	0	**0**

TOTAL pour la DG CNECT	Crédits	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**		**37,375**

TOTAL des crédits pour la RUBRIQUE 4 du cadre financier pluriannuel	(Total engagements = Total paiements)	**2,328**	**2,328**	**3,104**	**3,492**	**3,880**	**4,268**	**4,850**	**24,25**

En Mio EUR (à la 3e décimale)

		Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**	**TOTAL CFP 2028-2034**
TOTAL des crédits pour les	Engagements	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38

RUBRIQUES 1 à 4										
du cadre financier pluriannuel	Paiements	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38

3.2.2. Estimation des réalisations financées à partir des crédits opérationnels (cette section ne doit pas être complétée pour les organismes décentralisés)

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations ⇩			Année **2028**		Année **2029**		Année **2030**		Année **2031**		Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. section 1.6)						**TOTAL**	
	RÉALISATIONS (outputs)																	
	Type [102]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[103]...																		
- Réalisation																		
- Réalisation																		
- Réalisation																		
Sous-total objectif spécifique nº 1																		
OBJECTIF SPÉCIFIQUE nº 2…																		
- Réalisation																		

[102] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[103] Tel que décrit dans la section 1.3.2. «Objectif(s) spécifique(s)».

Sous-total objectif spécifique nº 2																
TOTAUX																

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☒ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

3.2.3,1. Crédits issus du budget voté

(supplémentaires)

CRÉDITS VOTÉS	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**	**TOTAL 2028-2034**
RUBRIQUE 4								
Ressources humaines	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Autres dépenses administratives	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Sous-total RUBRIQUE 4	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Hors RUBRIQUE 4								
Ressources humaines	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**
Autres dépenses de nature administrative	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Sous-total hors RUBRIQUE 4	**1,365**	**1,365**	**1,470**	**1,785**	**2,100**	**2,415**	**2,625**	**13,125**
TOTAL	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**

3.2.4. Estimation des besoins en ressources humaines (supplémentaires)

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– ☒ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

3.2.4,1. Financement sur le budget voté

Estimation à exprimer en équivalents temps plein (ETP)[104]

CRÉDITS VOTÉS	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**
• Emplois du tableau des effectifs (fonctionnaires et agents temporaires)							
20 01 02 01 (Au siège et dans les bureaux de représentation de la Commission)	12	12	16	18	20	22	25
20 01 02 03 (Délégations de l'UE)	0	0	0	0	0	0	0
(Recherche indirecte)	0	0	0	0	0	0	0
(Recherche directe)	0	0	0	0	0	0	0
Autres lignes budgétaires (à préciser)	0	0	0	0	0	0	0
• Personnel externe (en ETP)							

104 Veuillez préciser en dessous du tableau combien, sur le nombre d'ETP indiqué, sont déjà affectés à la gestion de l'action et/ou peuvent être redéployés au sein de votre DG, et quels sont vos besoins nets.

20 02 01 (AC, END de l'«enveloppe globale»)		0	0	0	0	0	0	0
20 02 03 (AC, AL, END et JPD dans les délégations de l'UE)		0	0	0	0	0	0	0
Ligne d'appui administratif	- au siège	0	0	0	0	0	0	0
[XX.01.YY.YY]	- dans les délégations de l'UE	0	0	0	0	0	0	0
(AC, END - Recherche indirecte)		0	0	0	0	0	0	0
(AC, END - Recherche directe)		0	0	0	0	0	0	0
Autres lignes budgétaires (à préciser) - Rubrique 4		0	0	0	0	0	0	0
Autres lignes budgétaires (à préciser) - Hors rubrique 4		13	13	14	17	20	23	25
TOTAL		**25**	**25**	**30**	**35**	**40**	**45**	**50**

Personnel nécessaire à la mise en œuvre de la proposition (en ETP):

	À couvrir par le personnel actuellement disponible dans les services de la Commission	**Personnel supplémentaire exceptionnel**		
		À financer sur la rubrique 7 ou la recherche	**À financer sur la ligne BA**	**À financer sur les redevances**
Emplois du tableau des effectifs		25		
Personnel externe (AC, END, INT)			25	

L'incidence estimée sur les dépenses et les effectifs pour 2028 et au-delà est indicative et ne préjuge pas du prochain cadre financier pluriannuel. La source de financement et la portée de l'engagement financier de l'Union pour la période postérieure à 2027 restent tributaires du résultat des négociations interinstitutionnelles sur le CFP 2028-2034, de la procédure budgétaire annuelle et du mécanisme d'orientation.

Description des tâches à exécuter par la DG compétente pour le secteur au sein de la Commission

les fonctionnaires et agents temporaires	**Coordination de l'ENISA (1)**: Représenter la Commission au conseil d'administration de l'Agence. Rédiger l'avis de la Commission sur le document unique de programmation de l'ENISA et surveiller la mise en œuvre de ce dernier. Superviser la préparation du budget de l'Agence et assurer le suivi de son exécution. Aider l'Agence à développer ses activités conformément aux politiques de l'Union, y compris en participant aux réunions pertinentes. **Programme d'attestation des compétences/Académie des compétences (2):** Des effectifs supplémentaires seront nécessaires au sein de la CNECT pour préparer les actes d'exécution établissant les redevances que l'ENISA percevra auprès des personnes demandant à devenir des fournisseurs agréés. Ces actes d'exécution seront au moins au nombre de 12, un par profil de l'ECSF. **Chaîne d'approvisionnement** (25) Aide à la préparation des évaluations coordonnées des risques de l'Union. Réalisation d'une analyse économique pour chacun des produits et services TIC considérés. Élaboration des actes d'exécution pertinents relatifs à l'identification des actifs essentiels, aux mesures d'atténuation proposées et à la désignation des pays présentant des risques stratégiques en matière de cybersécurité pour des actifs essentiels spécifiques, identification des fournisseurs à haut risque, vérification des demandes d'exemption et préparation des décisions de la Commission. Soutien de la mise en œuvre et de la supervision des mesures adoptées. **Cadre européen de certification de cybersécurité, normalisation et mise en œuvre des activités connexes, mise en œuvre de la directive SRI 2 (17):** Application du règlement sur la cybersécurité, en particulier la gouvernance des organismes d'évaluation de la conformité (défi des responsabilités) Participation (et assemblée) des parties prenantes Reconnaissance mutuelle avec des pays tiers Normalisation de l'élaboration des actes d'exécution (demandes détaillées soumises à consultations et élaboration de dispositions types) Maintenance des schémas, examen juridique, procédure de comitologie Coordination avec le groupe de coordination SRI et maintenance des schémas des entités Actes d'exécution au titre de la directive SRI 2 Alignement des organismes d'évaluation de la conformité sur le règlement sur la cybersécurité, présomption de conformité + normalisation Coordination entre les autorités de surveillance du marché et l'ANCC Alignement technique entre le règlement sur la cyberrésilience et les schémas de certification **Coordination opérationnelle et conscience situationnelle (5)**: Expertise d'acteurs du secteur et de la menace afin de contribuer à la conscience situationnelle au niveau de l'Union en ce qui concerne les menaces pesant sur les infrastructures critiques, y compris au moyen de technologies émergentes Coordination avec l'ENISA et d'autres entités et réseaux de l'UE afin de se préparer aux incidents de cybersécurité importants et majeurs

le personnel externe	Comme ci-dessus

Description des tâches supplémentaires à effectuer par l'ENISA:

les fonctionnaires et agents temporaires	Gestion de la réserve de cybersécurité de l'Union (gestionnaires nationaux et soutien à la mise en œuvre, tandis que les coûts opérationnels réels de la réserve sont couverts comme prévu dans le règlement sur la cybersolidarité) (10) Gestion de la plateforme unique de signalement au titre du règlement sur la cyberrésilience (fonctionnement) (9) Services de traitement des vulnérabilités liés à la plateforme unique de signalement (4) Extension de la plateforme unique de signalement au point d'entrée unique (développement & exploitation) (8) Élaboration d'orientations techniques, d'une expertise en matière de sécurité des produits et d'une analyse de marché pour faciliter la mise en œuvre du règlement sur la cyberrésilience (7) Normalisation destinée à faciliter la mise en œuvre du règlement sur la cyberrésilience/certification/SRI 2 (4) Soutien des activités de surveillance du marché au titre du règlement sur la cyberrésilience (4) Soutien des tests de conformité et des évaluations de la sécurité des produits (4) Soutien des États membres dans le cadre de l'assistance mutuelle (3) Fourniture de services de gestion des vulnérabilités, maintenance de la base de données européenne des vulnérabilités et fourniture de fonctions de conseil et d'enrichissement (divulgation coordonnée des vulnérabilités) (15) Coopération opérationnelle et conscience situationnelle –plateformes d'atténuation et de soutien telles que le réseau des CSIRT/CyCLONe; soutien des tâches liées aux notifications d'alertes; soutien du renforcement de la coordination avec d'autres entités concernées afin de mettre au point des répertoires de renseignements vérifiés et fiables sur les cybermenaces [article 11, paragraphe 1 *bis*, du règlement sur la cybersécurité 2] (5) Soutien à la résilience des secteurs critiques (y compris la mise en œuvre du plan d'action sur la cybersécurité dans le domaine des soins de santé) (4) Élaboration de schémas d'attestation de compétences (2) Maintenance et supervision des schémas d'attestation de compétences (6) Tâches administratives (Comptable pour les redevances/RH/informatique) (8) Maintenance des schémas de certification (11) Tâches horizontales – Implication accrue des parties prenantes, rédaction de spécifications techniques et participation aux activités de normalisation à l'appui des schémas (1)
le personnel externe	Comme ci-dessus Deux END obligatoires par État membre afin de soutenir les activités de l'Agence et de servir d'agents de liaison nationaux, en mettant l'accent sur la coopération opérationnelle et la divulgation coordonnée des vulnérabilités. (13) Les 27 autres END sont considérés comme gratuits et n'ont donc aucune incidence budgétaire.

Coûts opérationnels supplémentaires par an pour l'ENISA sur la période 2028-2034:

Coût	Budget	Calendrier	Explication
Site web consacré aux compétences en matière de cybersécurité	750 000 EUR	50 % en 2029 50 % en 2030	Afin de garantir la transparence des procédures, la proposition impose à l'ENISA de tenir à jour un site web contenant les profils de l'ECSF, les programmes d'attestation, des informations sur les redevances pour chaque programme, les redevances recommandées pour chaque attestation et la liste des fournisseurs d'attestation agréés.
Divulgation coordonnée des vulnérabilités	1 million d'EUR	À partir de 2028	La sécurité des produits et services utilisés dans nos infrastructures critiques dépend dans une grande mesure du partage en temps utile d'informations sur les vulnérabilités découvertes et sur les moyens de les atténuer.

Renseignements sur les menaces de cybersécurité	3 millions d'EUR	À partir de 2028	Pour la mise en place d'une conscience situationnelle effectuée en coopération entre l'ENISA et la Commission.
Guichet unique	8 millions d'EUR	6 millions d'EUR pour l'année 2028 500 000 EUR en 2029 500 000 EUR en 2030 500 000 EUR en 2031 500 000 EUR en 2032	Être en mesure de mettre en œuvre la proposition «omnibus numérique» de la Commission visant à simplifier le respect des obligations en matière de signalement des incidents de cybersécurité et des violations de données en développant et en maintenant un point d'entrée unique.
Maintenance de la plateforme unique de signalement au titre du règlement sur la cyberrésilience et autres	3 millions d'EUR	À partir de 2028	La plateforme unique de signalement introduite par les colégislateurs est le plus grand système informatique jamais développé dans l'histoire de l'ENISA et un pilier essentiel du règlement sur la cyberrésilience.

			Sa création est actuellement financée au moyen d'une convention de contribution, mais sa gestion quotidienne nécessitera des ETP (voir ci-dessus) ainsi que des coûts opérationnels. L'ENISA a un rôle essentiel à jouer pour garantir le succès du cadre de l'Union applicable à la sécurité des produits, à savoir le règlement sur la cyberrésilience.
Communication sécurisée et maturité de la cybersécurité de l'ENISA	2 millions d'EUR +	1,1 million d'EUR d'investissements en 2028 (plateformes CyCLONe/CSIRT + secrétariats et communication) 1 million d'EUR par an pour la maintenance à partir de 2029 1,5 million d'EUR pour la cybermaturité	Garantir la cybersécurité de l'Agence et des outils de communication.
Maintenance de la certification de cybersécurité	1 400 000 EUR	2028 600 000 2029 1 000 000 2030 1 200 000 2031 1 400 00 2032 1 400 000	Couverts par des redevances (intégralement à partir de 2032)

		2033 1 400 000 2034 1 400 000	
Programmes d'attestation de cybersécurité	212 920 EUR	50 % couverts par le budget de l'Union en 2030	Entièrement couverts par les redevances à partir de 2033

3.2.5. Vue d'ensemble de l'incidence estimée sur les investissements liés aux technologies numériques

Obligatoire: il convient d'indiquer dans le tableau figurant ci-dessous la meilleure estimation des investissements liés aux technologies numériques découlant de la proposition/de l'initiative.

À titre exceptionnel, lorsque la mise en œuvre de la proposition/de l'initiative l'exige, les crédits de la rubrique 4 doivent être présentés sur la ligne spécifique.

Les crédits des rubriques 1-3 doivent être présentés comme des «Dépenses pour les systèmes informatiques soutenant une politique consacrées aux programmes opérationnels». Ces dépenses correspondent au budget opérationnel à affecter à la réutilisation/à l'achat/au développement de plateformes et d'outils informatiques directement liés à la mise en œuvre de l'initiative et aux investissements qui y sont associés (par exemple, licences, études, stockage de données, etc.). Les informations figurant dans ce tableau doivent être cohérentes avec les données détaillées présentées à la section 4 «Dimensions numériques».

TOTAL des crédits numériques et informatiques	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**	**TOTAL CFP 2028-2034**
RUBRIQUE 4								
Dépenses informatiques (institutionnelles)	0	0	0	0	0	0	0	**0**
Sous-total RUBRIQUE 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Hors RUBRIQUE 4								
Dépenses pour les systèmes informatiques soutenant une politique consacrées aux programmes opérationnels	0	0	0	0	0	0	0	**0**
Sous-total hors RUBRIQUE 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

TOTAL	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6. Compatibilité avec le cadre financier pluriannuel actuel

La proposition/l'initiative:

– ☒ peut être intégralement financée par voie de redéploiement au sein de la rubrique concernée du cadre financier pluriannuel (CFP).

Sans préjudice des négociations sur le prochain CFP, les crédits alloués à l'Agence à partir de 2028 seront compensés par des redéploiements de programmes au titre du CFP 2028-2034. Si une réduction compensatoire est nécessaire, les ressources allouées à l'Agence ainsi que leurs sources et flux de financement pourraient devoir être révisés.

– ☐ nécessite l'utilisation de la marge non allouée sous la rubrique correspondante du CFP et/ou le recours aux instruments spéciaux comme le prévoit le règlement CFP.

– ☐ nécessite une révision du CFP.

3.2.7. Participation de tiers au financement

La proposition/l'initiative:

– ☒ ne prévoit pas de cofinancement par des tierces parties

– ☐ prévoit le cofinancement par des tierces parties estimé ci-après:

Crédits en Mio EUR (à la 3e décimale)

	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Total
Préciser l'organisme de cofinancement					
TOTAL crédits cofinancés					

3.2.8. Estimation des ressources humaines et utilisation des crédits nécessaires dans un organisme décentralisé

Besoins en personnel supplémentaire (en équivalents temps plein)

Agence: ENISA	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**
Agents temporaires (Grades AD)	5	11	17	19	19	19	19
Agents temporaires (Grades AST)	4	7	11	12	12	12	12
Sous-total des agents temporaires (AD+AST)	***9***	***18***	***28***	***31***	***31***	***31***	***31***
Agents contractuels	22	44	66	74	74	74	74
Experts nationaux détachés	4	8	11	13	13	13	13

Sous-total des agents contractuels et experts nationaux détachés	26	52	77	87	87	87	87
TOTAL des effectifs	35	70	105	118	118	118	118

Crédits couverts par la contribution du budget de l'UE en Mio EUR (à la 3e décimale)

Agence: ENISA	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**	**TOTAL 2028 – 2034**
Titre 1: Dépenses de personnel	4,488	8,466	12,507	13,648	10,584	10,012	9,537	**87,766**
Titre 2: Dépenses d'infrastructure et de fonctionnement								
Titre 3: Dépenses opérationnelles	16,413	11,588	11,528	11,788	11,613	11,613	11,113	**85,240**
TOTAL des crédits couverts par le budget de l'UE	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**

Crédits couverts par des redevances, le cas échéant, en Mio EUR (à la 3e décimale)

Agence: ENISA	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**	**TOTAL 2028 – 2034**
Titre 1: Dépenses de personnel		0,510	1,043	1,539	4,604	5,176	5,650	**18,522**
Titre 2: Dépenses d'infrastructure et de fonctionnement								**0,000**
Titre 3: Dépenses opérationnelles								**0,000**
TOTAL des crédits couverts par des redevances	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**

Vue d'ensemble/synthèse des ressources humaines et des crédits (en Mio EUR) nécessaires à la proposition/l'initiative dans un organisme décentralisé

Agence: ENISA	Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**	**TOTAL 2028 – 2034**
Agents temporaires (AD+AST)	9	18	28	31	31	31	31	*31*
Agents contractuels	22	44	66	74	74	74	74	74

Experts nationaux détachés	4	8	11	13	13	13	13	13
Total des effectifs	35	70	105	118	118	118	118	**118**
Crédits couverts par le budget de l'UE	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**
Crédits couverts par des redevances (le cas échéant)	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**
Crédits cofinancés (le cas échéant)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
TOTAL des crédits	**20,901**	**20,564**	**25,078**	**26,976**	**26,801**	**26,801**	**26,801**	**173,922**

3.3. Incidence estimée sur les recettes

– ☒ La proposition/l'initiative est sans incidence financière sur les recettes.

– ☐ La proposition/l'initiative a une incidence financière décrite ci-après:

– ☐ sur les ressources propres

– ☐ sur les autres recettes

– ☐ veuillez indiquer si les recettes sont affectées à des lignes de dépenses

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[105]						
		Année **2028**	Année **2029**	Année **2030**	Année **2031**	Année **2032**	Année **2033**	Année **2034**
Article …….								

Pour les recettes affectées, préciser la(les) ligne(s) budgétaire(s) de dépenses concernée(s).

Autres remarques (relatives par exemple à la méthode/formule utilisée pour le calcul de l'incidence sur les recettes ou toute autre information).

Les mécanismes de redevances sont liés à trois domaines d'activité de l'ENISA:

- Redevances liées à l'agrément de fournisseurs dans le cadre des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité.

105 En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.

Les redevances liées à cette activité seront fixées dans un acte d'exécution, à la suite de l'adoption du règlement révisé sur la cybersécurité. Toutefois, pour pouvoir estimer les investissements nécessaires et les coûts, les calculs ont été effectués à l'aide d'un modèle existant dans un État membre de l'Union[106]. Ce modèle comprend un paiement unique et une redevance annuelle.

Coûts fixes: 8 540 EUR

Redevance annuelle: 800 EUR

Les redevances sont destinées à refinancer les coûts de cette activité spécifique. Les coûts ont été estimés à 1 064 600 EUR sur une période de cinq ans. Les coûts spécifiques des activités incluses dans ce chiffres sont liés à l'élaboration et à la maintenance des schémas, y compris les dépenses des membres d'un groupe de travail ad hoc qui aiderait l'ENISA à élaborer les schémas (remboursement des dépenses et rémunération des rapporteurs), les missions d'audit des fournisseurs sur place et la formation des évaluateurs afin de garantir une application homogène des schémas:

A) le coût du groupe de travail ad hoc s'élèverait à 800 000 EUR.

B) la formation de deux évaluateurs par État membre coûterait 129 600 EUR.

C) l'audit d'une entité par État membre coûterait 135 000 EUR.

(A + B + C)/5 = 212 920 EUR de coûts par an.

La proposition prévoyait une période de transition et un investissement initial pendant les trois premières années. Pendant la période de transition, les coûts seront couverts par le budget de l'Union; pendant les quatrième et cinquième années, la couverture sera de 50 %, et pendant les sixième et septième années, les redevances seront intégralement appliquées.

Année	Redevances
2028	0
2029	0
2030	0
2031	106 460 (recettes)
2032	106 460 (recettes)
2033	212 920 (recettes)
2034	212 920 (recettes)

- Redevances destinées à couvrir les coûts de maintenance d'un schéma de certification de cybersécurité, adopté dans le cadre européen de certification de cybersécurité (ECCF).

Les redevances liées à cette activité seront fixées dans un acte d'exécution, à la suite de l'adoption du règlement révisé sur la cybersécurité. Les estimations des coûts de maintenance d'un schéma sont fondées sur une analyse de marché,

106 Décision RR-02: Barème des services de SNAS : https://www.snas.sk/storage/app/uploads/public/677/e79/e4c/677e79e4cac62903312474.pdf,

incluse dans l'analyse d'impact de la proposition de révision du règlement sur la cybersécurité. Le coût total de l'activité sur une période de cinq ans est estimé à 5 600 000 EUR pour les coûts opérationnels et à 7 100 000 EUR pour les ETP.

Le coût annuel des activités de maintenance est calculé, sur la base de l'expérience acquise, comme représentant 200 000 EUR par année de maintenance d'un schéma[107] et 2 ETP consacrés à ces activités (avec un coût annuel de 125 887 EUR par ETP), en tenant compte de l'année envisagée pour l'adoption du schéma. Les recettes tirées de ces redevances devraient augmenter progressivement avec la mise en place de chaque nouveau schéma et à mesure que ces schémas seront adoptés. À ce jour, un seul schéma a été adopté (l'EUCC) dans le cadre de l'ECCF et les premières recettes provenant de sa maintenance sont attendues en 2029. Les coûts devraient être couverts d'ici à 2032.

Les recettes estimées ont été calculées en formulant des hypothèses spécifiques pour chaque schéma potentiel sur les aspects suivants: l'adoption escomptée (nombre de certificats à délivrer), la durée de validité de chaque certificat et le nombre d'organismes d'évaluation de la conformité actifs. L'adoption d'un futur schéma sur la posture de cybersécurité devrait générer des recettes substantielles.

Année Recettes (pourcentage de coûts couverts/payés par le budget de l'Union)

2028 0

2029 250 000 (11%/ – 1 350 000 EUR) – un schéma (EUCC)

2030 783 000 (29%/ – 2 000 000 EUR) – trois schémas (EUCC, portefeuille d'identité, services de sécurité gérés)

2031 783 000 (25%/ – EUR 1 930 000) – trois schémas (EUCC, portefeuille d'identité, services de sécurité gérés)

2032 3 850 000 (122 %/– 2 400 000 EUR) – cinq schémas (EUCC, portefeuille d'identité, services de sécurité gérés, certification de sécurité de l'UE des services en nuage, 5G)

2033 4 000 000 (126%/ – 685 000 EUR) – six schémas (EUCC, portefeuille d'identité, services de sécurité gérés, certification de sécurité de l'UE des services en nuage, 5G, posture de cybersécurité)

2034 4 500 000 (141 %/+ 825 000 EUR) – sept schémas

Redevances liées aux outils de test destinés à faciliter les procédures d'évaluation de la conformité

Les redevances liées à cette activité seront fixées dans un acte d'exécution, à la suite de l'adoption du règlement révisé sur la cybersécurité. Toutefois, pour indiquer les coûts estimés et les recettes attendues, les calculs ont été effectués sur la base d'estimations fournies par l'ENISA et incluses dans l'analyse

[107] Plus précisément, la maintenance se compose de 2 réunions en présentiel avec des experts par an (100 000 EUR), de coûts de contractants chargés de soutenir l'élaboration et l'examen des documents justificatifs pour le schéma, de l'adoption de schémas de certification, d'un soutien aux évaluations par les pairs et de la réalisation d'évaluations de la conformité (4 x 15 000 = 60 000 EUR). Le coût comprend également la partie opérationnelle de la plateforme du MIE et le site web de certification de l'ENISA (40 000 EUR).

d’impact de la proposition de révision du règlement sur la cybersécurité. Les coûts liés au soutien des activités de test et d’évaluation sont estimés à:

ETP: 4 fois par an

Coûts opérationnels: 800 000 EUR par an

Coût total: 6 500 000 EUR (5 ans); par an: 1 300 000 EUR

Pour l’ENISA, on s’attend à ce que les investissements ponctuels de la première année soient suivis de coûts de maintenance. Ces coûts seraient progressivement couverts par les recettes tirées des redevances.

Année	Recettes
2028	0
2029	260 000
2030	260 000
2031	650 000
2032	650 000
2033	975 000
2034	975 000

4. DIMENSIONS NUMERIQUES

4.1. Exigences pertinentes en matière numérique

Description générale des exigences pertinentes en matière numérique et des catégories correspondantes (données, numérisation et automatisation des processus, solutions numériques et/ou services publics numériques)

Référence à l'exigence	**Description de l'exigence**	**Acteurs visés ou concernés par l'exigence**	**Processus généraux**	**Catégories**
Article 5, paragraphe 1, point a) Soutien à la mise en œuvre du droit de l'Union	(a) Aider les États membres à mettre en œuvre de manière cohérente la politique et le droit de l'Union en matière de cybersécurité, notamment **en publiant des rapports et des orientations techniques, en fournissant des conseils et en partageant les bonnes pratiques ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes à cette fin**;	- ENISA - États membres	- Traiter des données afin de publier des rapports et des orientations techniques, fournir des conseils, partager les bonnes pratiques et faciliter l'échange de bonnes pratiques entre les autorités compétentes - faciliter l'échange de bonnes pratiques	Traitement des données Flux de données
Article 5, paragraphe 1, point b) Soutien à la mise en œuvre du droit de l'Union	(b) soutenir **le partage d'informations au sein des secteurs et entre ceux-ci, en particulier en ce qui concerne les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555**, et les produits comportant des éléments numériques relevant du champ d'application du règlement (UE) 2024/2847, **en proposant des bonnes pratiques et des orientations sur les outils disponibles et sur les procédures**	- ENISA - secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555 - parties prenantes touchées par le règlement (UE) 2024/2847	Proposer des bonnes pratiques et des orientations sur les outils disponibles et sur les procédures	Traitement des données Flux de données

Article 5, paragraphe 1, point c) Soutien à la mise en œuvre du droit de l'Union	(c) à la demande de la Commission, aider les États membres en leur fournissant un soutien, tel que des **orientations techniques, y compris sur les mesures de gestion des risques de cybersécurité, des outils d'évaluation de la maturité en matière de cybersécurité et des manuels d'intervention en cas d'incident**, en adaptant l'aide offerte aux secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555, en vue de faciliter l'amélioration de leur niveau de maturité en matière de cybersécurité et du respect du droit de l'Union en matière de cybersécurité;	- Commission européenne - ENISA - secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555	Fournir des orientations techniques	Traitement des données Flux de données
Article 5, paragraphe 1, point e)	e) aider les États membres et les entités de l'Union concernées à **élaborer et à promouvoir des politiques en matière de cybersécurité** visant à soutenir la disponibilité et l'intégrité générales du noyau public de l'internet ouvert;	ENISA États membres Entités de l'UE	Contribuer à l'élaboration et à la promotion de politiques en matière de cybersécurité	Traitement des données Flux de données
Article 5, paragraphe 1, point f) Soutien à la mise en œuvre du droit de l'Union	f) conformément au règlement (UE) 2024/2847, **fournir des conseils et un soutien techniques** sur les questions ayant trait à la mise en œuvre et à l'application dudit règlement	-ENISA - parties prenantes touchées par le règlement (UE) 2024/2847	La fourniture de conseils et d'un soutien techniques nécessite le traitement et le partage d'informations sur les exigences réglementaires, les difficultés de mise en œuvre et les orientations en matière de conformité.	Traitement des données Flux de données
Article 5, paragraphe 1, point h)	h) à la demande du comité européen de la protection des données, fournir des conseils sur la mise en œuvre d'aspects spécifiques de la politique et de la législation de l'Union en matière de protection des données et de la vie privée ayant trait à la cybersécurité.	ENISA CEPD	Fournir des conseils sur demande	Traitement des données Flux de données

Article 5, paragraphe 2 Contribution aux évaluations des risques de cybersécurité au niveau de l'Union	L'ENISA contribue aux évaluations coordonnées des risques de cybersécurité au niveau de l'Union, y compris celles effectuées en application de l'article 22 de la directive (UE) 2022/2555.	ENISA États membres Grand public	Contribuer aux évaluations coordonnées des risques, ce qui nécessite le traitement de données et des flux de données	Traitement des données Flux de données
Article 5, paragraphe 3 L'ENISA publie des lignes directrices	L'ENISA **publie des lignes directrices** concernant l'interopérabilité transfrontière des réseaux et des systèmes d'information utilisés pour le partage d'informations, y compris en ce qui concerne les cyberpôles transfrontières visés à l'article 6, paragraphe 3, du règlement (UE) 2025/38.	ENISA États membres	L'ENISA publie des lignes directrices	Traitement des données Flux de données
Article 5, paragraphe 5 Soutien à la Commission	À la **demande de la Commission**, l'ENISA **fournit une expertise, des conseils techniques, des informations ou des analyses ou effectue des travaux préparatoires** sur des questions de cybersécurité spécifiques en vue d'éclairer l'élaboration des politiques de la Commission et le suivi de la mise en œuvre de la législation de l'Union.	Commission européenne ENISA	Préparation et transmission d'informations à la Commission	Traitement des données Flux de données

Article 6 Renforcement des capacités	L'ENISA apporte son aide en fournissant des connaissances et une expertise, des bonnes pratiques, etc.	ENISA États membres Entités de l'UE Parties prenantes publiques et privées Autorités de surveillance du marché Membres du GECC CECC	Fournir des connaissances et une expertise	Traitement des données Flux de données
Article 7 Sensibilisation et réservoir de talents	L'ENISA aide les États membres dans leurs efforts de sensibilisation aux politiques et à la législation de l'Union en matière de cybersécurité et favorise leur visibilité en **élaborant des outils et des orientations exploitables**. L'ENISA soutient les initiatives visant à accroître le réservoir européen de talents dans le domaine de la cybersécurité, notamment en coordonnant les concours.	ENISA États membres	Élaborer des outils et des orientations exploitables	Traitement des données
Article 8, paragraphe 1 Connaissance du marché et analyses	L'ENISA **effectue et diffuse des analyses** des principales tendances observées sur le marché de la cybersécurité, tant du côté de la demande que du côté de l'offre, en particulier en ce qui concerne les domaines dans lesquels des schémas européens de certification de cybersécurité existent ou sont prévus, les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555 et les catégories de produits couvertes par le règlement (UE) 2024/2847, y compris les annexes III et IV dudit règlement.	ENISA Secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555 Catégories de produits couvertes par le règlement (UE) 2024/2847	Effectuer et diffuser des analyses	Traitement des données Flux de données

Article 8, paragraphe 2 Connaissance du marché et analyses	L'ENISA **effectue et diffuse des analyses** des principales tendances technologiques en matière de cybersécurité en particulier en ce qui concerne les activités et entités relevant du champ d'application de la directive (UE) 2022/2555 et les produits comportant des éléments numériques relevant du champ d'application du règlement (UE) 2024/2847.	ENISA Grand public, parties prenantes au sens de la directive (UE) 2022/2555 et du règlement (UE) 2024/2847	Effectuer et diffuser des analyses	Traitement des données Flux de données
Article 8, paragraphe 3 Connaissance du marché et soutien des écosystèmes	L'ENISA développe des connaissances et **diffuse des conseils et des analyses techniques** sur les outils, les normes, les cadres et les bonnes pratiques les plus récents en matière de cybersécurité.	ENISA Grand public	Diffuser des conseils et des analyses techniques sur les outils, les normes, les cadres et les meilleures pratiques les plus récents en matière de cybersécurité.	Traitement des données Flux de données
Article 9 Coopération internationale	L'ENISA contribue en analysant les résultats des exercices internationaux et en en rendant compte au conseil d'administration, en facilitant l'échange de meilleures pratiques et en fournissant une expertise et des conseils à la Commission.	Public international ENISA Conseil d'administration de l'ENISA Commission européenne	Analyses et rapports; fournir des conseils, etc.	Traitement des données Flux de données
Article 10, paragraphes 2 et 3 Coopération opérationnelle	2. L'ENISA est membre du réseau des CSIRT nationaux établi en vertu de l'article 15, paragraphe 1, de la directive (UE) 2022/2555 et **assure le secrétariat** du réseau des CSIRT conformément à l'article 15, paragraphe 2, de la	ENISA CSIRTs [article 15, paragraphe 1, de la directive (UE) 2022/2555] EU-CyCLONe [article 16, paragraphe 2, de la directive (UE)	Faciliter l'échange d'informations, assurer le secrétariat des réseaux	Flux de données Solution numérique Service public

	directive (UE) 2022/2555. 3. L'ENISA **assure le secrétariat** du réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) conformément à l'article 16, paragraphe 2, deuxième alinéa, de la directive (UE) 2022/2555.	2022/2555]		numérique
Article 11, paragraphe 1, point b) Connaissance de la situation Article 12 Alertes précoces	**Émettre des alertes précoces** conformément à l'article 12	Commission européenne ENISA Europol Réseau UE-CyCLONe Réseau des CSIRT CERT-UE Entités énumérées aux annexes I et II de la directive (UE) 2022/2555	Émission d'alertes précoces	Traitement des données Flux de données Service public numérique
Article 10, paragraphe 4, point b) Coopération opérationnelle	(b) à la demande d'un ou plusieurs États membres, **fournir des conseils et des évaluations concernant un incident ou une cybermenace spécifique potentielle ou existante**, y compris en fournissant une expertise et en **facilitant la gestion technique de tels incidents**, et en **soutenant le partage volontaire d'informations et de solutions techniques pertinentes entre États membres;**	ENISA États membres	Fournir des conseils et des évaluations concernant un incident ou une cybermenace spécifique potentielle ou existante; faciliter la gestion technique de tels incidents; favoriser le partage volontaire d'informations pertinentes et de solutions techniques entre les États membres	Traitement des données Flux de données Services publics numériques

Article 10, paragraphe 4, point c) Coopération opérationnelle	(c) analyser les vulnérabilités, les menaces et les incidents;	ENISA États membres	Recueillir des données auprès de sources publiques et échanger des données avec les États membres	Traitement des données Flux de données
Article 10, paragraphe 4, point d) Coopération opérationnelle	d) à la **demande d'un ou de plusieurs États membres**, **apporter un soutien** en rapport avec les enquêtes techniques ex post sur les incidents importants au sens de la directive (UE) 2022/2555;	ENISA États membres	Analyse et soutien en réponse à des demandes techniques concernant des incidents	Traitement des données Flux de données
Article 10, paragraphe 4, point e) Coopération opérationnelle	e) contribuer à soutenir la gestion coordonnée des incidents et crises de cybersécurité majeurs au niveau opérationnel, notamment en **aidant EU-CyCLONe à préparer des rapports au niveau politique en facilitant le partage d'informations en temps utile entre le réseau des CSIRT et EU-CyCLONe**;	ENISA Réseau UE-CyCLONe Réseau des CSIRT	Analyser des données afin de contribuer à l'élaboration des rapports; faciliter le partage d'informations en temps utile entre les réseaux	Traitement des données Flux de données Service public numérique
Article 10, paragraphe 5 Coopération opérationnelle	À la **demande d'un État membre** ou d'une entité de l'Union, en coopération avec le CERT-UE, l'ENISA favorise une communication publique cohérente sur les incidents ou cybermenaces.	ENISA États membres	Réceptionner la demande et communiquer, si nécessaire	Flux de données

Article 10, paragraphe 6 Coopération opérationnelle	L'ENISA **soutient** la coopération entre les États membres et, par l'intermédiaire du CERT-UE, entre les entités de l'Union, en ce qui concerne le **déploiement d'outils de communication sécurisés**. L'ENISA utilise, au sein du réseau des CSIRT et d'EU-CyCLONe, des outils de communication sécurisés qui sont fournis par des entités juridiques non établies dans des pays tiers ni contrôlées par des pays tiers ou des ressortissants de pays tiers.	ENISA Commission européenne États membres Entités de l'UE Réseau des CSIRT Réseau UE-CyCLONe	Soutenir le déploiement d'outils de communication sécurisés et utiliser ces outils au sein du réseau des CSIRT et d'EU-CyCLONe.	Solution numérique Service public numérique
Article 11, paragraphe 1, point a) Conscience situationnelle commune en matière de cybersécurité	a) **mettre au point**, en coopération avec EU-CyCLONe, le réseau des CSIRT, la Commission, le CERT-UE, Europol et d'autres entités de l'Union concernées, des **répertoires** de renseignements vérifiés et fiables sur les cybermenaces, incluant les tendances en matière d'incidents, de tactiques, de techniques et de procédures;	Commission européenne ENISA Réseau UE-CyCLONe Réseau des CSIRT Europol Entités de l'UE CERT-UE	Mettre au point des répertoires	Flux numérique Solution numérique Service public numérique
Article 11, paragraphe 1, points c) à g) Appréciation commune de la situation en matière de cybersécurité	Fournir des analyses ad hoc en temps utile (certaines sur demande); fournir des analyses et des conseils techniques; préparer un rapport sur la situation technique en coopération avec d'autres entités; surveiller les tendances et les partager	ENISA États membres Commission européenne Entités de l'UE Réseau UE-CyCLONe Réseau des CSIRT	Analyse de données, partage d'informations et fourniture de rapports (certains sur demande)	Traitement des données Flux de données

Article 11, paragraphe 2, point a) Appréciation commune de la situation en matière de cybersécurité	L'ENISA **effectue des analyses** des cybermenaces, des incidents, des tendances, des technologies émergentes et de leurs incidences, y compris une **analyse** régulière portant sur les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555 et les catégories de produits pertinentes couvertes par le règlement (UE) 2024/2847;	ENISA Grand public	Analyser les données afin de fournir des informations ayant une incidence sur la cybersécurité; rapports réguliers	Traitement des données Flux de données
Article 11, paragraphe 2, point b) Appréciation commune de la situation en matière de cybersécurité	L'ENISA **publie, en coopération avec la Commission et, le cas échéant, le réseau des CSIRT, des avis, des orientations et des meilleures pratiques** en matière de sécurité des réseaux et des systèmes d'information, en particulier pour la sécurité des infrastructures sur lesquelles s'appuient les secteurs énumérés aux annexes I et II de la directive (UE) 2022/2555;	Commission européenne CERT-UE Réseau des CSIRT Grand public	Fournir des avis, des orientations et des meilleures pratiques	Traitement des données Flux de données
Article 11, paragraphe 2, point c) Appréciation commune de la situation en matière de cybersécurité	L'ENA réalise des **analyses stratégiques à long terme des cybermenaces** et des incidents afin d'**identifier** les tendances émergentes et de contribuer à prévenir les incidents;	ENISA Grand public	Analyse des données et détection des menaces émergentes	Traitement des données
Article 11, paragraphe 3 Appréciation commune de la situation en matière de cybersécurité	L'ENISA peut **rendre publics les analyses**, avis, orientations, meilleures pratiques et rapports visés au paragraphe 2, en accord avec les entités contributrices visées au paragraphe 2.	ENISA Grand public	Rendre publiques les informations	Flux de données Service public numérique

Article 13, paragraphe 2 Assistance lors de la réponse aux incidents	2. À la demande de la Commission ou d'EU-CyCLONe, l'ENISA, avec le soutien du réseau des CSIRT et avec l'approbation de l'État membre concerné, **examine et évalue les incidents de cybersécurité importants** ou les incidents de cybersécurité majeurs conformément à l'article 21 du règlement (UE) 2025/38.	Commission européenne ENISA Réseau UE-CyCLONe Réseau des CSIRT États membres	Examiner et évaluer les incidents de cybersécurité importants	Traitement des données
Article 14, paragraphe 2 Exercices de cybersécurité au niveau de l'Union	2. L'ENISA **tient un répertoire** des enseignements tirés des exercices visés au paragraphe 1 et fournit aux États membres et, le cas échéant, aux entités de l'Union des recommandations quant à la manière dont ils peuvent mettre en œuvre les enseignements tirés de manière efficace et efficiente.	ENISA États membres Entités de l'UE	Tenir à jour un répertoire	Traitement des données Solution numérique Service public numérique
Article 14 Exercices de cybersécurité au niveau de l'Union	Sur réception de demandes d'EU-CyCLONe, de la Commission, des États membres ou du CERT-UE, l'ENISA organise ou contribue à l'organisation d'exercices de cybersécurité. L'ENISA aide la Commission à élaborer un programme annuel continu d'exercices de cybersécurité au niveau de l'Union.	ENISA Commission États membres Entités de l'UE CERT-UE	Recevoir les demandes d'organisation ou de soutien de l'organisation d'exercices	Flux de données Traitement des données

Article 15 Disposition relative aux outils et plateformes	1. **L'ENISA établit, fournit, exploite, entretient et met à jour, si nécessaire, des outils techniques opérationnels, y compris des plateformes** relatives à la cybersécurité au niveau de l'Union, notamment la plateforme unique de signalement des incidents établie en vertu de l'article 16, paragraphe 1, du règlement (UE) 2024/2847 [et le point d'entrée unique établi en vertu de l'article 23 *bis* de la directive (UE) 2022/2555], et des outils de tests destinés à faciliter la mise en œuvre des procédures d'évaluation de la conformité conformément à la législation applicable de l'Union. 2. Si nécessaire aux fins du paragraphe 1, **l'ENISA coopère et échange des informations** avec le réseau des CSIRT et, le cas échéant, avec les autorités de surveillance du marché.	ENISA Réseau des CSIRT Grand public Autorités de surveillance du marché	L'ENISA établit, fournit, exploite, entretient et met à jour, si nécessaire, des outils techniques opérationnels, tels que des plateformes	Solution numérique Service public numérique Flux de données
Article 16, paragraphe 2 Services de gestion des vulnérabilités	(a) assurer la maintenance de la base de données européenne des vulnérabilités établie conformément à l'article 12, paragraphe 2, du règlement (UE) 2022/2555; (b) fournir des services de gestion des vulnérabilités aux **parties prenantes**, en s'appuyant sur la base de données européenne des vulnérabilités et en utilisant les informations pertinentes dont dispose l'ENISA; (c) le cas échéant, nouer une coopération structurée avec des **organisations** fournissant des programmes, des registres ou des bases de données similaires à la base de données européenne des vulnérabilités; (d) soutenir activement les **CSIRT** désignés comme coordinateurs conformément à l'article 12, paragraphe 1, de la directive (UE)	ENISA CSIRT nationaux Réseau des CSIRT Autorités nationales compétentes Industrie Communauté des chercheurs Grand public Acteurs internationaux fournissant des programmes, des registres ou des bases de données	Fournir des services de gestion des vulnérabilités; mettre en place une coopération structurée, le cas échéant; coopérer avec les parties prenantes	Solution numérique Service public numérique Flux de données

	2022/2555 en ce qui concerne la gestion de la divulgation coordonnée des vulnérabilités susceptibles d'avoir un impact important sur des entités de plusieurs États membres; e) élaborer et assurer la maintenance de méthodes et des mécanismes de gouvernance pour la détection des vulnérabilités et la divulgation coordonnée, **en coopération avec les autorités nationales compétentes, les CSIRT, l'industrie et la communauté des chercheurs;**			
Article 17 Certification de cybersécurité Article 18 Normalisation, spécifications techniques et orientations	Article 17, paragraphe 1 a) **préparer des schémas européens de certification de cybersécurité candidats (ci-après les «schémas candidats»)** pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités et les spécifications techniques connexes conformément à l'article 74; b) **assurer la maintenance des schémas européens de certification de cybersécurité adoptés** conformément à l'article 75, y compris en vue de leur éventuel réexamen conformément à l'article 76; c) promouvoir l'adoption des schémas adoptés et tenir à jour un site web dédié qui fournit des informations sur les schémas européens de certification de cybersécurité, les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne, et leur assure une publicité, conformément à l'article 79;	ENISA Grand public	Analyser les données et échanger des flux de données avec la Commission et d'autres parties prenantes; préparer le schéma de certification candidat; assurer la maintenance du site web de l'ENISA	Traitement des données Flux de données Service public numérique

	Article 17, paragraphe 2 a) **préparer** des dispositions types à faire figurer dans les schémas européens de certification de cybersécurité («schémas candidats») pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités conformément à l'article 81, paragraphe 5. Article 18 1. L'ENISA élabore des spécifications techniques et des orientations pour soutenir la mise en œuvre de la législation de l'Union dans le domaine de la cybersécurité. 2. L'ENISA **surveille les activités de normalisation menées au niveau de l'Union** et, conformément à l'article 9, au niveau international, **y participe et y joue un rôle moteur**. 3. L'ENISA soutient le développement et l'évaluation d'algorithmes cryptographiques. Lorsqu'un algorithme cryptographique évalué fait l'objet d'une évaluation positive, l'ENISA coopère, conformément au règlement (UE) nº 1025/2012, avec les organismes européens de normalisation afin d'en faciliter la normalisation. 4. L'ENISA **fournit une expertise technique** à la Commission et au GECC sur les normes ou spécifications techniques appropriées à l'appui des politiques de l'Union en matière de cybersécurité, en particulier le règlement (UE) 2024/2847, y compris pour la législation d'harmonisation de l'Union dans le domaine de			

	la cybersécurité et les schémas européens de certification de cybersécurité conformément à l'article 81, paragraphe 1, point d). 5. L'ENISA prête assistance à la Commission dans l'évaluation des projets de normes harmonisées visant à soutenir la mise en œuvre de la législation d'harmonisation de l'Union dans le domaine de la cybersécurité.			
Article 19 – Cadre européen des compétences en matière de cybersécurité	L'ENISA **élabore et met à la disposition du public un cadre européen des compétences en matière de cybersécurité (ci-après l'«ECSF»)**. Avant de mettre l'ECSF à la disposition du public ou de le mettre à jour conformément au paragraphe 4, l'ENISA **consulte la Commission**. Le recours à l'ECSF est **facultatif pour les entités publiques et privées**. L'ENISA peut **consulter les parties prenantes** lors de l'élaboration et de l'adoption de l'ECSF.	ENISA Commission Grand public États membres Entités de l'UE Parties prenantes publiques et privées	Maintenance de l'ECSF; consultation des parties prenantes; adoption de l'ECSF	Traitement des données Flux de données Solution numérique
Articles 20 à 23 – Programmes d'attestation individuelle européenne des compétences en matière de cybersécurité	L'ENISA **élabore et adopte des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité et en assure la maintenance**. Le recours à des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité est **facultatif pour les organismes publics nationaux et les entités privées**, sauf disposition contraire du droit national. Avant de lancer un nouveau programme d'attestation individuelle européenne des compétences en matière de cybersécurité, l'ENISA **consulte la Commission**. L'ENISA n'adopte un tel programme qu'après **avis favorable de la Commission**. Lors de	ENISA Commission Grand public États membres Entités de l'UE Parties prenantes publiques et privées (contribuant à l'élaboration d'un schéma d'attestation; demandeurs et fournisseurs d'attestations individuelles européennes de compétences en matière de cybersécurité, y compris les évaluateurs)	Élaborer les schémas et en assurer la maintenance; mener des consultations avec les parties prenantes; traiter les demandes; rendre des décisions; assurer la maintenance d'un site web	Traitement des données Flux de données Solution numérique Service public numérique

	l'élaboration d'un programme d'attestation individuelle européenne des compétences en matière de cybersécurité, l'ENISA peut **consulter les parties prenantes concernées.** L'ENISA veille à une **coopération étroite avec les États membres** tout au long de l'élaboration des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité. Les fournisseurs d'attestations agréés **évaluent si les personnes satisfont aux exigences** d'un programme d'attestation individuelle européenne des compétences en matière de cybersécurité et, lorsque ces exigences sont remplies, délivrent des attestations individuelles européennes de compétences en cybersécurité. L'ENISA **fournit des orientations aux évaluateurs et leur dispense une formation obligatoire** sur les exigences et les méthodes d'évaluation figurant dans le schéma européen d'attestation individuelle de compétences en matière de cybersécurité visées à l'article 20, paragraphe 3, point b). Les entités souhaitant devenir des fournisseurs d'attestations agréés ou renouveler leur agrément (ci-après les «**demandeurs**») **soumettent une demande** à l'ENISA. Les fournisseurs d'attestations agréés veillent à ce que, **à la demande de la personne**, les versions électroniques d'attestations individuelles européennes de compétences en matière de cybersécurité soient délivrées sous la forme d'attestations électroniques d'attributs			

	dans un format pouvant être stocké dans les portefeuilles européens d'identité numérique prévus par le règlement (UE) nº 910/2014. Les demandeurs et les fournisseurs d'attestations agréés permettent **à l'ENISA de procéder à des évaluations** dans le cadre de la procédure de demande initiale, du maintien de l'agrément ou de son renouvellement et communiquent toutes les informations pertinentes pour garantir que les exigences énoncées aux paragraphes 3 et 4 et les obligations énoncées au paragraphe 5 sont respectées ou continuent d'être respectées conformément à l'article 22, paragraphe 2. Les fournisseurs d'attestations agréés **informent immédiatement l'ENISA** si l'une des exigences énumérées au paragraphe 3 n'est plus satisfaite ou si un doute survient quant à son respect , y compris en ce qui concerne l'indépendance des évaluateurs. Les demandeurs **versent une redevance à l'ENISA** pour l'évaluation de leur demande. Les fournisseurs d'attestations agréés **versent une redevance à l'ENISA** pour le maintien de leur agrément. **L'ENISA évalue** si les exigences énoncées à l'article 21, paragraphes 3 et 4, et les obligations énoncées à l'article 21, paragraphe 5, sont respectées ou continuent d'être respectées par les demandeurs et les fournisseurs d'attestations agréés. Après examen d'une demande au regard des exigences énoncées à l'article 21, paragraphes 3 et 4, **l'ENISA peut**			

	rendre une décision. **L'ENISA peut modifier, suspendre ou révoquer ces décisions.** **L'ENISA assure la maintenance et la mise à jour régulière d'un site web dédié** fournissant des informations publiques sur: (a) l'ECSF, y compris le cadre et son calendrier de mise à jour; (b) les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, leur état d'avancement et leur calendrier d'élaboration; (c) les redevances associées à chaque schéma européen individuel d'attestation de compétences en matière de cybersécurité adopté en vertu de l'article 47 du présent règlement; (d) le coût indicatif d'une attestation individuelle européenne de compétences en matière de cybersécurité conformément à l'article 20, paragraphe 4; e) la liste des fournisseurs d'attestations agréés.			

Article 25 Composition du conseil d'administration	**Nommer les membres** du conseil d'administration de l'ENISA.	ENISA Commission européenne États membres	Nommer les membres	Flux de données Traitement des données
Article 28, paragraphe 1 Fonctions du conseil d'administration Article 30 Conseil exécutif	b. adopte le projet de document unique de programmation de l'ENISA visé à l'article 44, **avant de le soumettre pour avis à la Commission**; f) **évaluer** et adopter le rapport annuel consolidé sur les activités de l'ENISA, y compris les comptes et une description de la manière dont l'ENISA a atteint ses indicateurs de performance, et **transmettre**, au plus tard le 1er juillet de l'année suivante, **le rapport annuel et l'évaluation** de ce rapport au Parlement européen, au Conseil, à la Commission et à la Cour des comptes; rendre public le rapport annuel; i) assurer un **suivi adéquat des conclusions** et recommandations découlant des rapports d'audit et évaluations internes ou externes et des enquêtes de l'Office européen de lutte antifraude (OLAF) et du Parquet européen;	ENISA Commission européenne Parlement européen Conseil de l'UE Cour des comptes États membres Grand public	Soumettre le document unique de programmation à la Commission pour avis; évaluer et adopter le rapport annuel consolidé sur les activités de l'ENISA, y compris les comptes et une description de la manière dont l'ENISA a atteint ses indicateurs de performance, et transmettre le rapport annuel et l'évaluation; donner suite aux conclusions	Flux de données Traitement des données
Article 31, paragraphe 8 Nomination, révocation et prolongation du mandat	Le **conseil d'administration informe le Parlement européen** de son intention de proroger le mandat du directeur exécutif conformément au paragraphe 6. Dans les trois mois précédant cette prorogation, le directeur exécutif fait, s'il y est invité, une déclaration devant la commission concernée du Parlement européen et répond aux questions des députés.	ENISA Conseil d'administration de l'ENISA Parlement européen	Le conseil d'administration informe le Parlement européen	Flux de données

Article 32, paragraphe 3 Tâches et responsabilités du directeur exécutif Article 32, paragraphe 5	3. **Le directeur exécutif fait rapport au Parlement européen** sur l'exécution de ses tâches lorsqu'il y est invité. Le Conseil peut inviter le directeur exécutif à faire rapport de l'exécution de ses tâches. Préparation des projets de stratégies de plans budgétaires et des documents stratégiques.	Directeur exécutif de l'ENISA Parlement européen	Établir des rapports de performance	Flux de données Traitement des données
Article 35, paragraphes 5 et 6 Groupe consultatif de l'ENISA	5. Le groupe consultatif de l'ENISA **conseille l'ENISA** en ce qui concerne l'exécution des tâches de celle-ci, excepté l'application des dispositions des titres III, IV et V du présent règlement. Il conseille en particulier le directeur exécutif pour ce qui est de l'élaboration d'une proposition de programme de travail annuel pour l'ENISA et de la communication à assurer avec les parties prenantes concernées sur les questions liées au programme de travail annuel. 6. Le groupe consultatif de l'ENISA **informe régulièrement le conseil d'administration** de ses activités.	ENISA Membres du groupe consultatif de l'ENISA Conseil d'administration de l'ENISA Directeur exécutif de l'ENISA	Fournir des conseils et des orientations sur ses activités	Traitement des données Flux de données
Articles 36 à 43 Chambre de recours	L'ENISA **établit une chambre de recours** par décision du conseil d'administration. La chambre de recours est composée d'un président et de trois autres membres. Chaque membre de la chambre de recours a un suppléant. Les suppléants représentent les membres en leur absence. Le conseil d'administration nomme **le président, les autres membres ainsi que leurs suppléants** à partir d'une **liste de candidats**	ENISA Conseil d'administration de l'ENISA Commission Chambre de recours au sens de l'article 36 de la proposition de règlement sur la cybersécurité 2 Demandeurs (entités juridiques souhaitant devenir des fournisseurs d'attestations agréés	Rendre des décisions à la suite de recours Assurer le traitement des recours Préparer et publier le règlement intérieur Flux d'informations	Traitement des données Flux de données Service public numérique

	qualifiés établie par la Commission. La liste des candidats qualifiés est valable pour une durée de quatre ans. La validité de cette liste peut être prorogée par le conseil d'administration pour des périodes additionnelles de quatre ans, sur proposition de la Commission. Lorsque la chambre des recours considère que la nature du recours l'exige, elle peut demander au **conseil d'administration de nommer deux membres supplémentaires et leurs suppléants** figurant sur la liste visée au paragraphe 3. La commission de recours adopte **son règlement intérieur et le rend public**. Si, pour une des raisons visées au paragraphe 1 ou pour toute autre raison, un membre d'une chambre de recours estime qu'il ne peut prendre part à une procédure de recours, il **en informe cette chambre de recours**. La chambre de recours **décide des mesures à prendre** dans les cas énumérés aux paragraphes 2 et 3, sans la participation du membre concerné. Aux fins de cette décision, le membre concerné est remplacé à la commission de recours par son suppléant. Un recours formé en vertu du paragraphe 1 fait l'objet d'une révision préjudicielle conformément à l'article 41 avant d'être soumis à l'examen de la chambre de recours. Les demandeurs au sens de l'article 21, paragraphe 3, peuvent **former un recours contre**: les **décisions de l'ENISA** dont ils sont destinataires, en vertu de l'article 22, paragraphe 3, et les carences de l'ENISA à	ou obtenir le maintien ou le renouvellement de leur agrément)		

	l'égard de demandes qu'ils lui ont soumises dans les délais applicables prévus à l'article 22, paragraphe 4. Dans le cas visé au paragraphe 1, point a), le recours est **formé par écrit**, avec indication circonstanciée de ses motifs, conformément au règlement de procédure visé à l'article 36, paragraphe 5, dans un délai de deux mois à compter de la notification de la décision au demandeur concerné ou, à défaut, du jour où celui-ci en a eu connaissance. Dans le cas visé au paragraphe 1, point b), le recours est **formé par écrit auprès de l'ENISA** conformément au règlement intérieur visé à l'article 36, paragraphe 5, dans un délai de deux mois à compter du jour de l'expiration du délai fixé à l'article 22, paragraphe 4. Si l'ENISA estime que le recours est recevable et fondé, elle **corrige sa décision ou son absence d'action** visées à l'article 40, paragraphe 1. Si l'ENISA ne corrige pas la décision dans un délai d'un mois à compter de la réception du recours, elle **décide aussitôt si elle suspend ou non l'application de sa décision et défère le recours à la chambre de recours**. La **chambre de recours décide** de faire droit ou non au recours dans un délai de trois mois à compter de sa présentation. Lors de l'examen d'un recours, la chambre de recours statue dans les délais fixés par son règlement intérieur. Elle **invite** aussi souvent qu'il est nécessaire **les parties à la procédure de recours à présenter, dans un délai imparti, des observations sur**			

	les notifications qu'elle leur adresse ou sur les communications qui émanent des autres parties. Les parties à la procédure de recours sont autorisées à **présenter oralement leurs observations**. Lorsque la chambre de recours estime que le recours est fondé, elle **renvoie l'affaire à l'ENISA**. L'ENISA **arrête sa décision définitive** en conformité avec les conclusions de la chambre de recours et **motive ladite décision**. L'ENISA **informe les parties** à la procédure de recours en conséquence. Les recours en annulation des décisions de l'ENISA prises en vertu de l'article 22, paragraphe 3, ou les recours en carence en cas d'inaction dans les délais applicables en vertu de l'article 22, paragraphe 4, peuvent **être introduits devant la Cour de justice de l'Union européenne** après épuisement de la procédure de recours au sein de l'ENISA prévue aux articles 39 à 42 ou, en cas de carence, dans les délais applicables en vertu de l'article 41, paragraphe 2. L'ENISA est tenue de prendre toutes les mesures nécessaires pour se conformer à l'arrêt de la Cour de justice de l'Union européenne.			
Article 44 Document unique de programmation	2. Le directeur exécutif établit chaque année un projet de document unique de programmation, tel que visé au paragraphe 1, ainsi que la planification des ressources financières et humaines correspondantes, conformément à l'article 32 du règlement délégué (UE) 2019/715 de la Commission, et tenant compte des lignes directrices fixées par la Commission.	Directeur exécutif de l'ENISA Conseil d'administration de l'ENISA Commission européenne Parlement européen Conseil	Élaborer, adopter et transmettre un document unique de programmation chaque année	Flux de données

	3. Le conseil d'administration adopte, au plus tard le 30 novembre de chaque année, le document unique de programmation visé au paragraphe 1, en tenant compte de l'avis de la Commission visé à l'article 32, paragraphe 7, du règlement délégué (UE) 2019/715. Si le conseil d'administration décide de ne pas tenir compte de certains éléments de l'avis de la Commission, il fournit une justification détaillée de cette décision. Le conseil d'administration transmet, au plus tard le 31 janvier de l'année suivante, le document unique de programmation au Parlement européen, au Conseil et à la Commission, ainsi que toute version de ce document actualisée ultérieurement.			
Article 45 Établissement du budget de l'ENISA	4. La **Commission transmet le projet d'état prévisionnel à l'autorité budgétaire** en même temps que le projet de budget général de l'Union. Le projet d'état prévisionnel est également mis à la disposition de l'ENISA.	ENISA Commission européenne	Partage d'informations	Flux de données
Article 47 Redevances	En ce qui concerne les activités relatives aux programmes d'attestation individuelle européenne prévues à l'article 22, paragraphe 1, les **redevances suivantes sont perçues** auprès des demandeurs au sens de l'article 21, paragraphe 3, ou auprès des fournisseurs d'attestations agréés afin de contribuer à couvrir l'intégralité des coûts des activités menées par l'ENISA: a. délivrance d'agréments après examen portant sur le respect des	Commission ENISA Fournisseurs d'attestations Organismes d'évaluation de la conformité	Traiter les informations; payer les redevances; élaborer un rapport sur les redevances	Traitement des données Flux de données

	exigences énoncées à l'article 21, paragraphes 3 et 4, y compris la réalisation d'évaluations; b. maintien annuel de l'agrément; c. renouvellement des agréments pour les fournisseurs d'attestations individuelles européennes de compétences en matière de cybersécurité, y compris réalisation d'évaluations. En ce qui concerne la certification, **les redevances suivantes sont perçues auprès des organismes d'évaluation de la conformité** pour la maintenance des schémas européens de certification de cybersécurité dans le cadre desquels des certificats de cybersécurité européens sont délivrés, en particulier: une redevance annuelle pour la participation à un schéma européen de certification de cybersécurité; une redevance pour la délivrance de certificats de cybersécurité européens dans le cadre de schémas européens de certification de cybersécurité. Les redevances visées au point b) sont perçues lorsque l'organisme d'évaluation de la conformité soumet des certificats de cybersécurité européens à l'ENISA en vue de leur publication sur son site web conformément à l'article 79. La **Commission adopte des actes d'exécution** établissant les règles applicables aux redevances perçues par l'ENISA. L'ENISA inclut un **rapport sur les redevances**			

	perçues et leur incidence sur le budget de l'Agence dans sa procédure de reddition des comptes.			
Article 48 Article 49 Incidences budgétaires	Article 48 3. Le directeur exécutif **envoie** chaque année **à l'autorité budgétaire toute information pertinente** au sujet des résultats des procédures d'évaluation. Article 49 1. Le comptable de l'ENISA **envoie les comptes provisoires pour l'exercice** (exercice N) au comptable de la Commission et à la Cour des comptes au plus tard le 1er mars de l'exercice suivant (exercice N + 1). 2. Le comptable de l'ENISA **fournit** également **les informations comptables nécessaires à des fins de consolidation au comptable de la Commission**, selon les modalités et le format définis par ce dernier au plus tard le 1er mars de l'exercice N + 1. 3. **L'ENISA transmet un rapport sur la gestion budgétaire et financière pour l'exercice N au Parlement européen, au Conseil, à la Commission** et à la Cour des comptes, au plus tard le 31 mars de l'exercice N + 1. 4. **Dès réception des observations de la Cour des comptes pour l'exercice N sur les comptes provisoires de l'ENISA**, le comptable de l'Agence établit les comptes définitifs de l'ENISA.	ENISA Conseil d'administration de l'ENISA Commission européenne Conseil Parlement européen	Traiter et partager des informations sur le budget de l'ENISA.	Traitement des données Flux de données

	5. Le **conseil d'administration rend un avis** sur les comptes définitifs de l'ENISA pour l'année N. **Le comptable de l'Agence établit les comptes définitifs de l'ENISA sous sa propre responsabilité. Le directeur exécutif les transmet pour avis au conseil d'administration.**			
Article 52 Déclaration d'intérêts	Les parties **font une déclaration d'engagements et une déclaration indiquant l'absence ou la présence** de tout intérêt direct ou indirect qui pourrait être considéré comme préjudiciable à leur indépendance.	Direction de l'ENISA (directeur exécutif, directeur exécutif adjoint); Conseil d'administration, Experts nationaux détachés	Traiter et partager des données relatives à la déclaration d'intérêts	Traitement des données Flux de données
Article 58 Officiers de liaison	1. **Chaque État membre désigne au moins deux officiers de liaison** [dans leur autorité nationale de cybersécurité] en tant qu'experts nationaux détachés auprès de l'ENISA et qui travaillent à son siège ou à son bureau local, conformément à l'article 59, paragraphe 2. La Commission peut également désigner un officier de liaison. 2. Les agents de liaison désignés par leur État membre sont habilités à **demander et à recevoir de leur État membre toutes les**	ENISA États membres	Désigner des officiers de liaison et partager des informations	Traitement des données Flux de données

	informations pertinentes, tel que prévu dans le présent règlement, dans le plein respect du droit national ou de la pratique nationale de leur État membre, notamment pour ce qui est de la protection des données et des règles de confidentialité.			
Article 67 Traitement d'informations classifiées	Après **consultation de la Commission**, l'ENISA adopte des règles de sécurité en appliquant les principes de sécurité énoncés dans les règles de sécurité de la Commission visant à protéger les informations sensibles non classifiées et les ICUE, énoncées dans les décisions (UE, Euratom) 2015/443 et (UE, Euratom) 2015/444. Les règles de sécurité de l'ENISA couvrent les **dispositions relatives à l'échange, au traitement et au stockage de ces informations**.	ENISA Conseil d'administration Commission	Traiter des informations classifiées	Traitement des données Flux de données
Article 68, 69 et 70 Coopération avec les entités de l'Union et les autorités nationales Coopération avec les parties prenantes Coopération avec les pays tiers	L'ENISA coopère et échange des informations sur les questions liées à la cybersécurité avec les entités concernées de l'Union, les autorités de surveillance du marché et les autorités de contrôle; parties prenantes concernées; autorités compétentes de pays tiers ou d'organisations internationales	ENISA Europol CECC Comité européen de la protection des données Grand public Conseil	Partage d'informations	Flux de données

Article 72 sur l'information et la consultation du public sur les schémas européens de certification de cybersécurité	2. La Commission assure la maintenance et la mise à jour régulière d'un site web dédié fournissant des informations sur les aspects suivants: (a) les schémas européens de certification de cybersécurité dont l'élaboration est demandée; (b) les priorités stratégiques pour l'harmonisation des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou des exigences de sécurité de la législation de l'Union, y compris les domaines potentiels pour lesquels un schéma européen de certification de cybersécurité pourrait être demandé. 3. La Commission rend publiques, sur le site web visé au paragraphe 2 du présent article, les informations relatives à sa demande, adressée à l'ENISA, de préparer un schéma candidat visées à l'article 73 et sa décision d'accepter, de rejeter ou d'abandonner un schéma candidat transmis par l'ENISA conformément à l'article 74, paragraphe 7.	Commission européenne Grand public ENISA	Assurer la maintenance du site web d'information En vertu de cette disposition, la Commission est tenue de fournir des informations sur un site web accessible au public et de mener en permanence des activités connexes de gestion des données.	Service public numérique Solution numérique
Article 72 sur l'information et la consultation du public sur les schémas européens de certification de cybersécurité	Au cours de la préparation d'un schéma candidat par l'ENISA, en vertu de l'article 74, **le Parlement européen et le Conseil peuvent demander à la Commission**, en sa qualité de président du groupe GECC, et à l'ENISA, de présenter des informations pertinentes sur un projet de schéma candidat. **À la demande du Parlement européen ou du Conseil, l'ENISA, en accord avec la Commission**, et sans préjudice de l'article 54, peut **mettre à la disposition du Parlement européen et du**	ENISA Conseil de l'UE Parlement européen	Demander et envoyer des informations sur un projet de schéma candidat élaboré par l'ENISA	Flux de données

	Conseil des parties pertinentes d'un projet de schéma candidat d'une manière adaptée au niveau de confidentialité requis et, le cas échéant, de manière restreinte. **Le Parlement européen et le Conseil peuvent inviter la Commission et l'ENISA à discuter** de questions concernant la mise en œuvre de schémas européens de certification de cybersécurité pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités.			
Article 73 Demande de schéma européen de certification de cybersécurité Article 74 Élaboration et adoption de schémas européens de certification de cybersécurité **(couverts à l'article 17)**	**Article 73** **1. La Commission peut demander à l'ENISA de préparer un schéma européen de certification de cybersécurité candidat** pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités. Dans des cas dûment justifiés, le GECC peut suggérer à la Commission de présenter une demande visée au paragraphe 1. 4. Lorsqu'elle prépare la demande visée au paragraphe 1, **la Commission** consulte dûment l'ENISA et le GECC et tient compte des avis de toutes les **parties prenantes concernées** et des autres entités de l'Union concernées, y compris, le cas échéant, celles qui sont pertinentes en vertu d'actes législatifs de l'Union dans lesquels un schéma européen de certification de cybersécurité confère une présomption de conformité.	Commission européenne ENISA GECC Parties prenantes expertes	Préparer une demande et un schéma de certification et consulter les parties prenantes dans ce cadre	Traitement des données Flux de données Service public numérique (couverts à l'article 17)

	Article 74 3. Lors de la préparation du schéma candidat, l'ENISA **coopère étroitement avec le GECC**. **Celui-ci fournit aide et expertise à l'ENISA** dans le cadre de la préparation du schéma candidat et, le cas échéant, une spécification technique pour soutenir son travail. **L'ENISA demande aux membres du GECC de rendre un avis écrit sur le schéma candidat.** 4. **L'ENISA consulte en temps utile les parties prenantes** au moyen d'un processus de consultation formel, ouvert, transparent et inclusif. **L'ENISA coopère également avec les autorités publiques compétentes des États membres et avec les entités concernées de l'Union afin de recueillir leur expertise** en ce qui concerne la préparation du schéma candidat et, le cas échéant, une spécification technique pour soutenir son travail. 6. **L'ENISA transmet le schéma candidat** à la Commission au plus tard 60 jours à compter de la date de la demande visée au paragraphe 5. 7. Lorsqu'elle reçoit le **schéma** candidat, **la Commission évalue** s'il correspond à la demande formulée conformément à l'article 73. 8. Lorsque la Commission renvoie un schéma candidat à l'ENISA pour révision conformément au paragraphe 7, point b), les paragraphes 4, 5 et 7 du présent article s'appliquent en conséquence.			

Article 75 Maintenance d'un schéma européen de certification de cybersécurité	2. L'ENISA, en coopération avec la Commission et avec le soutien du GECC et de son sous-groupe pertinent sur la maintenance, assure la maintenance des schémas européens de certification de cybersécurité, y compris en vue de leur éventuel réexamen par la Commission. L'ENISA coopère et échange des informations avec les entités et groupes de l'Union concernés en ce qui concerne les activités de maintenance. 5. Le GECC peut émettre un avis sur la maintenance des schémas européens de certification de cybersécurité.	Commission européenne ENISA GECC Organismes d'évaluation de la conformité	L'ENISA assure la maintenance. Celle-ci comprend des réunions périodiques hybrides ou en ligne, des collectes d'informations, des analyses et du partage (en lien avec un schéma européen de certification de cybersécurité).	Traitement des données Flux de données
Article 76 Évaluation, réexamen et retrait d'un schéma européen de certification de cybersécurité	1. Au moins tous les quatre ans après l'entrée en application d'un schéma européen de certification de cybersécurité, l'ENISA évalue l'incidence et l'efficacité de ce schéma, en coopération avec le sous-groupe pertinent du GECC sur la maintenance, et en tenant compte des retours d'information reçus des parties prenantes. L'ENISA effectue l'évaluation en procédant à l'analyse de marché nécessaire conformément à l'article 8, paragraphe 1. 3. Lors du réexamen ou du retrait d'un schéma européen de certification de cybersécurité, la Commission consulte l'ENISA, le GECC et son sous-groupe pertinent sur la maintenance et tient également compte des points de vue des parties prenantes concernées et d'autres entités de l'Union. 4. Le GECC peut émettre un avis sur le réexamen ou le retrait d'un schéma européen de certification de cybersécurité. La Commission en tient dûment compte au moment de réexaminer ou de retirer le schéma européen de	Commission européenne ENISA GECC	La Commission réexamine les schémas en consultation avec les parties prenantes concernées.	Traitement des données Flux de données

	certification de cybersécurité.			
Article 77 Spécifications techniques dans les schémas européens de certification de cybersécurité	3. Lorsque des spécifications techniques sont mentionnées dans un schéma européen de certification de cybersécurité en application de l'article 74, paragraphe 10, elles sont mises à disposition sur le site web visé à l'article 79. 4. Dans des cas dûment justifiés, en particulier lorsque les spécifications techniques contiennent des informations susceptibles de compromettre la sécurité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou de la posture de cybersécurité d'entités qui ont été certifiés, elles ne sont diffusées qu'aux parties prenantes concernées par les exigences du schéma. Ce schéma n'est pas mentionné dans un schéma européen de certification de cybersécurité tel que visé à l'article 74, paragraphe 10.	ENISA États membres Organismes d'évaluation de la conformité	Mettre des informations à disposition sur le site web de l'ENISA consacré à la certification	Flux de données Service public numérique
Article 79 Site internet sur les schémas européens de certification de cybersécurité	1. L'ENISA organise des activités en vue d'encourager l'utilisation des schémas européens de certification de cybersécurité adoptés, y compris en tenant à jour le site web visé au paragraphe 2 du présent article. 2. L'ENISA assure la maintenance et la mise à jour régulière d'un site web dédié fournissant des informations publiques sur: (a) Systèmes européens de certification de cybersécurité	ENISA États membres Organismes d'évaluation de la conformité	Pour les besoins de la maintenance du site web d'information, l'ENISA doit collecter, traiter et tenir à jour des bases de données complètes d'informations relatives à la certification, ce qui nécessite des activités continues de gestion des données.	Service public numérique Solution numérique Traitement des données Flux de données

	(b) les redevances liées à la maintenance de chaque schéma européen de certification de cybersécurité; c) les spécifications techniques pertinentes de l'ENISA; (d) les certificats de cybersécurité européens et les déclarations de conformité de l'UE, y compris des informations sur les certificats et déclarations qui ne sont plus valables, qui ont été suspendus ou retirés ou qui ont expiré; e) des informations supplémentaires pertinentes sur la cybersécurité, fournies conformément à l'article 84, paragraphe 2; f) des résumés des examens par les pairs visés à l'article 89, paragraphe 7; g) les spécifications techniques mentionnées dans un schéma européen de certification de cybersécurité conformément à l'article 74, paragraphe 10. 3. Le cas échéant, le **site internet visé au paragraphe 2 indique également** les schémas nationaux de certification de cybersécurité qui ont été remplacés par un schéma européen de certification de cybersécurité.			
Article 81 Éléments des schémas européens de certification de cybersécurité	5. La Commission est habilitée à adopter des actes d'exécution établissant des principes communs et des dispositions types pour les éléments énoncés aux paragraphes 1, 2 et 3 dans l'ensemble des schémas européens de certification de cybersécurité. Un schéma européen de certification de cybersécurité peut inclure des références à ces principes et dispositions types, le cas échéant et lorsqu'elles	ENISA Grand public Autorités des États membres	Consulter les parties prenantes concernées, ce qui nécessite des flux et des traitements de données	Flux de données Traitement des données

	sont disponibles. Les actes d'exécution visés au paragraphe 5 sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2. **Lors de l'élaboration ou de la révision des principes communs et des dispositions types pour les éléments des schémas européens de certification de cybersécurité, la Commission consulte l'ENISA et tient compte, le cas échéant, des points de vue exprimés par le GECC, les parties prenantes concernées et d'autres organismes pertinents.**			
Article 83 Autoévaluation de la conformité	3. Le fabricant ou fournisseur de produits TIC, de services TIC, de processus TIC ou de services de sécurité gérés ou l'entité dont la posture de cybersécurité fait l'objet d'une certification garde à la disposition de l'autorité nationale de certification de cybersécurité désignée en vertu de l'article 89 la déclaration de conformité de l'Union européenne, la documentation technique et toutes les autres informations pertinentes relatives à la conformité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou de la posture de cybersécurité avec le schéma européen de certification de cybersécurité pendant la durée prévue dans ce schéma. **Une copie de la déclaration de conformité de l'Union européenne est transmise dans les plus brefs délais à l'autorité nationale de certification de cybersécurité et à l'ENISA.**	ENISA Grand public Autorités des États membres	Informations disponibles; partage des données Les données partagées doivent être traitées par l'ENISA et les autorités des États membres	Flux de données Traitement des données
Article 84	1. Le fabricant ou le fournisseur de produits	Fabricant ou fournisseur de	Mettre les informations à la	Flux de

Informations supplémentaires en matière de cybersécurité pour les produits TIC, services TIC et processus TIC certifiés	TIC, de services TIC ou de processus TIC pour lesquels une déclaration de conformité de l'UE a été délivrée **met les informations supplémentaires en matière de cybersécurité qui suivent à la disposition du public**:	produits TIC, de services TIC ou de processus TIC Grand public Organismes d'évaluation de la conformité	disposition du public sous forme électronique.	données
Article 85 Délivrance de certificats de cybersécurité européens	2. Les organismes d'évaluation de la conformité visés à l'article 91 délivrent des certificats de cybersécurité européens sur la base des critères figurant dans le schéma européen de certification de cybersécurité adopté conformément à l'article 74. 6. La personne physique ou morale qui soumet des produits TIC, services TIC, processus TIC ou services de sécurité gérés à la certification ou l'entité qui demande la certification de sa posture de cybersécurité **met toutes les informations nécessaires pour procéder à la certification à la disposition de l'autorité nationale de certification de cybersécurité** désignée en vertu de l'article 89, lorsque cette autorité est l'organisme délivrant le certificat de cybersécurité européen, ou de l'organisme d'évaluation de la conformité visé à l'article 91. 7. Les organismes d'évaluation de la conformité et, le cas échéant, les autorités nationales de certification de cybersécurité **informent l'ENISA** dans les meilleurs délais de leurs décisions ayant ont une incidence sur le statut des certificats de cybersécurité européens et des déclarations de conformité de l'Union conformément à l'article 94. 8. Le **titulaire d'un certificat de cybersécurité européen informe l'organisme d'évaluation de la conformité** et, le cas échéant, l'autorité	ENISA Grand public Autorités des États membres Organismes d'évaluation de la conformité	Partager des informations pertinentes pour les processus de certification	Flux de données Traitement des données

	nationale de certification de cybersécurité visée au paragraphe 7 de toute vulnérabilité ou non-conformité détectée ultérieurement concernant le produit TIC, service TIC, processus TIC ou service de sécurité géré certifié ou la posture de cybersécurité de l'entité certifiée susceptible d'avoir une incidence sur sa conformité avec le certificat. **Cet organisme transmet ces informations sans retard injustifié** à l'autorité nationale de certification de cybersécurité concernée et évalue l'incidence sur le certificat conformément aux conditions du schéma visées à l'article 81, point f).			
Article 86 Schémas nationaux de certification de cybersécurité	4. **Les États membres informent la Commission et le GECC avant d'adopter de nouveaux schémas nationaux de certification de cybersécurité** pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés et la posture de cybersécurité des entités.	ENISA États membres Commission européenne	Échange d'informations	Flux de données
Article 88 Autorités nationales de certification de cybersécurité	2. Chaque État membre **informe la Commission de l'identité des autorités nationales de certification de cybersécurité désignées**. Lorsqu'un État membre désigne plus d'une autorité, il communique en outre à la Commission des informations sur les tâches confiées à chacune de ces autorités. 6. Les autorités nationales de certification de cybersécurité: c) **contrôlent, en coopération avec les autorités de surveillance du marché concernées, le respect des obligations, énoncées dans le présent règlement, qui incombent aux fabricants ou fournisseurs** de	ENISA Autorités des États membres Commission européenne Grand public Organismes d'évaluation de la conformité	Les États membres informent la Commission des ANCC désignées Les autorités des États membres exécutent diverses tâches de surveillance, de contrôle et de coopération qui nécessitent des flux de données et des traitements de données	Flux de données Traitement des données

	produits TIC, services TIC, processus TIC ou services de sécurité gérés ou aux entités dont la posture de cybersécurité est certifiée qui sont établis sur leurs territoires respectifs et qui procèdent à une autoévaluation de conformité dans le schéma européen de certification de cybersécurité correspondant, et font respecter ces obligations; (d) sans préjudice de l'article 91, paragraphe 3, **assistent et soutiennent activement les organismes nationaux d'accréditation ou autres autorités compétentes dans le contrôle et la supervision** des activités des organismes d'évaluation de la conformité aux fins du présent règlement; e) coopèrent avec la Commission européenne lorsque la compétence d'un organisme d'évaluation de la conformité est contestée en vertu de l'article 94; f) **contrôlent et supervisent les activités** des organismes publics visées à l'article 85, paragraphe 3; g) lorsqu'il y a lieu, autorisent les organismes d'évaluation de la conformité à effectuer leurs tâches conformément à l'article 93, contrôlent le respect des obligations qui incombent aux organismes d'évaluation de la conformité en ce qui concerne les exigences spécifiques ou supplémentaires énoncées dans les schémas européens de certification de cybersécurité conformément à l'article 81, paragraphe 3, point f), et font respecter ces obligations et limitent, suspendent ou retirent les autorisations existantes lorsque les organismes			

	d'évaluation de la conformité ne répondent pas aux exigences du présent règlement; h) **traitent les réclamations** introduites par des personnes physiques ou morales en rapport avec les certificats de cybersécurité européens délivrés par des autorités nationales de certification de cybersécurité ou en rapport avec les certificats de cybersécurité européens délivrés par des organismes d'évaluation de la conformité conformément à l'article 85, paragraphe 4, ou en rapport avec les déclarations de conformité de l'Union européenne délivrées au titre de l'article 83, examinent l'objet de ces réclamations dans la mesure nécessaire et informent l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable; i) présente un rapport annuel sur leurs principales activités à la Commission, à l'ENISA et au GECC au plus tard le 31 mars [année d'entrée en vigueur + 12 mois] de chaque année et mettent ces rapports à la disposition de l'équipe chargée de l'examen par les pairs lorsque l'autorité nationale de certification de cybersécurité fait l'objet d'un examen par les pairs conformément à l'article 89; j) **coopèrent avec les autres autorités nationales de certification de cybersécurité**, les autorités de surveillance du marché ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuel non-respect par des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés et la posture de cybersécurité d'entités des			

	exigences du présent règlement ou des exigences de schémas de certification de cybersécurité spécifiques; k) **suivent les évolutions pertinentes dans le domaine de la certification de cybersécurité.** 8. Les autorités nationales de certification de cybersécurité coopèrent entre elles et avec la Commission et **échangent notamment des informations, expériences et bonnes pratiques** en ce qui concerne la certification de cybersécurité et les questions techniques relatives à la cybersécurité des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés et de la posture de cybersécurité des entités. 9. Au plus tard le [entrée en vigueur + 6 mois], l'ENISA élabore un modèle pour le rapport visé au paragraphe 6, point i), du présent article, en coopération avec la Commission et le GECC.			
Article 89 Examen par les pairs	5. **L'ENISA soutient** l'organisation du mécanisme d'examen par les pairs et des examens par les pairs, y compris **en élaborant des documents d'orientation et des modèles pertinents**, en coopération avec la Commission et le GECC. 7. Le **rapport final, qui contient les éventuelles** lignes directrices ou recommandations ainsi que le résumé de l'examen par les pairs, est examiné par le GECC, qui approuve le résumé en vue de sa	UE ENISA GECC	Mise à disposition des données en ligne	Flux de données Traitement des données

	publication sur le site web visé à l'article 79, paragraphe 2.			
Article 90 Groupe européen de certification de cybersécurité (GECC)	3. Le GECC a pour mission: [référence à d'autres articles] h) examiner les évolutions pertinentes dans le domaine de la certification de cybersécurité, y compris au niveau national conformément à l'article 86, et d'échanger des informations et de bonnes pratiques sur les schémas de certification de cybersécurité; i) faciliter la coopération entre les autorités nationales de certification de cybersécurité en vertu des règles énoncées dans le présent titre par le renforcement des capacités et l'échange d'informations, en particulier en ce qui concerne les questions relatives à la certification de cybersécurité, [référence à d'autres articles] k) faciliter l'alignement des schémas européens de certification de cybersécurité sur les normes internationalement reconnues, y compris dans le cadre de la maintenance des schémas européens de certification de cybersécurité existants et, s'il y a lieu, recommander à l'ENISA de nouer le dialogue avec les organisations européennes ou internationales de normalisation compétentes dans le but de remédier à des insuffisances ou à des lacunes affectant les normes en vigueur reconnues au niveau mondial ou européen.	États membres ENISA Commission européenne	Analyse, partage d'informations et coopération entre les autorités des États membres et les organisations internationales en ce qui concerne la certification européenne de cybersécurité	Traitement des données Flux de données

Article 92 Harmonisation supplémentaire de la compétence des organismes d'évaluation de la conformité	4. Lorsqu'une autorité nationale de certification de cybersécurité reçoit une demande en vertu du paragraphe 3, **elle informe l'autorité nationale de certification de cybersécurité de l'État membre dans lequel l'organisme d'évaluation de la conformité demandeur est établi.** Dans un tel cas, l'autorité nationale de certification de cybersécurité de cet État membre peut participer à l'autorisation en tant qu'observatrice.	Autorités des États membres Organismes d'évaluation de la conformité	Partage et conservation d'informations	Flux de données Traitement des données
Article 93 Notifications des organismes d'évaluation de la conformité	1. Pour chaque schéma européen de certification de cybersécurité, les **autorités nationales de certification de cybersécurité d'un État membre notifient à la Commission et aux autres États membres** les organismes d'évaluation de la conformité qui ont été accrédités et, le cas échéant, autorisés en vertu de l'article 92. 2. **Les autorités nationales de certification de cybersécurité procèdent à la notification comme indiqué au paragraphe 1** au moyen de l'outil de notification électronique mis au point et géré par la Commission.	ENISA États membres Commission européenne Organismes d'évaluation de la conformité	Notifications des organismes d'évaluation de la conformité accrédités et autorisés	Flux de données Traitement des données
Article 94 Contestation de la compétence des organismes d'évaluation de la conformité	1. 1. **La Commission enquête** sur tous les cas dans lesquels elle nourrit des doutes ou est avertie de doutes quant à la compétence d'un organisme d'évaluation de la conformité pour remplir les exigences qui lui sont applicables et s'acquitter des responsabilités qui lui incombent, ou quant au fait qu'il continue à remplir ces exigences et à s'acquitter de ces responsabilités. 2. L'autorité nationale de certification de cybersécurité communique à la Commission, sur demande, toutes les informations relatives au fondement de la notification ou au maintien de	Commission États membres ENISA	Contestation de la compétence des organismes d'évaluation de la conformité	Flux de données Traitement des données Service public numérique

	la compétence de l'organisme d'évaluation de la conformité concerné. 3. **La Commission veille à ce que toutes les informations sensibles obtenues au cours de ses enquêtes soient traitées de manière confidentielle.** 4. Lorsque la Commission établit qu'un organisme d'évaluation de la conformité ne répond pas ou ne répond plus aux exigences relatives à sa notification, **elle en informe l'autorité nationale de certification de cybersécurité** et l'invite à prendre les mesures correctives qui s'imposent, y compris la dénotification si nécessaire.			
Article 95 Obligation d'information et de conservation incombant aux organismes d'évaluation de la conformité	1. Les organismes d'évaluation de la conformité **informent l'autorité nationale de certification de cybersécurité** des éléments suivants: (a) tout refus, restriction, suspension ou retrait d'un certificat; (b) toute circonstance ayant une incidence sur la portée et les conditions de la notification visée à l'article 93, paragraphe 1; (c) toute demande d'information reçue des autorités de surveillance du marché concernant des activités d'évaluation de la conformité; (d) sur demande, les activités d'évaluation de la conformité accomplies dans le cadre de leur notification et toute autre activité réalisée, y compris les activités et sous-traitances transfrontières. 2. **Les organismes d'évaluation de la conformité fournissent également à l'ENISA les informations** visées au paragraphe 1, point a), en vue de faciliter	Autorités des États membres Organismes d'évaluation de la conformité	Échange d'informations entre les organismes d'évaluation de la conformité	Flux de données Traitement des données

	l'exécution de sa mission au titre de l'article 79. 3. Les **organismes d'évaluation de la conformité fournissent aux autres organismes d'évaluation de la conformité** au titre du présent règlement qui effectuent des activités similaires d'évaluation de la conformité couvrant les mêmes produits TIC, services TIC, processus TIC, services de sécurité gérés ou entités dont la posture de cybersécurité est certifiée, dans les meilleurs délais, **des informations pertinentes** sur les questions relatives aux résultats négatifs de l'évaluation de la conformité et, sur demande, aux résultats positifs. 4. **Les organismes d'évaluation de la conformité tiennent à jour un système d'archivage** contenant tous les documents et éléments de preuve produits ou reçus dans le cadre de chaque évaluation et certification qu'ils effectuent. L'enregistrement est conservé de manière sécurisée et accessible pendant la durée nécessaire aux fins de la certification et pendant au moins cinq ans après l'expiration ou le retrait d'un certificat de cybersécurité européen concerné.			
Article 96 Droit d'introduire une réclamation et droit à un recours	2. L'autorité ou l'organisme auprès duquel la réclamation a été introduite **informe l'auteur de la réclamation de l'état d'avancement** de la	Autorités des États membres Commission européenne Grand public	Flux d'informations entre les autorités et le grand public concernant les réclamations	Flux de données

juridictionnel effectif	procédure, de la décision prise et de son droit à un recours juridictionnel effectif visé aux paragraphes 3 et 4. 4. Les recours formés en vertu du présent article sont portés devant les juridictions de l'État membre dans lequel se trouve l'autorité ou l'organisme à l'encontre duquel le recours juridictionnel a été formé.	Titulaires d'un certificat	Procédures devant les juridictions de l'État membre	
Article 97 Sanctions	**Les États membres informent la Commission sans retard** du régime ainsi déterminé et des mesures ainsi prises, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.	Autorités des États membres Commission européenne	Flux d'informations relatif à la notification des sanctions par les États membres à la Commission.	Flux de données
Article 99 Évaluations des risques pour la sécurité	La Commission ou au moins trois États membres peuvent demander au groupe de coordination SRI de procéder à des évaluations coordonnées des risques dans un délai de six mois. La Commission peut demander des délais plus courts. Lors des évaluations des risques, des scénarios de risque sont élaborés et une analyse des risques est prise comme hypothèse. La préparation des évaluations coordonnées des risques pour la sécurité Dans les cas qui justifient une intervention immédiate, la Commission consulte sans tarder les États membres et procède à une évaluation des risques. Décisions relatives à la réalisation d'évaluations des risques (traitement/analyse de données).	Commission européenne États membres de l'UE Groupe de coopération SRI ENISA	Demander et recevoir des informations; analyse de données aux fins des évaluations coordonnées des risques Consultation des États membres et réalisation d'une évaluation des risques	Traitement des données Flux de données

Article 100, paragraphes 1 et 2 Désignation des pays tiers suscitant des préoccupations en matière de cybersécurité	1. Lorsque, à la suite de l'évaluation des risques pour la sécurité visée à l'article 99, ou sur la base d'autres sources, telles qu'une déclaration publique au nom de l'Union ou d'un État membre, il apparaît qu'un pays tiers présente des risques non techniques graves et structurels pour les chaînes d'approvisionnement des TIC, la Commission vérifie la menace posée par ce pays, en tenant compte d'une série d'éléments avant de procéder à un traitement/une analyse de données. 2. Lorsque la Commission, à la suite de la vérification visée au paragraphe 1, conclut qu'un pays tiers présente des risques non techniques graves et structurels pour les chaînes d'approvisionnement des TIC, elle peut décider, au moyen d'un acte d'exécution, de désigner ce pays tiers comme un pays suscitant des préoccupations en matière de cybersécurité pour les chaînes d'approvisionnement des TIC, ce qui débouche ensuite sur un traitement, une analyse et des flux de données.	États membres de l'UE Commission européenne	Recevoir, analyser et échanger des informations	Flux de données Traitement des données

Article 101 Mécanisme général de la chaîne d'approvisionnement des TIC Article 102 Identification des actifs de TIC essentiels Article 103 Mesures d'atténuation dans les chaînes d'approvisionnement des TIC	1. Lorsque le groupe de coopération SRI a procédé à une évaluation coordonnée au niveau de l'Union des risques pour la sécurité conformément à l'article 99, paragraphes 1 et 2, du présent règlement, ou après l'achèvement de la procédure en cas de cybermenace importante établie à l'article 99, paragraphe 3, la Commission peut prendre les mesures prévues aux articles 102 et 103. La Commission est habilitée à adopter des actes d'exécution qui identifieront les actifs de TIC essentiels et les mesures d'atténuation, y compris les restrictions et interdictions des chaînes d'approvisionnement des TIC (détaillées à la section 4.5 ci-dessous). Lors de la préparation de ce processus, la Commission tient compte de plusieurs aspects ayant trait au **traitement/à analyse de données et, dans certains cas, aux flux de donnée**s: Article 102, points a) à f) Article 103, paragraphe 4, points a) à d) Article 103, paragraphe 6	Commission européenne Groupe de coopération SRI Parties prenantes concernées	Analyse de données/traitement de données; consultation des acteurs concernés	Traitement des données Flux de données

Article 104 Recensement des fournisseurs à haut risque	La Commission établit, par voie d'actes d'exécution, des listes des fournisseurs à haut risque concernés par les interdictions énoncées dans les actes d'exécution adoptés conformément à l'article 103, paragraphe 1 ou par l'interdiction visée à l'article 111, paragraphe 1. La Commission répertorie les fournisseurs offrant des composants TIC ou des composants comprenant des composants TIC et procède à une évaluation initiale visant à déterminer quels fournisseurs pourraient être établis dans des pays tiers désignés conformément à l'article 100 ou contrôlés depuis de tels pays. La Commission évalue le lieu d'établissement ainsi que la structure de propriété et de contrôle. La Commission est habilitée à demander les informations nécessaires aux fournisseurs et communique au fournisseur concerné les conclusions préliminaires de son évaluation de l'établissement, de la propriété et du contrôle, en lui donnant la possibilité d'être entendu. La Commission peut demander à une autorité compétente de procéder à l'évaluation initiale de l'établissement, de la propriété et du contrôle d'un fournisseur, lorsque les caractéristiques du	Commission européenne Autorités compétentes Fournisseurs:	Analyse de données/traitement de données; consultation des autorités compétentes et des fournisseurs	Traitement des données Flux de données

	fonctionnement de ce fournisseur le justifient. Une autorité compétente peut proposer d'effectuer cette évaluation initiale. La Commission vérifie ces conclusions initiales afin de décider si le fournisseur doit être inclus dans la liste des fournisseurs à haut risque. La Commission met régulièrement à jour les listes des fournisseurs à haut risque afin de supprimer ou d'ajouter des fournisseurs à haut risque. Les fournisseurs à haut risque figurant sur la liste peuvent demander à la Commission de réévaluer leur structure d'établissement, de contrôle et de propriété s'ils apportent la preuve qu'il y a eu des changements pertinents.			
Article 105 Exemption des entités établies dans des pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlées par des entités de tels pays Article 108 Confidentialité	1) Une entité établie dans un pays tiers désigné comme suscitant des préoccupations en matière de cybersécurité ou contrôlée depuis un tel pays **peut adresser une demande motivée** à la Commission. 3) La Commission évalue et adopte une décision **tenant compte de plusieurs aspects** conduisant à une analyse de données. [article 105 (paragraphes 3 et 4)] Les informations obtenues par la Commission ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été acquises.	Commission européenne Entités établies dans des pays tiers désignés comme suscitant des préoccupations en matière de cybersécurité ou contrôlées par des entités de tels pays	Réception d'une demande par la Commission; analyse des données.	Flux de données Traitement des données

Article 107 Registre	La Commission tient un registre accessible au public reprenant ses décisions visées à l'article 105. Ce registre indique le nom des entités ayant fait l'objet des décisions.	Commission européenne Entités établies dans des pays tiers désignés comme suscitant des préoccupations en matière de cybersécurité ou contrôlées depuis de tels pays	La Commission tient un registre accessible au public.	Solution numérique
Article 111 Interdictions applicables aux réseaux de communications électroniques mobiles, fixes et par satellite	L'autorité compétente désignée en vertu du présent règlement **informe** sans délai l'autorité compétente conformément au règlement (UE) XX/XXXX [proposition de règlement sur les réseaux numériques] des mesures imposées aux fournisseurs de réseaux de communications électroniques mobiles, fixes et par satellite.	Autorité compétente au sens de l'article 9 ou 20 du règlement (UE) XX/XXXX [proposition de règlement sur les réseaux numériques] Fournisseurs de réseaux de communications électroniques mobiles, fixes et par satellite	Flux d'informations de l'autorité compétente vers les entités concernant les autorisations.	Flux de données
Article 112, paragraphes 1 et 4 Autorités compétentes	1) **Chaque État membre désigne** une ou plusieurs autorités compétentes chargées des tâches de supervision et d'exécution visées à l'article 114. 4) chaque État membre notifie dans les meilleurs délais à la Commission le nom des autorités compétentes désignées conformément au paragraphe 1, les tâches qui sont confiées à ces autorités et toute modification ultérieure les concernant. Chaque État membre rend également publics les noms des autorités compétentes désignées conformément au paragraphe 1.	États membres de l'UE Commission européenne Grand public	Les États membres désignent les autorités compétentes et notifient la Commission.	Flux de données

Article 113 Réseau des services de coopération et de soutien de la Commission	1. La Commission met en place un réseau de coopération entre les autorités compétentes des États membres et elle-même, qui sert de plateforme de coopération et d'échange d'informations. La Commission se charge d'apporter le soutien administratif à ce réseau. 2. Afin d'aider les États membres dans leurs tâches de supervision, la Commission évalue si les fournisseurs susceptibles d'être concernés par des interdictions spécifiques sont établis dans des pays tiers suscitant des préoccupations en matière de cybersécurité, désignés comme tels conformément à l'article 100, ou contrôlés à partir de tels pays. À cette fin, l'autorité compétente partage les informations pertinentes avec la Commission. 3. Aux fins de l'évaluation, la Commission est habilitée à demander les informations nécessaires aux fournisseurs susceptibles d'être concernés par des interdictions spécifiques qui sont établis dans des pays tiers désignés conformément à l'article 100, ou contrôlés à partir de tels pays. 4. Lorsqu'une évaluation est achevée, la Commission communique ses conclusions aux autorités compétentes au sein du réseau établi conformément au paragraphe 1. Les autorités compétentes informent en temps	Commission Autorités compétentes Entités du type visé aux annexes I et II de la directive (UE) 2022/2555	La Commission évalue les fournisseurs et communique le résultat aux autorités compétentes, qui le transmettent aux entités du type visé aux annexes I et II de la directive (UE) 2022/2555 La Commission demande des informations aux fournisseurs Les autorités compétentes informent la Commission	Traitement des données Flux de données

	utile les entités concernées du type visé aux annexes I et II de la directive (UE) 2022/2555 des conclusions. 5. Lorsqu'une autorité compétente apprend qu'un fournisseur susceptible d'être affecté par des interdictions spécifiques qui est établi dans un pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlé à partir d'un tel pays n'a pas fait l'objet d'une évaluation, elle en informe la Commission dans les meilleurs délais.			
Article 114 Mesures de supervision et d'exécution	Exigences imposées aux États membres qui garantiront un flux d'information avec les autorités compétentes des entités visées aux annexes I et II de la directive (UE) 2022/2555. Avant de prendre des mesures, les autorités compétentes informent les entités concernées de leurs conclusions préliminaires. Les autorités compétentes coopèrent les unes avec les autres ainsi qu'avec la Commission.	États membres de l'UE Commission européenne Entités relevant des annexes I et II de la directive (UE) 2022/2555	Exigences garantissant le flux d'informations;	Flux de données Traitement des données

Article 115 Sanctions	Les États membres informent la Commission du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.	Commission européenne États membres de l'UE	Les États membres notifient la Commission	Flux de données
Article 116 Assistance mutuelle	Lorsqu'une entité visée à l'annexe I ou II de la directive (UE) 2022/2555 fournit des services dans plusieurs États membres, ou fournit des services dans un ou plusieurs États membres alors que ses actifs essentiels sont situés dans un ou plusieurs autres États membres, **les autorités compétentes des États membres concernés coopèrent et se prêtent mutuellement assistance si nécessaire**. L'assistance mutuelle visée au premier alinéa, point c), peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés. Une autorité compétente à laquelle une demande d'assistance est adressée ne peut refuser cette demande que s'il est établi que l'autorité n'est pas compétente pour fournir l'assistance demandée, que l'assistance demandée n'est pas proportionnée aux tâches de supervision	États membres de l'UE	Assistance mutuelle dans le cadre des actions de supervision	Flux de données Traitement des données

	de l'autorité compétente ou que la demande concerne des informations ou implique des activités dont la divulgation ou l'exercice seraient contraires aux intérêts essentiels de la sécurité nationale, la sécurité publique ou la défense de cet État membre. Avant de refuser une telle demande, l'autorité compétente consulte les autres autorités compétentes concernées ainsi que, à la demande de l'un des États membres concernés, la Commission. Le cas échéant et d'un commun accord, les autorités compétentes de différents États membres peuvent mener à bien des actions communes de supervision.			
Article 1er, point 8), de la directive Signalement d'attaques par rançongiciel (Article 27, paragraphe 13, de la directive SRI 2)	À l'article 23, les paragraphes 12 et 13 suivants sont ajoutés: «13. Les États membres veillent à ce qu'en cas d'incident important causé par une attaque par rançongiciel, les entités concernées indiquent, 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, l'autorité compétente: si l'entité a reçu une demande de rançon et, le cas échéant, de qui; si une rançon a été payée et, dans l'affirmative, de quel montant, avec quel moyen de paiement et à quel destinataire, en précisant le crypto-actif et le prestataire de services sur crypto-actifs, le cas échéant.»	États membres de l'UE Entités essentielles et importantes	Rapports	Flux de données

Article 1er, point 10), de la directive Liste des entités et registre (Article 27, paragraphe 1, de la directive SRI 2)	**L'ENISA crée et tient un registre des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine sur la base des informations reçues des points de contact uniques conformément au paragraphe 2.**	ENISA États membres de l'UE (entités essentielles et importantes relevant de la directive SRI 2, entités fournissant des services d'enregistrement de noms de domaine)	L'ENISA crée et tient un registre	Solution numérique Service public numérique
Article 1er, point 11), de la directive Liste des entités et registre (Article 27, paragraphe 4, de la directive SRI 2)	**«4. À la réception des informations visées à l'article 3, paragraphe 4, le point de contact unique de l'État membre concerné les transmet sans retard injustifié à l'ENISA.»**	ENISA États membres de l'UE	Les États membres partagent des informations avec l'ENISA	Flux de données
Article 1er, point 12), de la directive Assistance mutuelle (Article 37 *bis*, paragraphes 1, 2 et 3, de la directive SRI 2)	**1. L'ENISA aide les États membres** à se prêter mutuellement assistance au sens de l'article 37 et **contribue à faciliter ces processus de coopération** pour les entités essentielles et importantes (...). 2. L'ENISA procède à une analyse complète (...). **L'ENISA élabore, en coopération avec** la Commission et le groupe de coopération, une méthode. Le rapport est mis à jour chaque année. 3) L'ENISA formule, le cas échéant, des recommandations, élabore des lignes directrices, aide (...)	ENISA États membres de l'UE Entités importantes et essentielles au sens de la directive SRI 2 Commission européenne	L'ENISA assiste les États membres et contribue à faciliter le processus de coopération. Réalisation d'analyses, de lignes directrices, de méthodes et de rapports.	Traitement des données Flux de données
Article 1er, point 12), de la directive Assistance mutuelle (Article 37 *bis*, paragraphe 4, de la directive SRI 2)	4. Aux fins du paragraphe 4, point e), du présent article, les autorités compétentes **des États membres concernés fournissent, lorsqu'ils sont disponibles, les éléments suivants à l'ENISA** (...).	ENISA États membres de l'UE	Échange d'informations	Flux de données

	5. Lorsqu'un État membre bénéficie de l'assistance mutuelle visée à l'article 37, paragraphe 1, premier alinéa, point c), **le point de contact unique informe l'ENISA** que l'assistance mutuelle a eu lieu.			
Article 119 Exercice de la délégation	3. Aussitôt qu'elle adopte un acte délégué, la Commission **le notifie simultanément** au Parlement européen et au Conseil.	Commission européenne Parlement européen Conseil	Transmission d'informations au PE et au Conseil	Flux de données
Article 120 Évaluation et révision	1. Au plus tard le [JJ MM AAAA], et tous les cinq ans par la suite, la Commission commande une évaluation des performances de l'ENISA au regard de ses objectifs, de son mandat, de sa mission, de ses tâches, de sa gouvernance et de sa localisation, conformément aux lignes directrices de la Commission. 5. La Commission fait rapport des conclusions de l'évaluation au Parlement européen, au Conseil et au conseil d'administration. Les résultats de l'évaluation sont rendus publics.	ENISA Commission Grand public	Collecte et analyse de données; Mise à la disposition des informations au public	Traitement des données Flux de données

4.2. Données

Description générale des données relevant du champ d'application et de toute norme/spécification connexe

Type de données	**Référence(s) à l'exigence**	**Norme et/ou spécification (le cas échéant)**

Données liées aux analyses/rapports présentant un intérêt pour la résilience en matière de cybersécurité et la société	**Article 5, paragraphe 1, points a), b), c), e), f) et h)** **Article 5, paragraphes 2, 3 et 4** **Article 6** **Article 7** **Article 8** **Article 9** **Article 10** **Article 11, paragraphe 2, points b) et c)** **Article 12, paragraphe 4** **Article 15** **Article 1er, point 7), de la directive**	Dans l'exercice des activités énumérées à l'article 11, paragraphe 1, points a) à e), et paragraphe 2, l'ENISA utilise ses propres analyses et, le cas échéant, les informations reçues dans l'exercice de ses fonctions, y compris: a) les informations fournies dans des sources accessibles au public, y compris les vulnérabilités notoirement connues des produits TIC ou services TIC disponibles dans la base de données européenne des vulnérabilités établie conformément à l'article 12, paragraphe 2, de la directive (UE) 2022/2555; b) les informations partagées par les États membres, les entités de l'Union, le CERT-UE, les partenaires du secteur privé ou non gouvernementaux et les pays tiers et les organisations internationales, sous réserve d'éventuelles limitations de la diffusion ultérieure de ces informations, indiquées au moyen d'un marquage visible. L'ENISA publie des lignes directrices concernant l'interopérabilité transfrontière des réseaux et des systèmes d'information utilisés pour le partage d'informations, y compris en ce qui concerne les cyberpôles transfrontières visés à l'article 6, paragraphe 3, du règlement (UE) 2025/38.
Données pertinentes pour la coopération opérationnelle et l'appréciation de la situation	**Article 10, paragraphe 4, points a) à g)** **Article 10, paragraphe 6** **Article 11, paragraphe 1, points a) à g)** **Article 11, paragraphe 2, points a), b) et c)** **Article 11, paragraphe 3**	**Normes en matière de confidentialité et de traitement des informations sensibles** Dans l'exercice des activités énumérées à l'article 11, paragraphe 1, points a) à e), et paragraphe 2, l'ENISA utilise ses propres analyses et, le cas échéant, les informations reçues dans l'exercice de ses fonctions, y compris: a) les informations fournies dans des sources accessibles au public, y compris les vulnérabilités notoires des produits TIC ou services TIC disponibles dans la base de données européenne des vulnérabilités établie conformément à l'article 12, paragraphe 2,

	Article 11, paragraphe 4 **Article 13, paragraphe 2** **Article 15** **Article 16, paragraphe 2, point e)**	de la directive (UE) 2022/2555; b) les informations partagées par les États membres, les entités de l'Union, le CERT-UE, les partenaires du secteur privé ou non gouvernementaux et les pays tiers et les organisations internationales, sous réserve d'éventuelles limitations de la diffusion ultérieure de ces informations, indiquées au moyen d'un marquage visible.
Données pertinentes pour les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité et l'autorisation des fournisseurs **Données pertinentes au regard des objectifs, de la finalité et du contenu des schémas européens de certification de cybersécurité**	**Article 17** **Article 18** **Articles 19 à 23** **Articles 72, 73, 74, 75, 76, 77, 79, 81, 83 et 84**	Un schéma européen individuel d'attestation de compétences en matière de cybersécurité comprend (...): les règles relatives à la conservation des archives par les fournisseurs d'attestations agréés; Les fournisseurs agréés veillent à ce que, à la demande de la personne, les versions électroniques d'attestations individuelles européennes de compétences en matière de cybersécurité soient délivrées sous la forme d'attestations électroniques d'attributs dans un format pouvant être stocké dans les portefeuilles européens d'identité numérique prévus par le règlement (UE) nº 910/2014. . La Commission et l'ENISA devraient suivre les dispositions pertinentes de la législation de l'Union lorsqu'elles établissent un schéma européen de certification de cybersécurité pour ce qui concerne les données.
Données relatives à la gouvernance du cadre européen de certification de cybersécurité	**Articles 85, 86, 88, 89, 90, 92, 93, 94, 95, 96 et 97**	L'ENISA, les organismes d'évaluation de la conformité et les autorités nationales de certification de cybersécurité devraient garantir la confidentialité des données et suivre les dispositions d'un schéma pertinent faisant référence à des normes internationales qui précisent les exigences.
Données présentant un intérêt pour les fonctions internes de l'ENISA	**Article 25** **Article 28,**	**Modèles et lignes directrices concernant le règlement financier; Lignes directrices internes**

(budget, document unique de programmation, stratégies internes)	**paragraphe 1 Article 30 Article 31, paragraphe 8 Article 32, paragraphes 3 et 5 Article 35, paragraphes 5 et 6 Articles 36 à 43 Article 44 Article 45 Article 47, paragraphe 10 Articles 48 à 49 Article 52, article 58**	
Données à caractère personnel	**Article 22 Titre II, chapitre III, section 6 Chambre de recours Article 66 Article 80, paragraphe 1, point c) x) Article 81, paragraphe 2 article 88 paragraphe 6, point h) Article 95 Article 96**	**Règlement (UE) 2018/1725 Règlement (UE) 2016/679**

Données recueillies et analysées dans le cadre de la réalisation d'évaluations coordonnées des risques, de l'élaboration de scénarios de risque et de l'identification des actifs de TIC essentiels	**Article 98** **Article 99** **Article 102** **Article 103** **Article 105**	Sans préjudice de l'article 13 du règlement (UE) 2024/2847 et de l'article 21 de la directive (UE) 2022/2555
Données relatives aux pays tiers/entités de pays tiers	**Article 100, paragraphes 1, 3 et 4** **Article 104** **Article 105** **Article 107** **Article 113**	s.o.
Données relatives aux autorités nationales	**Article 112** **Article 114** **Article 116**	s.o.
Données pertinentes pour les évaluations des risques	**Article 5, paragraphe 2**	**Normes en matière de confidentialité et de traitement des informations sensibles**
Assistance mutuelle entre États membres	**Article 5, paragraphe 1, point g), du règlement et article 1er, point 12), de la directive**	/

Alignement sur la stratégie européenne pour les données

Expliquer comment les exigences sont alignées sur la stratégie européenne pour les données

Les exigences incluses dans la proposition de règlement sur la cybersécurité 2 sont alignées sans incidence spécifique en ce qui concerne la stratégie européenne pour les données.

Alignement sur le principe «une fois pour toutes»

Expliquer comment le principe «une fois pour toutes» a été pris en considération et de quelle manière la possibilité de réutiliser des données existantes a été étudiée

L'un des objectifs de la proposition est de maximiser les efforts de simplification de la Commission et de réduire la charge administrative pour les États membres et les parties prenantes. Ces dernières années, l'ENISA est devenue une plateforme d'information qui détient des informations provenant de différentes sources. En ce sens, bon nombre des tâches de l'ENISA sont liées à la réutilisation et au recyclage des informations aux fins de diverses analyses. Par exemple: à certaines fins, l'ENISA réutilise les informations notifiées conformément aux articles 23 et 30 de la directive (UE) 2022/2555, et notifiées, partagées ou analysées conformément à l'article 14, paragraphes 1 à 3, à l'article 15 et à l'article 17, paragraphes 1 et 3, du règlement (UE) 2024/2847. Les dispositions du cadre relatif à la chaîne d'approvisionnement supposent que la mise en œuvre de ce cadre est étayée par les données reçues au titre de l'article 22 de la directive (UE) 2022/2555, ce qui démontre la réutilisation des informations et la coordination.

Expliquer comment les données nouvellement créées sont faciles à trouver, accessibles, interopérables et réutilisables, et répondent à des normes de qualité élevée

La proposition législative indique explicitement quand les données devraient être mises à la disposition du public. La proposition tient compte de la nature des dispositions qui ont des aspects strictement liés à la sécurité et à la confidentialité et, par conséquent, toutes les données créées au titre de la nouvelle version du règlement sur la cybersécurité ne seront pas destinées à la consommation publique. Pour les dispositions nécessaires, l'alignement sur le portefeuille européen d'identité numérique a été assuré. L'ENISA est chargée de proposer un service d'alerte précoce dans un format lisible par machine.

Flux de données

Description générale des données relevant du champ d'application et de toute norme/spécification connexe

Type de données	**Expliquer le flux de données**	**Références**
L'ENISA fournit des rapports et des analyses, des orientations techniques et des bonnes pratiques.	Il s'agit d'un flux de données destiné aux parties prenantes de l'ENISA, qui facilite la mise en œuvre de la politique et de la législation de l'Union. Dans ces flux de données, l'ENISA recueille des informations, la plupart du temps par l'intermédiaire de sources publiques, effectue des analyses et partage les résultats avec ses parties prenantes. L'ENISA exécute également certaines tâches à la demande de la Commission.	Article 5, paragraphe 1, points a), b), c), e), f) et h) Article 5, paragraphe 2; Article 5, paragraphe 3; Article 5, paragraphe 5 Article 6 Article 7 Article 8 Article 9 Article 10 Article 11, paragraphe 2 Article 11, paragraphe 4 Article 14
Flux de données entre la Commission, l'ENISA, les États membres et d'autres acteurs concernés au sein de l'écosystème de cybersécurité de l'Union, au sens de la coopération opérationnelle.	Les flux de données de ce type sont mis en place aux fins de la coopération opérationnelle et de l'appréciation de la situation. L'échange d'informations se fait dans les deux sens (entrant et sortant). L'échange porte sur des données opérationnelles.	Article 10, paragraphe 4, points a) à g) Article 11, paragraphe 1, points b) à g) Article 11, paragraphe 2, points a) et b) Article 11, paragraphe 3 Article 15 Article 16, paragraphe 2, point e)
Flux de données mis en place pour soutenir l'ECSF et les schémas européens individuels d'attestation de compétences en matière de cybersécurité ainsi que leur mise en œuvre	Ces flux de données facilitent les échanges entrants et sortants pour: – la maintenance et l'adoption de l'ECSF, avec des flux entre l'ENISA et les membres de son groupe de travail ad hoc et entre l'ENISA et la Commission; – l'élaboration et la maintenance de programmes d'attestation individuelle européenne des	Articles 19 à 23 Articles 36 à 43

	compétences en matière de cybersécurité, avec des flux entre l'ENISA et les membres de son groupe de travail ad hoc ainsi qu'entre l'ENISA, la Commission et les États membres; – la mise en œuvre de programmes d'attestation individuelle européenne des compétences en matière de cybersécurité avec des flux de données entre les demandeurs et l'ENISA; – des flux de données entre la chambre de recours, l'ENISA, la Commission et les demandeurs.	
Données pertinentes au regard des objectifs, de la finalité et du contenu des schémas européens de certification de cybersécurité	Les flux de données de ce type sont pertinents pour la planification, la demande, l'élaboration, l'adoption et la maintenance (y compris la révision éventuelle) des schémas européens de certification de cybersécurité. Ils sont notamment liés à l'implication et aux conseils d'experts des parties prenantes, de l'ENISA et des autorités des États membres par l'intermédiaire du GECC à différents stades de la procédure. En outre, des flux de données supplémentaires concernent la fourniture d'informations pertinentes au grand public par l'intermédiaire de sites web dédiés de la Commission et de l'ENISA. Enfin, le cadre prévoit la mise à la disposition du public d'informations supplémentaires en matière de cybersécurité par les fabricants ou les fournisseurs de produits TIC, de services TIC ou de processus TIC pour lesquels une déclaration de conformité de l'UE ou un certificat de cybersécurité européen a été délivré par leurs propres moyens.	Article 18 Article 19 Articles 72, 73, 74, 75, 76, 77, 79, 81, 83 et 84

Données relatives à la gouvernance du cadre européen de certification de cybersécurité	Ces flux de données facilitent les échanges entrants et sortants pour: - la coordination et la gestion des schémas européens de certification de cybersécurité; - l'accréditation et l'autorisation des organismes d'évaluation de la conformité ainsi que leur notification ultérieure par l'intermédiaire de la plateforme pertinente et des procédures connexes; – les procédures de recours telles que le droit d'introduire une réclamation, le recours juridictionnel et les procédures de modification	Articles 85, 86, 88, 89, 90, 92, 93, 94, 95 et 96
Flux de données liés aux activités administratives de l'Agence	Flux entre l'ENISA, le conseil d'administration, les États membres et la Commission. Les informations concernent les activités administratives de l'Agence, dans les deux sens. Des informations sont également transmises au Parlement européen dans certains cas (le flux de données qui s'y rapporte est présenté ci-dessous).	Article 25 Article 28, paragraphe 1 Article 30 Article 31, paragraphe 8 Article 32, paragraphes 3 et 5 Article 35, paragraphes 5 et 6 Articles 36 à 43 Article 44 Article 45
Données envoyées au Parlement européen	Flux vers le Parlement européen concernant les activités de l'ENISA et l'exécution de ses tâches; gestion budgétaire et financière, coopération avec les pays tiers et les organisations internationales, audition du candidat au poste de directeur exécutif; questions liées à la certification européenne de cybersécurité	Article 28, paragraphe 1, point f), article 31, paragraphe 8, article 32, paragraphe 3, article 44, paragraphe 3, article 49, paragraphe 6, article 49, paragraphe 9, article 70, paragraphe 5, article 72, paragraphes 4 et 5, article 119, paragraphe 3, Exercice de la délégation, article 120, Évaluation et réexamen
Données envoyées au Conseil de l'UE	Flux vers le Parlement européen concernant les activités de l'ENISA et l'exécution de ses tâches; gestion budgétaire et financière, coopération avec les pays tiers et les organisations internationales,	Article 28, paragraphe 1, point f), article 31, paragraphe 8, article 32, paragraphe 3, article 32, paragraphe 7, article 49, paragraphe 6, article 49, paragraphe 9, article 70, paragraphe 5, article 72, paragraphes 4 et 5, article 119,

	audition du candidat au poste de directeur exécutif; schémas candidats en cours d'élaboration conformément au cadre européen de certification de cybersécurité.	paragraphe 3, Exercice de la délégation, article 120, Évaluation et réexamen
Flux de données liés à l'introduction d'une réclamation	Flux de données servant à traiter les réclamations introduites par des personnes physiques ou morales en rapport avec les certificats de cybersécurité européens délivrés par des autorités nationales de certification de cybersécurité ou en rapport avec les certificats de cybersécurité européens délivrés par des organismes d'évaluation de la conformité conformément à l'article 84, paragraphe 4, ou en rapport avec les déclarations de conformité de l'Union européenne Les personnes physiques et morales ont le droit d'introduire une réclamation auprès de l'émetteur d'un certificat de cybersécurité européen ou, lorsque la réclamation est en rapport avec un certificat de cybersécurité européen délivré par un organisme d'évaluation de la conformité	Article 55, paragraphe 3; Article 88, paragraphe 7, point f); Article 96
Flux de données relatifs aux attaques par rançongiciel	Communication de certaines informations en cas d'attaques par rançongiciel	Article 1er, point 8), de la directive

Type de données	**Référence(s) à l'exigence ou aux exigences**	**Acteurs qui fournissent les données**	**Acteurs recevant les données**	**Déclencheur de l'échange de données**	**Fréquence (le cas échéant)**
Flux de données entre la Commission et les États membres dans le cadre de la réalisation d'évaluations	Article 99 Évaluations des risques pour la	Commission et États membres	États membres (groupe de coopération SRI)	Article 99 Évaluations des risques pour la	s.o.

Type de données	Référence(s) à l'exigence ou aux exigences	Acteurs qui fournissent les données	Acteurs recevant les données	Déclencheur de l'échange de données	Fréquence (le cas échéant)
coordonnées au niveau de l'Union des risques pour la sécurité.	sécurité			sécurité	
Flux de données entre la Commission et le Conseil en ce qui concerne la désignation de pays tiers en tant que pays suscitant des préoccupations en matière de cybersécurité	Article 100 Désignation de pays tiers suscitant des préoccupations en matière de cybersécurité	Commission	Conseil	Article 100 Vérification par la Commission de la menace représentée par un pays tiers	
Flux de données entre la Commission et les États membres en ce qui concerne les mesures d'atténuation en cas de circonstances exceptionnelles	Article 103, paragraphe 6 Mesures d'atténuation dans les chaînes d'approvisionnement des TIC	Commission	États membres	Circonstances exceptionnelles	s.o.
Flux de données entre la Commission et les fournisseurs et entre la Commission et les autorités compétentes concernant l'évaluation de l'établissement, de la propriété et du contrôle des fournisseurs	Article 104, paragraphes 4, 5 et 6 Recensement des fournisseurs à haut risque	Fournisseurs: Commission Autorités compétentes	Autorités compétentes Fournisseurs: Commission	Actes d'exécution adoptés conformément à l'article 103, paragraphe 1, et en ce qui concerne l'interdiction visée à l'article 111,	s.o.

Type de données	Référence(s) à l'exigence ou aux exigences	Acteurs qui fournissent les données	Acteurs recevant les données	Déclencheur de l'échange de données	Fréquence (le cas échéant)
				paragraphe 1	
Flux de données entre la Commission et les États membres concernant les pouvoirs de supervision liés à la mise en œuvre du cadre de confiance pour la sécurité de la chaîne d'approvisionnement des TIC	Article 112, paragraphes 1 et 4 Autorités compétentes Article 114 Mesures de supervision et d'exécution	États membres	Commission	Article 112, paragraphes 1 et 4 Autorités compétentes Article 114 Mesures de supervision et d'exécution (la Commission, en coopération avec les États membres, publie une liste des entités affiliées à des fournisseurs à haut risque).	s.o.
Flux de données entre la Commission et des tiers pour les exemptions	Article 105 Exemption des entités établies dans des pays tiers suscitant des préoccupations en matière de cybersécurité ou	Tiers [entités établies dans un pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlées par des entités	Commission (lors de la réception de la demande d'exemption) Tiers [entités établies dans un pays tiers	Décision au titre de l'article 100 Désignation des pays tiers suscitant des préoccupations en matière de cybersécurité	s.o.

Type de données	Référence(s) à l'exigence ou aux exigences	Acteurs qui fournissent les données	Acteurs recevant les données	Déclencheur de l'échange de données	Fréquence (le cas échéant)
	contrôlées depuis de tels pays	provenant de tels pays (au sens de l'article 100)] (lors de l'introduction d'une demande d'exemption)] Commission européenne (lors de l'adoption de décisions)	suscitant des préoccupations en matière de cybersécurité ou contrôlées par des entités provenant de tels pays (au sens de l'article 100)] (lors de la réception de la décision de la Commission)]		
Flux de données entre des États membres et des tiers concernant les interdictions dans les réseaux de communications électroniques	Article 111 Interdictions applicables aux réseaux de communications électroniques mobiles, fixes et par satellite	États membres (autorités compétentes)	Tiers (fournisseurs de réseaux de communications électroniques mobiles, fixes et par satellite)	L'autorité compétente désignée en vertu du présent règlement informe sans délai l'autorité compétente conformément au règlement (UE) XX/XXXX [proposition de règlement sur les	s.o.

Type de données	Référence(s) à l'exigence ou aux exigences	Acteurs qui fournissent les données	Acteurs recevant les données	Déclencheur de l'échange de données	Fréquence (le cas échéant)
				réseaux numériques] des mesures imposées aux fournisseurs de réseaux de communications électroniques mobiles, fixes et par satellite.	
Flux de données entre la Commission et les États membres dans le cadre du réseau de services de coopération et de soutien	Article 113 Réseau des services de coopération et de soutien de la Commission	Commission États membres (autorités compétentes)	Commission États membres (autorités compétentes)	Désignation de pays tiers suscitant des préoccupations en matière de cybersécurité	
Flux de données entre des États membres et des tiers concernant les mesures de supervision et d'exécution	Article 114 Mesures de supervision et d'exécution	Tiers (entités du type visé aux annexes I et II de la directive (UE) 2022/2555)	États membres (autorités compétentes)	Mise en œuvre des mesures prévues au titre IV	
Flux de données entre États membres aux fins de l'assistance mutuelle	Article 116 Assistance mutuelle	États membres	États membres	Lorsqu'une entité visée à l'annexe I ou II de la directive (UE) 2022/2555 fournit des services	s.o.

Type de données	Référence(s) à l'exigence ou aux exigences	Acteurs qui fournissent les données	Acteurs recevant les données	Déclencheur de l'échange de données	Fréquence (le cas échéant)
				dans plusieurs États membres, ou fournit des services dans un ou plusieurs États membres alors que ses actifs de TIC essentiels sont situés dans un ou plusieurs autres États membres, les autorités compétentes des États membres concernés coopèrent et se prêtent mutuellement assistance si nécessaire.	

4.3. Solutions numériques

Description générale des solutions numériques

Pour chaque solution numérique, expliquer de quelle manière celle-ci se conforme aux politiques numériques et dispositions législatives applicables

Solution numérique	Référence(s) à l'exigence ou aux exigences	Principales fonctionnalités requises	Organisme responsable	Comment l'accessibilité est-elle prise en compte?	Comment la possibilité de réutilisation est-elle envisagée?	Utilisation des technologies de l'IA (le cas échéant)
L'ENISA assure le **secrétariat du réseau des CSIRT et d'EU-CyCLONe** et déploie, au sein du réseau des CSIRT et d'EU-CyCLONe, des **outils de communication sécurisés** qui sont fournis par des entités juridiques non établies dans des pays tiers ni contrôlées par des pays tiers ou des ressortissants de pays tiers.	Article 10, paragraphes 2, 3 et 5	Informations non publiques.	ENISA	Informations non publiques.	Informations non publiques.	Informations non publiques.
Mettre au point, en coopération avec EU-CyCLONe, le réseau des CSIRT, la Commission, Europol, le CERT-UE et les entités de l'Union concernées, des **répertoires de renseignements vérifiés et fiables sur les cybermenaces**, incluant les tendances en matière d'incidents, de tactiques, de techniques et de procédures.	Article 11, paragraphe 1, point a)	répertoires de renseignements vérifiés et fiables sur les cybermenaces, incluant les tendances en matière d'incidents, de tactiques, de techniques et de procédures	ENISA EU-CyCLONe, le réseau des CSIRT, la Commission, Europol, le CERT-UE et les entités concernées de l'Union	s.o.	s.o.	s.o.
L'ENISA **tient à jour un répertoire des enseignements tirés**.	Article 14, paragraphe 2	L'ENISA tient un répertoire des enseignements tirés des exercices et fournit aux États membres et, le cas échéant, aux entités de l'Union des recommandations quant à	ENISA	s.o.	s.o.	s.o.

		la manière dont ils peuvent mettre en œuvre les enseignements tirés de manière efficace et efficiente.				
L'ENISA établit, fournit, exploite, entretient et met à jour, si nécessaire, des outils techniques opérationnels, tels que des **plateformes** relatives à la cybersécurité au niveau de l'Union, notamment la plateforme unique de signalement établie en vertu de l'article 16, paragraphe 1, du règlement (UE) 2024/2847 [et le point d'entrée unique établi en vertu de l'article 23 *bis* de la directive (UE) 2022/2555], ou des outils de tests destinés à faciliter la mise en œuvre des procédures d'évaluation de la conformité conformément à la législation applicable de l'Union.	Article 15	Plateforme unique de signalement Article 16, paragraphe 1, du règlement (UE) 2024/2847 [point d'entrée unique article 23 *bis* de la directive (UE) 2022/2555]	ENISA	s.o.	s.o.	s.o.
Assurer la maintenance de la base de données européenne des vulnérabilités établie conformément à l'article 12, paragraphe 2, du règlement (UE) 2022/2555 et **fournir des services de gestion des vulnérabilités**	Article 16, paragraphe 2	article 12, paragraphe 2, de la directive (UE) 2022/2555 Assurer la maintenance du registre et fournir des services de gestion des vulnérabilités	ENISA	s.o.	s.o.	s.o.
L'ENISA assure la maintenance et la mise à jour régulière d'un site web dédié fournissant des informations publiques	Articles 19 à 23	Assurer la maintenance et la mise à jour régulière d'un site web dédié fournissant des	ENISA	s.o.	s.o.	s.o.

		informations publiques sur l'ECSF, y compris sur le cadre et son calendrier de mise à jour; les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, leur état d'avancement et leur calendrier d'élaboration; les redevances associées à chaque schéma européen individuel d'attestation de compétences en matière de cybersécurité; le coût indicatif d'une attestation individuelle européenne de compétences en matière de cybersécurité; la liste des fournisseurs d'attestations agréés.				
La **Commission assure la maintenance et la mise à jour régulière d'un site web dédié**	Article 72	Suivre les informations: (a) les schémas européens de certification de cybersécurité dont l'élaboration est demandée; (b) les priorités stratégiques pour l'harmonisation des	Commission européenne	Respect des lignes directrices	Respect des lignes directrices	s.o.

		produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou des exigences de sécurité de la législation de l'Union, y compris les domaines potentiels pour lesquels un schéma européen de certification de cybersécurité pourrait être demandé.				
L'ENISA tient à jour un site internet dédié	Article 79	Fournir des informations sur: a) les schémas européens de certification de cybersécurité; b) les redevances liées à la maintenance de chaque schéma européen de certification de cybersécurité; c) les spécifications techniques pertinentes de l'ENISA; d) les certificats de cybersécurité européens et les déclarations de conformité de l'UE, y compris des informations	ENISA	Respect des lignes directrices	Respect des lignes directrices	s.o.

		sur les certificats et déclarations qui ne sont plus valables, qui ont été suspendus ou retirés ou qui ont expiré; e) des informations supplémentaires pertinentes sur la cybersécurité, fournies conformément à l'article 84, paragraphe 2; f) des résumés des examens par les pairs visés à l'article 89, paragraphe 7; g) les spécifications techniques mentionnées dans un schéma européen de certification de cybersécurité conformément à l'article 74, paragraphe 10.				
Registre (des exemptions d'entités établies dans des pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlées par des entités de tels pays)	Article 107 Registre	La Commission tient un registre accessible au public reprenant ses décisions visées à l'article 105, paragraphe 4. Ce registre	Commission	«La Commission tient un registre accessible au public.»	s.o.	s.o.

		indique le nom des entités ayant fait l'objet des décisions. La Commission le met régulièrement à jour.				
Plateforme (pour la coopération et l'échange d'informations entre la Commission et les autorités compétentes)	Article 113	La Commission met en place un réseau de coopération entre les autorités compétentes des États membres et elle-même, qui sert de plateforme de coopération et d'échange d'informations. La Commission se charge d'apporter le soutien administratif à ce réseau.	Commission	Non public, uniquement pour les autorités compétentes	s.o.	s.o.
L'ENISA crée et tient un registre des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine	Article 1er, point 11), de la directive	Registre des entités essentielles et importantes et des entités fournissant des services d'enregistrement de noms	ENISA	s.o.	Sur la base des informations reçues des points de	s.o.

		de domaine			contact uniques conformément au paragraphe 2 (article 27 de la directive SRI 2)	

Solutions numériques incluses dans le tableau ci-dessus

Politique numérique et/ou sectorielle (le cas échéant)	**Expliquer de quelle manière la solution s'aligne sur l'élément en question**
Règlement sur l'IA	s.o.
Cadre de l'UE en matière de cybersécurité	s.o.
eIDAS	s.o.
Portail numérique unique et IMI	s.o.
Autres	s.o.

Description générale du (des) service(s) public(s) numérique(s) concerné(s) par les exigences

Service public numérique ou catégorie de services publics numériques	**Description**	**Référence(s) à l'exigence ou aux exigences**	**Solution(s) interopérable(s) pour l'Europe (SANS OBJET)**	**Autre(s) solution(s) d'interopérabilité**
L'ENISA, en tant que	L'ENISA assure le secrétariat du	Article 11	//	s.o.

secrétariat des réseaux et agence déployant des outils de communication sécurisés	réseau des CSIRT conformément à l'article 15, paragraphe 2, de la directive (UE) 2022/2555. L'ENISA assure le secrétariat d'EU-CyCLONe conformément à l'article 16, paragraphe 2, de la directive (UE) 2022/2555 [et du point d'entrée unique pour la notification des incidents établi en vertu de l'article 23 *bis* de la directive (UE) 2022/2555] et des outils de tests destinés à faciliter la mise en œuvre des procédures d'évaluation de la conformité conformément à la législation applicable de l'Union. L'ENISA déploie, au sein du réseau des CSIRT et d'EU-CyCLONe, des outils de communication sécurisés qui sont fournis par des entités juridiques non établies dans des pays tiers ni contrôlées par des pays tiers ou des ressortissants de pays tiers.			
Alertes précoces	Émission d'alertes précoces	Article 11 Article 12		
Soutien concernant un incident ou une cybermenace spécifique potentielle ou existante	À la demande d'un ou plusieurs États membres, fournir des conseils et des évaluations concernant un incident ou une cybermenace spécifique potentielle ou existante, y compris en fournissant une expertise et en facilitant la gestion technique de tels incidents, et en soutenant le partage volontaire d'informations et de solutions techniques pertinentes entre États membres.	Article 10		
Appui à la gestion coordonnée des	Contribuer à soutenir la gestion coordonnée des incidents et crises de	Article 10		

incidents de cybersécurité majeurs et des crises au niveau opérationnel	cybersécurité majeurs au niveau opérationnel, notamment en aidant EU-CyCLONe à préparer des rapports au niveau politique en facilitant le partage d'informations en temps utile entre le réseau des CSIRT et EU-CyCLONe.			
Répertoires de renseignements vérifiés et fiables sur les cybermenaces	Mettre au point, en coopération avec EU-CyCLONe, le réseau des CSIRT, la Commission, Europol, le CERT-UE et les entités de l'Union concernées, des répertoires de renseignements vérifiés et fiables sur les cybermenaces, incluant les tendances en matière d'incidents, de tactiques, de techniques et de procédures.	Article 11		
Répertoire des enseignements tirés	L'ENISA tient un répertoire des enseignements tirés de ces exercices et fournit aux États membres et, le cas échéant, aux entités de l'Union des recommandations quant à la manière dont ils peuvent mettre en œuvre les enseignements tirés de manière efficace et efficiente.	Article 14		
L'ENISA établit, fournit, exploite, entretient et met à jour, si nécessaire, des outils techniques opérationnels, tels que des plateformes	L'ENISA établit, fournit, exploite, entretient et met à jour, si nécessaire, des outils techniques opérationnels, tels que des plateformes relatives à la cybersécurité au niveau de l'Union, notamment la plateforme unique de signalement établie en vertu de l'article 16, paragraphe 1, du règlement (UE) 2024/2847 [et le point d'entrée unique établi en vertu de l'article 23 *bis* de la directive (UE) 2022/2555] et des outils de tests destinés à faciliter la mise en œuvre	Article 15		

	des procédures d'évaluation de la conformité conformément à la législation applicable de l'Union.			
Assurer la maintenance de la base de données européenne des vulnérabilités établie conformément à l'article 12, paragraphe 2, du règlement (UE) 2022/2555	Assurer la maintenance de la base de données européenne des vulnérabilités établie conformément à l'article 12, paragraphe 2, du règlement (UE) 2022/2555. Fournir des services de gestion des vulnérabilités aux parties prenantes, en s'appuyant sur la base de données européenne des vulnérabilités et en utilisant les informations pertinentes dont dispose l'ENISA. Nouer une coopération structurée avec des organisations fournissant des programmes, des registres ou des bases de données similaires à la base de données européenne des vulnérabilités. Soutenir activement les **CSIRT** désignés comme coordinateurs conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555 en ce qui concerne la gestion de la divulgation coordonnée des vulnérabilités susceptibles d'avoir un impact important sur des entités de plusieurs États membres. Élaborer et assurer la maintenance de méthodes et des mécanismes de gouvernance pour la détection des vulnérabilités et la divulgation coordonnée, en coopération avec les autorités nationales compétentes, les CSIRT, l'industrie et la communauté des chercheurs.	Article 16		

Préparer des schémas européens de certification de cybersécurité candidats («schémas candidats»)	a) préparer des schémas européens de certification de cybersécurité candidats (ci-après les «schémas candidats») pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités et les spécifications techniques connexes conformément à l'article 74. Assurer la maintenance des schémas européens de certification de cybersécurité adoptés conformément à l'article 75, y compris en vue de leur éventuel réexamen conformément à l'article 76.	Article 17		
L'ENISA élabore des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité et en assure la maintenance	L'ENISA élabore des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité et en assure la maintenance. L'ENISA adopte une décision motivée autorisant le demandeur à délivrer des attestations individuelles européennes pour la fourniture et la maintenance des programmes et de l'agrément, refusant l'agrément ou clôturant le traitement de la demande si le demandeur n'a pas fourni suffisamment d'informations ou n'a pas répondu à une demande d'informations supplémentaires.	Articles 20 à 22		
L'ENISA assure la maintenance et la mise à jour régulière d'un site web dédié.	L'ENISA assure la maintenance et la mise à jour régulière d'un site web dédié fournissant des informations publiques sur:	Article 23		

	(a) l'ECSF, y compris le cadre et son calendrier de mise à jour; (b) les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité, leur état d'avancement et leur calendrier d'élaboration; (c) les redevances associées à chaque schéma européen individuel d'attestation de compétences en matière de cybersécurité adopté en vertu de l'article 47 du présent règlement; (d) le coût indicatif d'une attestation individuelle européenne de compétences en matière de cybersécurité conformément à l'article 20, paragraphe 4; e) la liste des fournisseurs d'attestations agréés.			
La Commission assure la maintenance et la mise à jour régulière d'un site web dédié	La Commission assure la maintenance et la mise à jour régulière d'un site web dédié fournissant des informations sur les aspects suivants: a) les schémas européens de certification de cybersécurité dont l'élaboration est demandée; b) les priorités stratégiques pour l'harmonisation des produits TIC, des services TIC, des processus TIC, des services de sécurité gérés ou des exigences de sécurité de la législation de l'Union, y compris les domaines potentiels pour lesquels un schéma européen de certification de cybersécurité pourrait être demandé.	Article 72		
L'ENISA tient à jour un site internet dédié	L'ENISA assure la maintenance et la mise à jour régulière d'un site web	Article 79		

	dédié fournissant des informations publiques sur: a) Systèmes européens de certification de cybersécurité; b) les redevances liées à la maintenance de chaque schéma européen de certification de cybersécurité; c) les spécifications techniques pertinentes de l'ENISA; d) les certificats de cybersécurité européens et les déclarations de conformité de l'UE, y compris des informations sur les certificats et déclarations qui ne sont plus valables, qui ont été suspendus ou retirés ou qui ont expiré; e) des informations supplémentaires pertinentes sur la cybersécurité, fournies conformément à l'article 84, paragraphe 2; f) des résumés des examens par les pairs visés à l'article 89, paragraphe 7; g) les spécifications techniques mentionnées dans un schéma européen de certification de cybersécurité conformément à l'article 74, paragraphe 10.			
Enquêtes	La Commission enquête sur tous les cas dans lesquels elle nourrit des doutes ou est avertie de doutes quant à la compétence d'un organisme d'évaluation de la conformité pour remplir les exigences qui lui sont applicables et s'acquitter des responsabilités qui lui incombent, ou quant au fait qu'il continue à remplir ces exigences et à s'acquitter de ces	Article 94		

	responsabilités. La Commission veille à ce que toutes les informations sensibles obtenues au cours de ses enquêtes soient traitées de manière confidentielle.			
L'ENISA crée et tient un registre des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine	Registre des entités essentielles et importantes et des entités fournissant des services d'enregistrement de noms de domaine. L'ENISA autorise les autorités compétentes, à leur demande, à accéder aux informations relatives aux fournisseurs de services DNS, aux registres des noms de domaine de premier niveau, aux entités qui fournissent des services d'enregistrement de noms de domaine, aux fournisseurs de services d'informatique en nuage, aux fournisseurs de services de centres de données, aux fournisseurs de réseaux de diffusion de contenu, aux fournisseurs de services gérés, aux fournisseurs de services de sécurité gérés, ainsi qu'aux fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux enregistrées dans ce répertoire, tout en veillant, le cas échéant, à la protection de la confidentialité des informations.	Article 1er, point 11), de la directive		

4.4. Évaluation de l'interopérabilité

Incidence de l'exigence ou des exigences sur l'interopérabilité transfrontière pour chaque service public numérique

Registres/plateformes/alertes précoces/secrétariat/coopération opérationnelle/base de données sur la divulgation coordonnée des vulnérabilités

Évaluation	Mesures	Obstacles potentiels restants
Évaluer l'alignement sur les politiques numériques et sectorielles existantes **Énumérer les politiques numériques et sectorielles applicables recensées**	*Cybersécurité*	*Pas d'obstacles connus*
Évaluer les mesures organisationnelles en faveur d'une fourniture transfrontière sans heurts de services publics numériques **Énumérer les mesures de gouvernance prévues**	*Conseil d'administration de l'ENISA* *Réseau des CSIRT* *Réseau UE-CyCLONe* *Groupe de coopération SRI* *Tous ces endroits sont des enceintes dans lesquelles des questions peuvent être soulevées.*	*s.o.*
Évaluer les mesures prises pour garantir une compréhension commune des données **Énumérer ces mesures**	*s.o.*	*s.o.*
Évaluer l'utilisation de spécifications et de normes techniques ouvertes convenues d'un commun accord **Énumérer ces mesures**	*s.o.*	*s.o.*

Schémas européens individuels d'attestation de compétences en matière de cybersécurité

Évaluation	Mesures	Obstacles potentiels restants
Évaluer l'alignement sur les politiques numériques et sectorielles existantes **Énumérer les politiques numériques et sectorielles applicables recensées**	*La proposition s'appuie sur la communication COM(2023) 207 final (L'académie des compétences en matière de cybersécurité): «l'ENISA mettra au point un projet pilote afin d'étudier la mise en place d'un système*	*Pas d'obstacles connus*

	européen d'attestation des compétences en matière de cybersécurité». *Elle fait usage du règlement (UE) 2024/1183 (portefeuille européen d'identité numérique) en disposant que «l'ENISA et les fournisseurs d'attestations agréés veillent à ce que les versions électroniques de l'attestation individuelle européenne de compétences en matière de cybersécurité soient délivrées aux portefeuilles européens d'identité numérique».* *Cybersécurité* *RGPD (conservation des enregistrements par les fournisseurs)*	
Évaluer les mesures organisationnelles en faveur d'une fourniture transfrontière sans heurts de services publics numériques **Énumérer les mesures de gouvernance prévues**	*Consultation des parties prenantes lors de l'élaboration d'un schéma européen individuel d'attestation de compétences en matière de cybersécurité* *Séparation des activités au sein de l'ENISA afin d'assurer leur exécution indépendante* *Chambre de recours*	*L'utilisation et la reconnaissance des programmes d'attestation individuelle européenne des compétences en matière de cybersécurité restent facultatives pour les entités publiques et privées.*
Évaluer les mesures prises pour garantir une compréhension commune des données **Énumérer ces mesures**	*Élaborer des schémas détaillant, entre autres, les règles relatives au contenu et au format des attestations* *Les fournisseurs agréés veillent à ce que, à la demande de la personne, les versions électroniques d'attestations individuelles européennes de compétences en matière de cybersécurité soient délivrées sous la forme d'attestations électroniques d'attributs dans un format pouvant être stocké dans les portefeuilles européens d'identité numérique.*	*Les programmes devraient être aussi détaillés que possible pour en garantir une compréhension commune et en faciliter la mise en œuvre, et l'ENISA fournira des orientations aux évaluateurs et leur dispensera une formation obligatoire pour que la mise en œuvre des programmes soit cohérente, mais des circonstances imprévues peuvent survenir, dans lesquelles les fournisseurs d'attestations agréés doivent interagir avec l'ENISA, avec d'autres fournisseurs ou avec les évaluateurs.*

	L'ENISA fournit des orientations aux évaluateurs et leur dispense une formation obligatoire sur les exigences et les méthodes d'évaluation figurant dans le programme d'attestation individuelle européenne des compétences en matière de cybersécurité *Mise à disposition d'informations publiques sur un site web* *Actes d'exécution concernant les redevances*	
Évaluer l'utilisation de spécifications et de normes techniques ouvertes convenues d'un commun accord **Énumérer ces mesures**	*Les programmes d'attestation individuelle européenne des compétences en matière de cybersécurité sont élaborés avec le soutien des parties prenantes concernées*	*s.o.*

Préparation de schémas européens de certification de cybersécurité candidats («schémas candidats»)/attribution de numéros aux organismes d'évaluation de la conformité

Évaluation	**Mesures**	**Obstacles potentiels restants**
Évaluer l'alignement sur les politiques numériques et sectorielles existantes **Énumérer les politiques numériques et sectorielles applicables recensées**	*La proposition vise à aligner la gouvernance sur le nouveau cadre législatif, en particulier en ce qui concerne le règlement (CE) nº 765/2008*[26]*.* *La proposition vise à faciliter le respect de la législation sectorielle pertinente en matière de cybersécurité grâce à l'élaboration de schémas européens de certification de cybersécurité spécifiques.*	*Pas d'obstacles connus*
Évaluer les mesures organisationnelles en faveur d'une fourniture transfrontière sans heurts	*Groupe européen de certification de cybersécurité;* *ENISA;*	*L'utilisation de la certification européenne de cybersécurité est facultative, sauf disposition contraire*

de services publics numériques **Énumérer les mesures de gouvernance prévues**	*Groupes de travail ad hoc;* *assemblée européenne pour la certification de cybersécurité;* *consultation des parties prenantes lors de la demande, de l'élaboration et de l'adoption de schémas européens de certification de cybersécurité;* *procédures de comitologie pour les actes d'exécution envisagés relatifs aux schémas européens de certification de cybersécurité.*	*de la législation européenne.*
Évaluer les mesures prises pour garantir une compréhension commune des données **Énumérer ces mesures**	*Actes d'exécution énumérés à la section 4.5.*	*L'utilisation de la certification européenne de cybersécurité est facultative, sauf disposition contraire de la législation européenne.*
Évaluer l'utilisation de spécifications et de normes techniques ouvertes convenues d'un commun accord **Énumérer ces mesures**	*Actes d'exécution énumérés à la section 4.5.* *Les exigences du schéma européen de certification de cybersécurité qui ont été définies sont des exigences cohérentes de la législation de l'Union.* *Les schémas européens de certification de cybersécurité utilisent et mentionnent les normes internationales, européennes ou nationales appliquées lors de l'évaluation ou, lorsque ces normes ne sont pas disponibles ou appropriées, les spécifications techniques élaborées par l'ENISA.*	*s.o.*

Sites web accessibles au public

Évaluation	**Mesures**	**Obstacles potentiels restants**
Évaluer l'alignement sur les politiques numériques et sectorielles existantes **Énumérer les politiques numériques**	*Acte législatif de l'Union sur l'accessibilité et directive sur l'accessibilité du web* *Cybersécurité*	*Pas d'obstacles connus*

et sectorielles applicables recensées		
Évaluer les mesures organisationnelles en faveur d'une fourniture transfrontière sans heurts de services publics numériques Énumérer les mesures de gouvernance prévues	*s.o.*	*s.o.*
Évaluer les mesures prises pour garantir une compréhension commune des données Énumérer ces mesures		*s.o.*
Évaluer l'utilisation de spécifications et de normes techniques ouvertes convenues d'un commun accord Énumérer ces mesures		*s.o.*

4.5. Mesures de soutien de la mise en œuvre numérique

Description générale des mesures de soutien de la mise en œuvre numérique

Description de la mesure	**Référence(s) à l'exigence ou aux exigences**	**Rôle de la Commission** (le cas échéant)	**Acteurs à associer** (le cas échéant)	**Calendrier prévu** (le cas échéant)
La Commission est habilitée à adopter, sur la base du schéma candidat préparé par l'ENISA, des actes d'exécution prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, les services TIC, les processus TIC, les services de sécurité gérés ou la posture de cybersécurité des entités qui satisfont aux exigences énoncées aux articles 80 et 81.	Article 75, paragraphe 9	La Commission est habilitée à adopter des actes d'exécution		s.o.

Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.				
La Commission est habilitée à adopter des actes délégués conformément à l'article 119 afin de modifier le paragraphe 1 du présent article en ajoutant ou en modifiant des objectifs de sécurité afin de veiller à ce qu'ils reflètent les dernières évolutions technologiques et les nouvelles menaces connexes, ainsi qu'à adopter de nouveaux actes législatifs de l'Union établissant la présomption de conformité, au moyen de la certification européenne de cybersécurité, avec les exigences pertinentes desdits actes.	Article 80, paragraphe 2	La Commission est habilitée à adopter des actes d'exécution		s.o.
La Commission est habilitée à adopter des actes d'exécution établissant des principes communs et des dispositions types pour les éléments énoncés aux paragraphes 1, 2 et 3 dans l'ensemble des schémas européens de certification de cybersécurité. Un schéma européen de certification de cybersécurité peut inclure des références à ces principes et dispositions types, le cas échéant et lorsqu'elles sont disponibles. Les actes d'exécution visés au premier alinéa sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2. Lors de l'élaboration ou de la révision des principes communs et des	Article 81, paragraphe 5	La Commission est habilitée à adopter des actes d'exécution	ENISA GECC	s.o.

dispositions types pour les éléments des schémas européens de certification de cybersécurité, la Commission consulte l'ENISA et tient compte, le cas échéant, des points de vue exprimés par le GECC, les parties prenantes concernées et d'autres organismes pertinents.				
La Commission est habilitée à adopter des actes d'exécution précisant les procédures pour les modèles d'approbation préalable ou de délégation générale visés au paragraphe 4 du présent article. Dans le cadre du processus d'élaboration de ces actes d'exécution, la Commission consulte le GECC. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.	Article 85, paragraphe 5	La Commission est habilitée à adopter des actes d'exécution	GECC	s.o.
Les certificats de produits TIC, de services TIC, de processus TIC, de services de sécurité gérés et de postures de cybersécurité d'entités délivrés dans des pays tiers peuvent être reconnus, au moyen d'un acte d'exécution ou par la conclusion d'un accord entre l'Union et le pays tiers en question ou une organisation internationale, comme étant équivalents aux certificats de cybersécurité européens si les exigences du schéma du pays tiers en question ou de l'organisation internationale pertinente sont considérées comme équivalentes à celles	Article 87, paragraphe 1	La Commission est habilitée à adopter des actes d'exécution		s.o.

des schémas européens de certification de cybersécurité. La Commission est habilitée à adopter de tels actes d'exécution. L'acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.				
La Commission est habilitée à adopter des actes d'exécution établissant un plan pour l'examen par les pairs couvrant une période d'au moins cinq ans et définissant les critères concernant la composition de l'équipe chargée de l'examen par les pairs, la méthode utilisée pour mener cet examen, ainsi que le programme, la fréquence et les autres tâches liées à l'examen par les pairs. Dans le cadre de l'élaboration de ces actes d'exécution, la Commission consulte le GECC et l'ENISA. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.	Article 89, paragraphe 6	La Commission est habilitée à adopter des actes d'exécution		s.o.
La Commission est habilitée à adopter des actes d'exécution pour établir les procédures d'autorisation des organismes d'évaluation de la conformité, y compris en ce qui concerne la coopération transfrontière. Dans le cadre du processus d'élaboration de ces actes d'exécution, la Commission consulte l'ENISA et le GECC. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen	Article 92, paragraphe 8	La Commission est habilitée à adopter des actes d'exécution	ENISA GECC	s.o.

visée à l'article 118, paragraphe 2.				
La Commission est habilitée à adopter des actes d'exécution visant à établir les circonstances, formats et procédures pour les notifications visées au paragraphe 1 du présent article, y compris la procédure d'opposition par d'autres États membres au cours du processus de notification, l'identification unique des organismes d'évaluation de la conformité ainsi que les circonstances dans lesquelles une notification peut être restreinte, suspendue ou retirée. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 118, paragraphe 2.	Article 93, paragraphe 3	La Commission est habilitée à adopter des actes d'exécution		s.o.
La Commission peut adopter des actes d'exécution conformément à l'article 100 afin de désigner un pays tiers comme pays suscitant des préoccupations en matière de cybersécurité pour les chaînes d'approvisionnement des TIC.	Article 100, paragraphe 2 Désignation de pays tiers suscitant des préoccupations en matière de cybersécurité	Adoption d'actes d'exécution		s.o. Pas de calendrier, mais les actes d'exécution devraient être réexaminés régulièrement
La Commission peut adopter des actes d'exécution pour prévoir une ou plusieurs mesures d'atténuation visées à l'article 103, paragraphe 2.	Article 103, paragraphe 2 Mesures d'atténuation dans les chaînes d'approvisionnement des TIC	Adoption d'actes d'exécution	s.o.	s.o. Pas de calendrier, mais réexamen nécessaire tous les 36 mois (conformément à la procédure d'examen visée à l'article 118,

				paragraphe 2)
La Commission peut adopter des actes d'exécution conformément à l'article 102 pour identifier les actifs de TIC essentiels utilisés pour la fabrication de produits ou la fourniture de services par les types d'entités visés aux annexes I et II de la directive (UE) 2022/2555.	Article 102, paragraphe 1 Identification des actifs de TIC essentiels	Adoption d'actes d'exécution	s.o.	s.o.
La Commission peut adopter des actes d'exécution interdisant d'utiliser, d'installer ou d'intégrer, sous quelque forme que ce soit, des composants TIC ou des composants comprenant des composants TIC provenant de fournisseurs à haut risque désignés conformément à l'article 100, paragraphe 2, dans des actifs de TIC essentiels identifiés conformément à l'article 102.	Article 103, paragraphe 1 Mesures d'atténuation dans les chaînes d'approvisionnement des TIC	Adoption d'actes d'exécution	s.o.	s.o.
La Commission peut adopter des actes d'exécution afin d'établir qu'il est interdit aux entités des types visés aux annexes I et II de la directive (UE) 2022/2555 d'utiliser, d'installer ou d'intégrer des composants TIC ou des composants comprenant des composants TIC provenant d'une entité donnée.	Article 103, paragraphe 7	Adoption d'actes d'exécution	Consultation des États membres et des entités concernées	s.o.
La Commission établit, par voie d'actes d'exécution, des listes des fournisseurs à haut risque concernés par les interdictions	Article 104, paragraphe 1	Adoption d'actes d'exécution	s.o.	s.o.

énoncées dans les actes d'exécution adoptés conformément à l'article 103, paragraphe 1 ou par l'interdiction visée à l'article 1110, paragraphe 1.				
La Commission peut adopter des actes d'exécution afin de préciser davantage les conditions visées à l'article 105, paragraphe 2, point b), et d'établir des règles détaillées en ce qui concerne les procédures visées à l'article 105.	Article 105 Exemption des entités établies dans des pays tiers suscitant des préoccupations en matière de cybersécurité ou contrôlées par des entités de tels pays	Adoption d'actes d'exécution	s.o.	s.o.
La Commission peut adopter des actes d'exécution établissant des règles détaillées relatives aux redevances, précisant le montant de celles-ci et leurs modalités de paiement.	Article 109 Redevances	Adoption d'actes d'exécution	s.o.	s.o.
La Commission adopte des actes d'exécution afin de préciser les délais de suppression progressive des composants TIC ou composants qui incluent des composants TIC provenant de fournisseurs à haut risque en ce qui concerne les réseaux de communications électroniques fixes et par satellite.	Article 110, paragraphe 4 Actifs de TIC essentiels pour les réseaux de communications électroniques mobiles, fixes et par satellite	Adoption d'actes d'exécution	s.o.	s.o.
La Commission peut adopter des actes délégués conformément à l'article 119 pour modifier l'annexe II afin de l'adapter aux évolutions technologiques en tenant compte des éléments visés à l'article 103, paragraphe 3.	Article 110, paragraphe 5	Adoption d'actes d'exécution	s.o.	s.o.

7. L'article 21, paragraphe 5 est modifiée comme suit: (a) le deuxième 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 visées 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 visés au présent alinéa doivent être adoptés pour des secteurs ou des types d'entités spécifiques afin d'améliorer le fonctionnement du marché intérieur. Sur la base des résultats de cette évaluation, la Commission peut proposer de tels actes d'exécution pour les secteurs ou types d'entités concernés. Lorsqu'elle prépare cette évaluation, la Commission se concentre en particulier sur la nature transfrontière des secteurs ou des types d'entités et mène un processus de consultation ouvert, transparent et inclusif avec les parties prenantes concernées et les États membres.», (b) l'alinéa suivant est inséré après le quatrième alinéa: «Lorsque la Commission adopte des actes	Article 1er, point 7), de la directive Harmonisation maximale	La Commission peut adopter des actes d'exécution		s.o.

d’exécution visés aux premier et deuxième alinéas du présent paragraphe, les États membres n’imposent aucune exigence technique ou méthodologique supplémentaire concernant les mesures visées à l’article 21, paragraphe 2, de la directive (UE) 2022/2555 aux entités relevant du champ d’application de ces actes d’exécution.»				