COM (2022) 122 final

ASSEMBLÉE NATIONALE
QUINZIÈME LÉGISLATURE

SÉNAT
SESSION ORDINAIRE DE 2021-2022

Reçu à la Présidence de l'Assemblée nationale
le 25 mars 2022

Enregistré à la Présidence du Sénat
le 25 mars 2022

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 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union

E16597

Conseil de
l'Union européenne

Bruxelles, le 22 mars 2022
(OR. en)

7474/22

Dossier interinstitutionnel:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	22 mars 2022
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2022) 122 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union

Les délégations trouveront ci-joint le document COM(2022) 122 final.

p.j.: COM(2022) 122 final

COMMISSION
EUROPÉENNE

Bruxelles, le 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union

{SWD(2022) 67 final} - {SWD(2022) 68 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

La présente proposition établit un cadre destiné à assurer des règles et des mesures communes en matière de cybersécurité au sein des institutions, organes et organismes de l'Union. Elle vise à améliorer la résilience de toutes les entités ainsi que leurs capacités de réaction aux incidents. Elle est conforme aux priorités de la Commission consistant à adapter l'Europe à l'ère du numérique et à bâtir une économie au service des personnes et parée pour l'avenir. En outre, garantir la sûreté et la résilience de l'administration publique est une pierre angulaire de la transformation numérique de la société dans son ensemble.

La présente proposition s'appuie sur la stratégie de l'UE pour l'union de la sécurité [COM(2020) 605 final] et sur la stratégie de cybersécurité de l'UE pour la décennie numérique [JOIN(2020) 18 final].

La proposition modernise le cadre juridique existant de l'équipe d'intervention en cas d'urgence informatique (CERT- UE) et tient compte, d'une part, de l'évolution et de l'intensification de la transformation numérique au sein des institutions, organes et organismes de l'Union ces dernières années et, d'autre part, de l'évolution du paysage des menaces qui pèsent sur la cybersécurité. Ces deux phénomènes se sont amplifiés depuis le début de la crise de la COVID-19, tandis que le nombre d'incidents continue d'augmenter, les attaques devenant de plus en plus sophistiquées et provenant de sources très diverses.

La proposition prévoit que l'«équipe d'intervention en cas d'urgence informatique» (la CERT-UE) sera désormais dénommée «centre pour la cybersécurité» (le CERT-UE») pour les institutions, organes et organismes de l'Union, pour faire écho à l'évolution observée dans les États membres et au niveau mondial, où de nombreuses CERT ont été renommées «centres de cybersécurité». La dénomination abrégée «CERT-UE» est toutefois maintenue en raison de sa notoriété.

• Cohérence avec les dispositions existantes dans le domaine d'action

La présente proposition vise à améliorer la résilience en matière de cybersécurité des institutions, organes et organismes de l'Union face aux menaces informatiques, tout en s'alignant sur la législation existante:

- la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Elle s'aligne aussi sur la proposition de directive (UE) XXXX/XXXX concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 [proposition de directive SRI 2];
- le règlement (UE) 2019/881 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 (règlement sur la cybersécurité);
- la proposition de règlement (UE) XXXX/XXXX relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union;
- la recommandation de la Commission du 23 juin 2021 sur la création d'une unité conjointe de cybersécurité;

- la recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs.

L'annexe de la recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs présente un plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs.

Dans ses conclusions du 9 mars 2021, le Conseil de l'Union européenne a souligné que la cybersécurité est essentielle au fonctionnement de l'administration publique, tant au niveau national qu'au niveau de l'UE, ainsi que pour la société et l'économie dans son ensemble, et a souligné l'importance que revêt un cadre de sécurité solide et cohérent pour protéger l'ensemble du personnel, des données, des réseaux de communication et des systèmes d'information ainsi que des processus décisionnels de l'UE. À cette fin, il convient en particulier d'accroître la résilience et d'améliorer la culture de sécurité des institutions, organes et organismes de l'Union. Il faut veiller à ce que des ressources et des capacités suffisantes soient mises à disposition, y compris dans le cadre du renforcement du mandat du CERT-UE.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La base juridique du présent règlement est l'article 298 du traité sur le fonctionnement de l'Union européenne (TFUE), en vertu duquel, dans l'accomplissement de leurs missions, les institutions, organes et organismes de l'Union s'appuient sur une administration européenne ouverte, efficace et indépendante. Dans le respect du statut et du régime adoptés sur la base de l'article 336, le Parlement européen et le Conseil, statuant par voie de règlements conformément à la procédure législative ordinaire, fixent les dispositions à cet effet.

Les technologies de l'information ont fourni aux institutions, organes et organismes de l'Union de nouveaux moyens de travailler, d'interagir avec les citoyens et d'améliorer leur fonctionnement global. Cependant, le paysage des cybermenaces évolue parallèlement au développement des technologies. Les institutions, organes et organismes de l'Union sont devenus des cibles très attrayantes pour les cyberattaques sophistiquées. La mise en place de systèmes et d'exigences visant à assurer la cybersécurité semble contribuer à l'efficacité et à l'indépendance de l'administration européenne, de sorte que, dans l'accomplissement de leurs missions, les institutions, organes et organismes de l'Union puissent fonctionner de manière plus efficace dans un monde numérique.

En outre, les disparités détaillées à la section 3 ci-dessous, qui existent au sein des institutions, organes et organismes de l'Union en ce qui concerne la posture de cybersécurité et l'approche adoptée dans ce domaine constituent des obstacles supplémentaires à une administration européenne ouverte, efficace et indépendante. En l'absence d'approche commune, les postures de cybersécurité au sein de chaque institution, organe et organisme de l'Union continueraient à évoluer dans des directions divergentes. Cette base juridique est dès lors appropriée étant donné que le règlement vise à créer un cadre juridique commun en matière de cybersécurité au sein des institutions, organes et organismes de l'Union.

• Subsidiarité

Le règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité pour l'ensemble des institutions, organes et organismes de l'Union relève de la compétence exclusive de l'Union.

- **Proportionnalité**

Les règles proposées dans le présent règlement ne vont pas au-delà de ce qui est nécessaire pour réaliser les objectifs spécifiques de manière satisfaisante. Les mesures envisagées contribueront à un niveau élevé commun de cybersécurité sans aller au-delà de ce qui est nécessaire pour atteindre cet objectif eu égard aux risques de plus en plus élevés auxquels les institutions, organes et organismes de l'Union sont confrontés.

- **Choix de l'instrument**

Le choix d'un règlement, instrument juridique directement applicable, est jugé approprié pour définir et rationaliser les obligations imposées aux institutions, organes et organismes de l'Union. Pour permettre des améliorations ciblées, le règlement est l'instrument juridique le plus approprié.

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

- **Évaluations ex ante**

La CERT-UE a procédé à une évaluation des principales cybermenaces auxquelles les institutions, organes et organismes de l'Union sont actuellement exposés ou sont susceptibles de l'être dans un avenir prévisible.

Trois catégories d'observations ont été utilisées dans cette analyse:

- les tentatives de violation de la sécurité de l'infrastructure informatique des institutions, organes et organismes de l'Union (en cas de succès, elles sont traitées comme des incidents; dans les autres cas, elles sont toujours enregistrées comme des tentatives détectées);
- les menaces détectées à proximité des institutions, organes et organismes de l'Union (par exemple, dans les secteurs relevant de leur compétence, dans leurs communautés de parties prenantes ou en Europe);
- les principales tendances en matière de menaces observées à l'échelle mondiale.

En outre, l'analyse a examiné l'influence des grands changements en cours sur la façon dont les institutions de l'Union gèrent et utilisent leurs infrastructures et services informatiques. Parmi ces changements, citons notamment:

- l'augmentation du télétravail;
- la migration des systèmes vers le nuage;
- l'externalisation accrue des services informatiques.

Entre 2019 et 2021, le nombre d'incidents importants[1] touchant des institutions, organes et organismes de l'Union et perpétrés par des acteurs de menaces persistantes avancées a considérablement augmenté. Au cours du premier semestre de 2021, on a enregistré autant d'incidents importants que sur l'ensemble de l'année 2020. Cette évolution est également visible dans le nombre de copies-images (instantanés du contenu des systèmes ou dispositifs concernés) analysées en 2020 par la CERT-UE, qui a triplé par rapport à 2019, tandis que le nombre d'incidents importants a été multiplié par plus de dix depuis 2018.

[1] «Incident important»: tout incident, sauf s'il a un impact limité et si la méthode ou la technologie utilisées sont susceptibles d'être déjà bien comprises.

En 2020, le comité de pilotage de la CERT-UE a fixé à cette dernière un nouvel objectif stratégique consistant à garantir à l'ensemble des institutions, organes et organismes de l'Union un niveau global de cyberdéfense, en assurant une protection d'une étendue et d'une profondeur appropriées, qui s'adapte en permanence aux menaces existantes ou imminentes, y compris les attaques contre les appareils mobiles, les environnements en nuage et les dispositifs de l'internet des objets.

En complément de l'analyse des menaces menée par la CERT-UE, la Commission a procédé à une évaluation du fonctionnement de vingt institutions, organes et organismes de l'Union du point de vue de la cybersécurité. Cette évaluation a permis de mieux comprendre, au moyen d'une analyse comparative externe de certains contrôles techniques de sécurité, les pratiques établies en matière de cybersécurité et les capacités de gestion de la cybersécurité.

Elle s'appuyait sur des questionnaires auxquels les institutions, organes et organismes concernés ont répondu, sur des données accessibles au public et sur des données fournies directement par les institutions, organes et organismes de l'Union eux-mêmes. Elle a permis d'obtenir suffisamment d'informations sur la situation actuelle pour tirer les conclusions suivantes:

- le niveau de maturité en matière de cybersécurité, la taille des infrastructures informatiques et le niveau des capacités varient considérablement au sein des institutions, organes et organismes de l'Union évalués;
- bien que, en général, les institutions, organes et organismes de l'Union soient nombreux à disposer de capacités de détection et de réaction matures, leurs capacités de gouvernance en matière de cybersécurité présentent des niveaux variables de gestion intégrée des risques;
- si, en général, les cadres de cybersécurité (stratégie, politique et règles de base) des institutions, organes et organismes de l'Union évalués sont bien établis dans les domaines clés de la cybersécurité énumérés à l'annexe I du règlement, le niveau de maturité en ce qui concerne la gestion de la continuité des activités, la conformité, l'audit et l'amélioration continue est insuffisant dans certains des institutions, organes et organismes de l'Union;
- les mesures techniques considérées comme de meilleures pratiques sont appliquées de manière inégale par les institutions, organes et organismes de l'Union évalués.

En résumé, l'analyse des vingt institutions, organes et organismes de l'Union concernés fait apparaître des disparités considérables en ce qui concerne leur gouvernance, leur hygiène informatique, leurs capacités globales et leur maturité. Par conséquent, pour remédier à cette hétérogénéité des niveaux de maturité et amener l'ensemble des institutions, organes et organismes de l'Union à un niveau élevé commun de cybersécurité, il est essentiel d'exiger de l'ensemble des institutions, organes et organismes de l'Union qu'ils mettent en œuvre une base de référence en cybersécurité.

Jusqu'à présent, aucun acte législatif de l'Union n'a été axé sur la cybersécurité des institutions, organes et organismes de l'Union ni n'a abordé de manière exhaustive le paysage des menaces qui pèsent sur la cybersécurité et les risques informatiques émergents liés à la transformation numérique.

- **Consultations des parties intéressées**

La Commission a consulté les parties intéressées dans l'ensemble des institutions, organes et organismes de l'Union, ainsi que les représentants des États membres au Conseil et des parties intéressées au Parlement européen. Le 25 juin 2021, les représentants des États membres et

des parties intéressées des institutions, organes et organismes de l'Union ont participé à un atelier organisé par la Commission afin de discuter du contenu de la future proposition de règlement.

- **Analyse d'impact**

La présente proposition aura une incidence sur les institutions, organes et organismes de l'Union. Une analyse d'impact spécifique n'est donc pas nécessaire car les États membres ne sont pas concernés.

- **Droits fondamentaux**

L'Union européenne a la volonté de respecter des normes élevées de protection des droits fondamentaux. Tous les échanges d'informations fondés sur le présent règlement seraient réalisés dans des environnements de confiance, dans le plein respect du droit à la protection des données à caractère personnel consacré à l'article 8 de la charte des droits fondamentaux de l'Union européenne et de la législation applicable en matière de protection des données, notamment le règlement (UE) 2018/1725 du Parlement européen et du Conseil.

4. INCIDENCE BUDGÉTAIRE

D'après les études et les analyses comparatives du marché[2], les dépenses directes en matière de cybersécurité représentent généralement entre 4 et 7 % du total des dépenses informatiques des organisations. Toutefois, l'analyse des menaces menée par la CERT-UE à l'appui de la présente proposition législative indique que les organisations politiques et organismes internationaux sont confrontés à des risques accrus et qu'il semblerait plus approprier de consacrer 10 % des dépenses informatiques à la cybersécurité. Il est impossible de déterminer le coût exact de ces efforts en raison du manque d'informations détaillées sur les dépenses informatiques des institutions, organes et organismes de l'Union et sur la part que représentent les dépenses de cybersécurité.

S'il est par conséquent probable que beaucoup d'institutions, organes et organismes de l'UE consacrent moins de ressources financières à la cybersécurité qu'ils ne devraient, le présent règlement n'entraînera pas en lui-même une augmentation des dépenses actuelles dans ce domaine. Même sans ce règlement, chaque entité devrait garantir un niveau adéquat de cybersécurité. Le règlement prévoit la poursuite de la coopération au sein du comité de pilotage du CERT-UE et formalise un niveau d'échange d'informations qui existe déjà en partie aujourd'hui. Comme indiqué dans la fiche financière législative, le CERT-UE aura besoin de ressources supplémentaire pour mener à bien sa mission élargie et ces ressources devraient être réaffectées à partir des institutions, organes et organismes de l'UE bénéficiant des services du CERT-UE.

[2] Source: Gartner, «Identifying the Real Information Security Budget» (2016). Il convient d'ajouter à cela les dépenses indirectes en matière de sécurité informatique, notamment en ce qui concerne la sécurité des réseaux (pare-feux, antivirus et responsabilités des propriétaires des systèmes, par exemple en matière d'évaluation des risques et de mise en œuvre des contrôles de sécurité). Selon un document de 2020, les dépenses de cybersécurité représentent entre 10 et 11 % des dépenses informatiques des établissements financiers; source: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

5. AUTRES ÉLÉMENTS

- **Modalités concernant la mise en œuvre, le suivi, l'évaluation et la communication d'informations**

Le conseil interinstitutionnel de cybersécurité (IICB), assisté du CERT-UE, devrait réexaminer le fonctionnement du présent règlement, procéder à des évaluations et soumettre à la Commission un rapport contenant ses conclusions. La Commission devrait veiller à présenter régulièrement des rapports au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions,

Le CERT-UE peut rédiger une proposition de document d'orientation ou de recommandation, que l'IICB peut choisir d'adopter. Un document d'orientation est un avis adressé à l'ensemble des institutions, organes et organismes de l'Union ou à un sous-ensemble de ceux-ci, tandis qu'une recommandation est adressée à une institution, un organe ou un organisme de l'Union en particulier. Un appel à l'action est un avis de sécurité du CERT-UE décrivant les mesures de sécurité urgentes que les institutions, organes et organismes de l'Union sont vivement encouragés à prendre dans un délai déterminé.

- **Explication détaillée des différentes dispositions de la proposition**

Dispositions générales

Le règlement établit des mesures destinées à assurer un niveau élevé commun de cybersécurité et s'applique aux institutions, organes et organismes de l'Union afin de leur permettre d'accomplir leurs missions respectives de manière ouverte, efficace et indépendante. (Articles 1er-3, 23-25)

Mesures destinées à assurer un niveau élevé commun de cybersécurité

Les institutions, organes et organismes de l'Union sont tenus d'établir un cadre interne pour la gestion, la gouvernance et le contrôle des risques de cybersécurité, garantissant une gestion efficace et prudente de tous ces risques. Les institutions, organes et organismes adoptent en outre une base de référence en cybersécurité pour faire face aux risques identifiés au moyen de ce cadre, effectuent régulièrement des évaluations de la maturité en matière de cybersécurité et adoptent un plan de cybersécurité. (Articles 4-8)

Conseil interinstitutionnel de cybersécurité

Il est institué un conseil interinstitutionnel de cybersécurité chargé de suivre la mise en œuvre du présent règlement par les institutions, organes et organismes de l'Union, ainsi que de surveiller la mise en œuvre des priorités et des objectifs généraux par le CERT-UE et de fournir à ce dernier des orientations stratégiques. (Articles 9-11)

CERT-UE

Le CERT-UE contribue à la sécurité de l'environnement informatique de l'ensemble des institutions, organes et organismes de l'Union en les conseillant, en les aidant à prévenir, à détecter et à limiter les incidents, ainsi qu'à y répondre, et en faisant office de plateforme d'échange d'informations et de coordination des réponses aux incidents dans le domaine de la cybersécurité. (Articles 12-17)

Obligations en matière de coopération et de communication d'informations

Le règlement garantit la coopération et l'échange d'informations entre le CERT-UE et les institutions, organes et organismes de l'Union afin de renforcer la confiance. À cette fin, le CERT-UE peut demander aux institutions, organes et organismes de l'Union de lui fournir

des informations pertinentes et il peut échanger des informations spécifiques à un incident avec les institutions, organes et organismes de l'Union afin de faciliter la détection des cybermenaces ou incidents similaires sans le consentement de la partie concernée. Le CERT-UE ne peut échanger des informations spécifiques à un incident qui révèlent l'identité de la cible de l'incident de cybersécurité qu'avec le consentement de la partie concernée.

En particulier, l'ensemble des institutions, organes et organismes de l'Union notifient au CERT-UE les cybermenaces importantes, les vulnérabilités importantes et les incidents importants dans les plus brefs délais et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance. (Articles 18-22).

2022/0085 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 298,

vu le traité instituant la Communauté européenne de l'énergie atomique, et notamment son article 106 *bis*,

vu la proposition de la Commission européenne,

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

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) À l'ère numérique, les technologies de l'information et des communications constituent l'un des piliers d'une administration de l'Union ouverte, efficace et indépendante. L'évolution de la technologie ainsi que la complexité et l'interdépendance croissantes des systèmes numériques amplifient les risques de cybersécurité et rendent l'administration de l'Union plus vulnérable aux cybermenaces et aux incidents, ce qui, en définitive, met en péril la continuité des activités de l'administration et la capacité de celle-ci à sécuriser ses données. Alors que le recours accru aux services en nuage, l'utilisation généralisée des technologies de l'information, le degré élevé de numérisation, le télétravail et l'évolution des technologies et de la connectivité sont devenus des caractéristiques essentielles de toutes les activités des entités administratives de l'Union, la résilience numérique n'est pas encore suffisamment intégrée.

(2) Le panorama des cybermenaces auxquelles sont confrontés les institutions, organes et organismes de l'Union est en constante évolution. Les tactiques, les techniques et les procédures employées par les acteurs de la menace sont toujours en mutation, tandis que leurs motivations principales changent peu, allant du vol d'informations précieuses non divulguées à la recherche de profit, la manipulation de l'opinion publique ou l'affaiblissement des infrastructures numériques. Le rythme auquel les acteurs de la menace mènent leurs cyberattaques ne cesse d'augmenter, tandis que leurs campagnes sont de plus en plus sophistiquées et automatisées, ciblant des surfaces d'attaque exposées qui ne cessent de s'étendre et exploitant rapidement les vulnérabilités.

(3) Les environnements informatiques des institutions, organes et organismes de l'Union sont interdépendants, leurs flux de données sont intégrés et leurs utilisateurs collaborent étroitement. En raison de cette interdépendance, toute perturbation, même initialement limitée à une institution, un organe ou un organisme de l'Union, peut être à l'origine d'effets en cascade plus larges, entraînant éventuellement des incidences négatives durables et de grande ampleur pour les autres entités. En outre, certains

environnements informatiques des institutions, organes et organismes sont connectés aux environnements informatiques des États membres, de sorte qu'un incident dans une entité de l'Union présente un risque pour la cybersécurité des environnements informatiques des États membres et inversement.

(4) Les institutions, organes et organismes de l'Union sont des cibles attrayantes qui doivent faire face à des acteurs de la menace hautement qualifiés et disposant de ressources suffisantes, ainsi qu'à d'autres menaces. Dans le même temps, le degré et le niveau de maturité de la cyber-résilience ainsi que la capacité à détecter les actes de cybermalveillance et à y réagir varient considérablement selon les entités. Il est donc nécessaire, pour le fonctionnement de l'administration européenne, que les institutions, organes et organismes de l'Union atteignent un niveau élevé commun de cybersécurité grâce à une base de référence en cybersécurité (un ensemble de règles minimales en matière de cybersécurité que les réseaux et systèmes d'information et leurs opérateurs et utilisateurs doivent respecter afin de réduire au minimum les risques en matière de cybersécurité), à l'échange d'informations et à la collaboration.

(5) La directive [proposition SRI 2] concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union vise à améliorer encore la résilience en matière de cybersécurité et les capacités de réaction en cas d'incident des entités publiques et privées, des autorités et organismes nationaux compétents ainsi que de l'Union dans son ensemble. Il est donc nécessaire que les institutions, organes et organismes de l'Union suivent cet exemple en se dotant de règles qui soient compatibles avec la directive [proposition SRI 2] et correspondent à son niveau d'ambition.

(6) Pour atteindre un niveau élevé commun de cybersécurité, il est nécessaire que chaque institution, organe et organisme de l'Union établisse un cadre interne de gestion, de gouvernance et de contrôle des risques de cybersécurité, qui garantisse une gestion efficace et prudente de tous les risques de cybersécurité et tienne compte de la continuité des activités et de la gestion des crises.

(7) En raison des différences entre les institutions, organes et organismes de l'Union, il y a lieu de faire preuve de souplesse dans la mise en œuvre car un modèle unique ne conviendra pas à toutes les entités. Les mesures en faveur d'un niveau élevé commun de cybersécurité ne devraient pas inclure d'obligations qui interfèrent directement avec l'exercice des missions des institutions, organes et organismes de l'Union ou qui empiètent sur leur autonomie institutionnelle. Il convient, par conséquent, que ces institutions, organes et organismes établissent leurs propres cadres de gestion, de gouvernance et de contrôle des risques de cybersécurité, et adoptent des bases de référence et des plans de cybersécurité qui leur sont propres.

(8) Pour éviter que la charge financière et administrative imposée aux institutions, organes et organismes de l'Union ne soit excessive, il convient que les exigences en matière de gestion des risques de cybersécurité soient proportionnées aux risques que présentent le réseau et le système d'information concernés, compte tenu de l'état le plus avancé de la technique en ce qui concerne ces mesures. Chaque institution, organe et organisme de l'Union devrait s'efforcer d'allouer un pourcentage adéquat de son budget informatique à l'amélioration de son niveau de cybersécurité; l'objectif à atteindre à plus long terme devrait être de l'ordre de 10 %.

(9) Pour parvenir à un niveau élevé commun de cybersécurité, la supervision de la cybersécurité devrait être assurée par le niveau hiérarchique le plus élevé de chaque institution, organe et organisme de l'Union. Celui-ci devrait approuver une base de

référence en cybersécurité, destinée à faire face aux risques identifiés dans le cadre que chaque institution, organe et organisme doit établir. La prise en compte de la culture de la cybersécurité, c'est-à-dire la pratique quotidienne de la cybersécurité, fait partie intégrante d'une base de référence en cybersécurité dans l'ensemble des institutions, organes et organismes de l'Union.

(10) Les institutions, organes et organismes de l'Union devraient évaluer les risques liés aux relations avec les fournisseurs et les fournisseurs de services, y compris les fournisseurs de services de stockage et de traitement des données ou de services de sécurité gérés, et prendre les mesures appropriées pour y faire face. Ces mesures devraient faire partie de la base de référence en cybersécurité et être précisées dans des documents d'orientation ou des recommandations publiés par le CERT-UE. Lors de la définition des mesures et des lignes directrices, il convient de tenir dûment compte de la législation et des politiques pertinentes de l'UE, notamment des évaluations des risques et des recommandations formulées par le groupe de coopération SRI, telles que l'évaluation coordonnée des risques au niveau de l'UE et la boîte à outils de l'UE sur la cybersécurité de la 5G. En outre, la certification des produits, services et processus TIC pertinents pourrait être requise, dans le cadre de schémas de certification de cybersécurité de l'UE spécifiques adoptés en vertu de l'article 49 du règlement (UE) 2019/881.

(11) En mai 2011, les secrétaires généraux des institutions et organes de l'Union ont décidé de mettre en place une équipe de préconfiguration en vue de la création d'une équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union (CERT-UE), supervisée par un comité de pilotage interinstitutionnel. En juillet 2012, les secrétaires généraux ont confirmé les modalités pratiques et sont convenus que la CERT-UE demeurerait une entité permanente, afin de continuer à contribuer à l'amélioration du niveau général de la sécurité informatique des institutions, organes et organismes de l'UE. Il s'agit là d'un exemple visible de coopération interinstitutionnelle dans le domaine de la cybersécurité. En septembre 2012, la CERT-UE a été créée sous la forme d'une task-force de la Commission européenne dotée d'un mandat interinstitutionnel. En décembre 2017, les institutions et organes de l'Union ont conclu un accord interinstitutionnel sur l'organisation et le fonctionnement de la CERT-UE[3]. Cet accord devrait continuer à évoluer afin de soutenir la mise en œuvre du présent règlement.

(12) L'«équipe d'intervention en cas d'urgence informatique» (la CERT-UE) devrait désormais être dénommée «centre de cybersécurité» pour les institutions, organes et organismes de l'Union (le CERT-UE), pour faire écho à l'évolution observée dans les États membres et au niveau mondial, où de nombreuses CERT ont été renommées «centres de cybersécurité». La dénomination abrégée «CERT-UE» devrait toutefois être conservée en raison de sa notoriété.

(13) De nombreuses cyberattaques s'inscrivent dans le cadre de campagnes plus larges qui ciblent des groupes d'institutions, d'organes et d'organismes de l'Union ou de communautés d'intérêt auxquelles appartiennent les institutions, organes et organismes de l'Union. Afin de permettre la détection proactive, la réaction en cas d'incident ou l'adoption de mesures d'atténuation, les institutions, organes et organismes de l'Union devraient notifier au CERT-UE les cybermenaces importantes, les vulnérabilités importantes et les incidents importants et partager les renseignements

[3] JO C 12 du 13.1.2018, p. 1.

techniques appropriés permettant de détecter ou d'atténuer les cybermenaces, vulnérabilités et incidents similaires, ainsi que de réagir à ces menaces, vulnérabilités et incidents dans d'autres institutions, organes et organismes de l'Union. Suivant la même approche que celle envisagée dans la directive [proposition SRI 2], lorsque les entités ont connaissance d'un incident important, elles devraient être tenues de soumettre une première notification au CERT-UE dans un délai de 24 heures. Cet échange d'informations devrait permettre au CERT-UE de communiquer les informations à d'autres institutions, organes et organismes de l'Union, ainsi qu'à leurs homologues concernés, afin de contribuer à protéger les environnements informatiques de l'Union et de ses homologues contre des incidents, menaces et vulnérabilités similaires.

(14) Outre l'extension des missions du CERT-UE et l'élargissement de son rôle, il convient de créer un conseil interinstitutionnel de cybersécurité (IICB), qui devrait faciliter l'instauration d'un niveau élevé commun de cybersécurité parmi les institutions, organes et organismes de l'Union en surveillant la mise en œuvre du présent règlement par les institutions, organes et organismes de l'Union, en supervisant la mise en œuvre des priorités et des objectifs généraux par le CERT-UE et en fournissant des orientations stratégiques au CERT-UE. L'IICB devrait assurer la représentation des institutions et inclure des représentants des agences et organismes par l'intermédiaire du réseau des agences de l'UE.

(15) Le CERT-UE devrait soutenir la mise en œuvre de mesures visant à assurer un niveau élevé commun de cybersécurité en proposant des documents d'orientation et des recommandations à l'intention de l'IICB ou en lançant des appels à l'action. Ces documents d'orientation et recommandations devraient être approuvés par l'IICB. Le cas échéant, le CERT-UE devrait lancer des appels à l'action décrivant les mesures de sécurité urgentes que les institutions, organes et organismes de l'Union sont vivement encouragés à prendre dans un délai déterminé.

(16) L'IICB devrait contrôler le respect du présent règlement ainsi que le suivi des documents d'orientation, des recommandations et des appels à l'action émanant du CERT-UE. Sur les questions techniques, l'IICB devrait être assisté de groupes consultatifs techniques dont la composition sera adaptée à ses besoins, qui devraient travailler en étroite coopération avec le CERT-UE, les institutions, organes et organismes de l'Union et d'autres parties prenantes, le cas échéant. Si nécessaire, l'IICB devrait émettre des avertissements non contraignants et recommander des audits.

(17) Le CERT-UE devrait avoir pour mission de contribuer à la sécurité de l'environnement informatique de l'ensemble des institutions, organes et organismes de l'Union. Le CERT-UE devrait jouer un rôle équivalent à celui de coordinateur désigné pour les institutions, organes et organismes de l'Union, aux fins de la divulgation coordonnée des vulnérabilités dans le registre européen des vulnérabilités visée à l'article 6 de la directive [proposition SRI 2].

(18) En 2020, le comité de pilotage du CERT-UE avait fixé à cette dernière un nouvel objectif stratégique consistant à garantir à l'ensemble des institutions, organes et organismes de l'Union un niveau global de cyberdéfense, en assurant une protection d'une étendue et d'une profondeur appropriées, qui s'adapte en permanence aux menaces existantes ou imminentes, y compris les attaques contre les appareils mobiles, les environnements en nuage et les dispositifs de l'internet des objets. L'objectif stratégique comprend également les centres d'opérations de sécurité (COS) à large

spectre qui surveillent les réseaux, et la surveillance 24 heures sur 24, 7 jours sur 7 des menaces d'une gravité élevée. Le CERT-UE devrait soutenir les équipes chargées de la sécurité informatique des institutions, organes et organismes de l'Union de plus grande taille, y compris dans le cadre de la surveillance 24 heures sur 24, 7 jours sur 7 de première ligne. Pour les institutions, organes et organismes de l'Union de petite taille et de taille moyenne, le CERT-UE devrait fournir l'ensemble des services.

(19) Le CERT-UE devrait également remplir le rôle qui lui est assigné dans la directive [proposition SRI 2] en ce qui concerne la coopération et l'échange d'informations avec le réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT). En outre, conformément à la recommandation (UE) 2017/1584[4] de la Commission, le CERT-UE devrait, en ce qui concerne la réaction, assurer la coopération et la coordination avec les parties prenantes concernées. Afin de contribuer à un niveau élevé de cybersécurité dans l'ensemble de l'Union, le CERT-UE devrait partager avec ses homologues nationaux des informations spécifiques aux incidents. Il devrait également collaborer avec d'autres homologues publics et privés, y compris au sein de l'OTAN, sous réserve de l'approbation préalable de l'IICB.

(20) Pour soutenir la cybersécurité opérationnelle, le CERT-UE devrait faire appel à l'expertise disponible de l'Agence de l'Union européenne pour la cybersécurité dans le cadre de la coopération structurée prévue par le règlement (UE) 2019/881 du Parlement européen et du Conseil[5]. Le cas échéant, des accords dédiés entre les deux entités devraient être conclus afin de définir les modalités pratiques de la mise en œuvre de cette coopération et d'éviter la duplication des activités. Le CERT-UE devrait coopérer avec l'Agence de l'Union européenne pour la cybersécurité en ce qui concerne l'analyse des menaces et partager régulièrement son rapport sur le panorama des menaces avec l'Agence.

(21) Pour appuyer l'unité conjointe de cybersécurité créée conformément à la recommandation de la Commission du 23 juin 2021[6], le CERT-UE devrait coopérer et échanger des informations avec les parties prenantes afin de promouvoir la coopération opérationnelle et de permettre aux réseaux existants de réaliser pleinement leur potentiel de protection de l'Union.

(22) Toutes les données à caractère personnel faisant l'objet d'un traitement dans le cadre du présent règlement devraient être traitées conformément à la législation en matière de protection des données, y compris le règlement (UE) 2018/1725 du Parlement européen et du Conseil[7].

(23) Le traitement des informations par le CERT-UE et les institutions, organes et organismes de l'Union devrait être conforme aux règles énoncées dans le règlement

---

4 Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

5 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).

6 Recommandation C(2021)4520 de la Commission du 23.6.2021 sur la création d'une unité conjointe de cybersécurité.

7 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).

[proposition de règlement sur la sécurité de l'information]. Pour veiller à la coordination en matière de sécurité, tout contact que les services nationaux de sécurité ou de renseignement établissent ou tentent d'établir avec le CERT-UE devrait être signalé sans délai à la direction de la sécurité de la Commission et au président du comité de pilotage de l'IICB.

(24) Étant donné que les services et les missions du CERT-UE sont dans l'intérêt de l'ensemble des institutions, organes et organismes de l'Union, chaque institution, organe et organisme de l'Union engageant des dépenses informatiques devrait contribuer équitablement à ces services et missions. Ces contributions sont sans préjudice de l'autonomie budgétaire des institutions, organes et organismes de l'Union.

(25) L'IICB, avec l'aide du CERT-UE, devrait examiner et évaluer la mise en œuvre du présent règlement et faire part de ses conclusions à la Commission. La Commission devrait s'appuyer sur ces conclusions pour faire rapport au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Chapitre I
DISPOSITIONS GÉNÉRALES

Article premier
Objet

Le présent règlement établit:

(a) les obligations incombant aux institutions, organes et organismes de l'Union en ce qui concerne l'établissement d'un cadre interne de gestion, de gouvernance et de contrôle des risques de cybersécurité;

(b) les obligations incombant aux institutions, organes et organismes de l'Union en ce qui concerne la gestion des risques de cybersécurité et la communication d'informations;

(c) les règles relatives à l'organisation et au fonctionnement du centre de cybersécurité des institutions, organes et organismes de l'Union (CERT-UE) et à l'organisation et au fonctionnement du conseil interinstitutionnel de cybersécurité.

Article 2
Champ d'application

Le présent règlement s'applique à la gestion, à la gouvernance et au contrôle des risques de cybersécurité par l'ensemble des institutions, organes et organismes de l'Union, ainsi qu'à l'organisation et au fonctionnement du CERT-UE et du conseil interinstitutionnel de cybersécurité.

Article 3
Définitions

Aux fins du présent règlement, on entend par:

(1) «institutions, organes et organismes de l'Union»: les institutions, organes et organismes de l'Union créés par le traité sur l'Union européenne, le traité sur le

fonctionnement de l'Union européenne ou le traité instituant la Communauté européenne de l'énergie atomique, ou sur la base de ces traités;

(2) «réseau et système d'information»: un réseau et système d'information au sens de l'article 4, point 1), de la directive [proposition SRI 2];

(3) «sécurité des réseaux et des systèmes d'information»: la sécurité des réseaux et des systèmes d'information au sens de l'article 4, point 2), de la directive [proposition SRI 2];

(4) «cybersécurité»: la cybersécurité au sens de l'article 4, point 3), de la directive [proposition SRI 2];

(5) «niveau hiérarchique le plus élevé»: un responsable, un organe de direction ou un organe de coordination et de surveillance au niveau administratif le plus élevé, en fonction des dispositifs de gouvernance à haut niveau propres à chaque institution, organe ou organisme de l'Union;

(6) «incident»: un incident au sens de l'article 4, point 5), de la directive [proposition SRI 2];

(7) «incident important»: tout incident, sauf s'il a un impact limité et que la méthode ou la technologie utilisées sont susceptibles d'être déjà bien comprises;

(8) «attaque majeure»: tout incident nécessitant davantage de ressources que celles dont disposent les institutions, organes ou organismes de l'Union touchés et le CERT-UE;

(9) «traitement des incidents»: le traitement des incidents au sens de l'article 4, point 6), de la directive [proposition SRI 2];

(10) «cybermenace»: une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;

(11) «cybermenace importante»: une cybermenace caractérisée par l'intention, la possibilité et la capacité de provoquer un incident important;

(12) «vulnérabilité»: une vulnérabilité au sens de l'article 4, point 8), de la directive [proposition SRI 2];

(13) «vulnérabilité importante»: une vulnérabilité susceptible d'entraîner un incident important si elle est exploitée;

(14) «risque de cybersécurité»: toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information;

(15) «unité conjointe de cybersécurité»: une plateforme virtuelle et physique de coopération pour les différentes communautés de cybersécurité de l'Union, axée sur la coordination opérationnelle et technique pour faire face aux menaces et incidents transfrontières de cybersécurité majeurs au sens de la recommandation de la Commission du 23 juin 2021;

(16) «base de référence en cybersécurité»: un ensemble de règles minimales en matière de cybersécurité que les réseaux et systèmes d'information et leurs opérateurs et utilisateurs doivent respecter afin de réduire au minimum les risques de cybersécurité.

Chapitre II
MESURES DESTINÉES À ASSURER UN NIVEAU ÉLEVÉ COMMUN DE CYBERSÉCURITÉ

Article 4

Gestion, gouvernance et contrôle des risques

1. Chaque institution, organe et organisme de l'Union établit son propre cadre interne de gestion, de gouvernance et de contrôle des risques de cybersécurité (ci-après le «cadre»), à l'appui de sa mission et dans l'exercice de son autonomie institutionnelle. Ces travaux sont placés sous la supervision du niveau hiérarchique le plus élevé de l'entité, afin de garantir une gestion efficace et prudente de tous les risques de cybersécurité. Le cadre est en place au plus tard le... [15 mois après l'entrée en vigueur du présent règlement].

2. Le cadre couvre l'ensemble de l'environnement informatique de l'institution, de l'organe ou de l'organisme concernés, y compris l'environnement informatique sur site, les actifs et services externalisés dans des environnements d'informatique en nuage ou hébergés par des tiers, les appareils mobiles, les réseaux d'entreprise, les réseaux professionnels non connectés à l'internet et tout appareil connecté à l'environnement informatique. Le cadre tient compte de la continuité des activités et de la gestion des crises et prend en considération la sécurité de la chaîne d'approvisionnement ainsi que la gestion des risques humains susceptibles d'avoir une incidence sur la cybersécurité de l'institution, de l'organe ou de l'organisme de l'Union concernés.

3. Le niveau hiérarchique le plus élevé de chaque institution, organe et organisme de l'Union assure la surveillance du respect, par son entité, des obligations liées à la gestion, à la gouvernance et au contrôle des risques de cybersécurité, sans préjudice des responsabilités formelles incombant aux autres niveaux hiérarchiques en matière de conformité et en ce qui concerne la gestion des risques dans leurs domaines de compétence respectifs.

4. Chaque institution, organe et organisme de l'Union dispose de mécanismes efficaces pour garantir qu'un pourcentage adéquat du budget informatique est consacré à la cybersécurité.

5. Chaque institution, organe et organisme de l'Union désigne un responsable local de la cybersécurité ou une fonction équivalente qui fait office de point de contact unique pour tous les aspects liés à la cybersécurité.

Article 5

Base de référence en cybersécurité

1. Le niveau hiérarchique le plus élevé de chaque institution, organe et organisme de l'Union approuve la base de référence en cybersécurité propre à l'entité pour faire face aux risques identifiés dans le cadre visé à l'article 4, paragraphe 1, à l'appui de sa mission et dans l'exercice de son autonomie institutionnelle. La base de référence en cybersécurité est en place au plus tard le... [18 mois après l'entrée en vigueur du présent règlement] et concerne les domaines énumérés à l'annexe I et les mesures énumérées à l'annexe II.

2. Les membres de l'encadrement supérieur de chaque institution, organe et organisme de l'Union suivent régulièrement des formations spécifiques afin d'acquérir des

connaissances et des compétences suffisantes pour appréhender et évaluer les pratiques en matière de gestion des risques et de gestion de la cybersécurité et leur incidence sur les activités de l'entité.

Article 6
Évaluations de la maturité

Chaque institution, organe et organisme de l'Union procède, au moins tous les trois ans, à une évaluation de la maturité en matière de cybersécurité portant sur l'ensemble des éléments de son environnement informatique comme décrit à l'article 4, en tenant compte des documents d'orientation et recommandations pertinents adoptés conformément à l'article 13.

Article 7
Plans de cybersécurité

1. Compte tenu des conclusions tirées de l'évaluation de la maturité et des actifs et des risques identifiés conformément à l'article 4, le niveau hiérarchique le plus élevé de chaque institution, organe et organisme de l'Union approuve un plan de cybersécurité dans les meilleurs délais après l'établissement du cadre de gestion, de gouvernance et de contrôle des risques et de la base de référence en cybersécurité. Le plan vise à accroître la cybersécurité globale de l'entité concernée et contribue ainsi à atteindre un niveau élevé commun de cybersécurité parmi l'ensemble des institutions, organes et organismes de l'Union, ou à le renforcer. Pour appuyer la mission de l'entité sur la base de son autonomie institutionnelle, le plan comprend au moins les domaines énumérés à l'annexe I, les mesures énumérées à l'annexe II, ainsi que les mesures liées à la préparation aux incidents, à la réaction et au rétablissement, telles que la surveillance de la sécurité et la journalisation. Le plan est révisé au moins tous les trois ans, à la suite des évaluations de la maturité effectuées conformément à l'article 6.
2. Le plan de cybersécurité précise le rôle des membres du personnel dans sa mise en œuvre ainsi que les responsabilités qui leur incombent.
3. Le plan de cybersécurité prend en considération tous les documents d'orientation et recommandations applicables émis par le CERT-UE.

Article 8
Mise en œuvre

1. Lorsque les évaluations de la maturité sont terminées, les institutions, organes et organismes de l'Union les soumettent au conseil interinstitutionnel de cybersécurité. Une fois les plans de sécurité achevés, les institutions, organes et organismes de l'Union en informent le conseil interinstitutionnel de cybersécurité. À la demande du conseil interinstitutionnel de cybersécurité, ils font rapport sur des aspects spécifiques du présent chapitre.
2. Les documents d'orientation et les recommandations établis conformément à l'article 13 soutiennent la mise en œuvre des dispositions du présent chapitre.

Chapitre III
CONSEIL INTERINSTITUTIONNEL DE CYBERSÉCURITÉ

Article 9
Conseil interinstitutionnel de cybersécurité

1. Un conseil interinstitutionnel de cybersécurité (IICB) est institué.

2. L'IICB est chargé:

   (a) de suivre la mise en œuvre du présent règlement par les institutions, organes et organismes de l'Union;

   (b) de superviser la mise en œuvre des priorités et objectifs généraux par le CERT-UE et de lui fournir des orientations stratégiques.

3. L'IICB est composé de trois représentants nommés par le réseau des agences de l'Union européenne (EUAN), sur proposition de son comité consultatif sur les TIC, pour représenter les intérêts des organes et organismes qui gèrent leur propre environnement informatique, ainsi que d'un représentant désigné par chacune des entités suivantes:

   (a) le Parlement européen;

   (b) le Conseil de l'Union européenne;

   (c) la Commission européenne;

   (d) la Cour de justice de l'Union européenne;

   (e) la Banque centrale européenne;

   (f) la Cour des comptes européenne;

   (g) le service européen pour l'action extérieure;

   (h) le Comité économique et social européen;

   (i) le Comité européen des régions;

   (j) la Banque européenne d'investissement;

   (k) l'Agence de l'Union européenne pour la cybersécurité.

   Chaque membre peut être assisté d'un suppléant. D'autres représentants des entités susmentionnées ou d'autres institutions, organes et organismes de l'Union peuvent être invités par le président à assister aux réunions de l'IICB sans droit de vote.

4. L'IICB adopte son règlement intérieur.

5. L'IICB désigne un président parmi ses membres, conformément à son règlement intérieur et pour une période de quatre ans. Son suppléant devient membre à part entière de l'IICB pour la même durée.

6. L'IICB se réunit à l'initiative de son président, à la demande du CERT-UE ou à la demande de l'un de ses membres.

7. Chaque membre de l'IICB dispose d'une voix. Les décisions de l'IICB sont prises à la majorité simple, sauf disposition contraire du présent règlement. Le président ne peut voter qu'en cas d'égalité, sa voix pouvant alors être décisive.

8. L'IICB peut statuer par la voie d'une procédure écrite simplifiée lancée conformément au règlement intérieur de l'IICB. Dans le cadre de cette procédure, la

décision concernée est réputée approuvée dans le délai fixé par le président, sauf objection d'un membre.

9. Le chef du CERT-UE, ou son suppléant, participe aux réunions de l'IICB, sauf décision contraire de l'IICB.

10. Le secrétariat de l'IICB est assuré par la Commission.

11. Les représentants nommés par l'EUAN sur proposition du comité consultatif sur les TIC transmettent les décisions de l'IICB aux agences et entreprises communes de l'Union. Tout organe ou organisme de l'UE a le droit de soulever auprès des représentants ou du président de l'IICB toute question qu'il estime devoir être portée à l'attention de l'IICB.

12. L'IICB peut statuer par la voie d'une procédure écrite simplifiée lancée par le président, la décision concernée étant alors réputée approuvée dans le délai fixé par celui-ci, sauf objection d'un membre.

13. L'IICB peut nommer un comité exécutif pour l'assister dans ses travaux et lui déléguer certains de ses pouvoirs et tâches. L'IICB établit le règlement intérieur du comité exécutif, y compris ses tâches et pouvoirs, ainsi que le mandat de ses membres.

Article 10
Tâches de l'IICB

Lorsqu'il exerce ses responsabilités, l'IICB doit notamment:

(a) examiner tout rapport demandé au CERT-UE sur l'état d'avancement de la mise en œuvre du présent règlement par les institutions, organes et organismes de l'Union;

(b) approuver, sur la base d'une proposition du chef du CERT-UE, le programme de travail annuel du CERT-UE et en suivre la mise en œuvre;

(c) approuver, sur la base d'une proposition du chef du CERT-UE, le catalogue de services du CERT-UE;

(d) approuver, sur la base d'une proposition présentée par le chef du CERT-UE, la planification financière annuelle des recettes et des dépenses, y compris en matière d'effectifs, pour les activités du CERT-UE;

(e) approuver, sur la base d'une proposition du chef du CERT-UE, les modalités des accords de niveau de service;

(f) examiner et approuver le rapport annuel établi par le chef du CERT-UE concernant les activités du CERT-UE et sa gestion des fonds;

(g) approuver les indicateurs clés de performance relatifs au CERT-UE qui sont définis sur proposition du chef du CERT-UE, et en assurer le suivi;

(h) approuver les accords de coopération et les accords ou contrats de niveau de service conclus entre le CERT-UE et d'autres entités conformément à l'article 17;

(i) créer autant de groupes consultatifs techniques que nécessaire afin d'assister l'IICB dans ses travaux, approuver leur mandat et désigner leurs présidents respectifs.

Article 11
Respect

L'IICB suit la mise en œuvre du présent règlement et des documents d'orientation, recommandations et appels à l'action adoptés par les institutions, organes et organismes de l'Union. Lorsque l'IICB constate que les institutions, organes ou organismes de l'Union n'ont pas effectivement appliqué ou mis en œuvre le présent règlement ou les documents d'orientation, recommandations et appels à l'action élaborés au titre du présent règlement, il peut, sans préjudice des procédures internes de l'institution, organe ou organisme de l'Union concerné:

(a) émettre un avertissement; lorsque cela s'avère nécessaire en raison d'un risque de cybersécurité impérieux, les destinataires de l'avertissement sont limités de manière appropriée;

(b) recommander un service compétent pour réaliser un audit.

Chapitre IV
CERT-UE

Article 12
Mission et tâches du CERT-UE

1. La mission du CERT-UE, centre interinstitutionnel autonome de cybersécurité au service de l'ensemble des institutions, organes et organismes de l'Union, est de contribuer à la sécurité de l'environnement informatique non classifié de l'ensemble des institutions, organes et organismes de l'Union en leur fournissant des conseils concernant la cybersécurité, en les aidant à prévenir et à détecter les incidents, ainsi qu'à en atténuer les effets et à y répondre, et en faisant office de pôle d'échange d'informations sur la cybersécurité et de coordination des réponses aux incidents.

2. Le CERT-UE accomplit les tâches suivantes pour les institutions, organes et organismes de l'Union:

   (a) les soutenir dans la mise en œuvre du présent règlement et contribuer à la coordination de l'application du présent règlement par l'intermédiaire des mesures énoncées à l'article 13, paragraphe 1, ou des rapports ad hoc demandés par l'IICB;

   (b) les soutenir au moyen d'un ensemble de services de cybersécurité décrits dans son catalogue de services («services de base»);

   (c) gérer un réseau de pairs et de partenaires pour soutenir les services visés aux articles 16 et 17;

   (d) attirer l'attention de l'IICB sur toute question relative à la mise en œuvre du présent règlement et à la mise en œuvre des documents d'orientation, recommandations et appels à l'action;

   (e) rendre compte des cybermenaces auxquelles sont confrontés les institutions, organes et organismes de l'Union et contribuer à la conscience situationnelle de la cybersécurité de l'UE.

3. Le CERT-UE contribue à l'unité conjointe de cybersécurité, mise en place conformément à la recommandation de la Commission du 23 juin 2021, notamment dans les domaines suivants:

(a) la préparation, la coordination face aux incidents, l'échange d'informations et la réaction aux crises au niveau technique dans les cas liés aux institutions, organes et organismes de l'Union;

(b) la coopération opérationnelle concernant le réseau des centres de réponse aux incidents de sécurité informatique (CSIRT), y compris en matière d'assistance mutuelle, et la communauté de cybersécurité au sens plus large;

(c) les renseignements sur les cybermenaces, y compris la conscience situationnelle;

(d) tout sujet nécessitant l'expertise technique du CERT-UE en matière de cybersécurité.

4. Le CERT-UE mène une coopération structurée avec l'Agence de l'Union européenne pour la cybersécurité en ce qui concerne le renforcement des capacités, la coopération opérationnelle et les analyses stratégiques à long terme des cybermenaces conformément au règlement (UE) 2019/881 du Parlement européen et du Conseil.

5. Le CERT-UE peut fournir les services suivants non décrits dans son catalogue de services («services payants»):

(a) des services soutenant la cybersécurité de l'environnement informatique des institutions, organes et organismes de l'Union, autres que ceux visés au paragraphe 2, sur la base d'accords de niveau de service et sous réserve des ressources disponibles;

(b) des services soutenant les opérations ou projets de cybersécurité des institutions, organes et organismes de l'Union, autres que ceux visant à protéger leur environnement informatique, sur la base d'accords écrits et avec l'approbation préalable de l'IICB;

(c) des services soutenant la sécurité de l'environnement informatique fournis à des entités autres que les institutions, organes et organismes de l'Union qui coopèrent étroitement avec les institutions, organes et organismes de l'Union, par exemple par l'intermédiaire de tâches ou de responsabilités confiées en vertu du droit de l'Union, sur la base d'accords écrits et avec l'approbation préalable de l'IICB.

6. Le CERT-UE peut organiser des exercices de cybersécurité ou recommander la participation à des exercices existants, le cas échéant en étroite coopération avec l'Agence de l'Union européenne pour la cybersécurité, afin de tester le niveau de cybersécurité des institutions, organes et organismes de l'Union.

7. Le CERT-UE peut fournir une assistance aux institutions, organes et organismes de l'Union en ce qui concerne les incidents survenant dans des environnements informatiques classifiés s'il y est explicitement invité par la partie concernée.

Article 13

Documents d'orientation, recommandations et appels à l'action

1. Le CERT-UE soutient la mise en œuvre du présent règlement en élaborant:

(a) des appels à l'action décrivant les mesures de sécurité urgentes que les institutions, organes et organismes de l'Union sont instamment invités à prendre dans un délai déterminé;

(b) des propositions soumises à l'IICB concernant des documents d'orientation destinés à l'ensemble ou à une partie des institutions, organes et organismes de l'Union;

(c) des propositions soumises à l'IICB concernant des recommandations destinées à titre individuel aux institutions, organes et organismes de l'Union.

2. Les documents d'orientation et les recommandations peuvent inclure:

(a) les modalités de la gestion des risques de cybersécurité et de la base de référence en cybersécurité, ou les améliorations à y apporter;

(b) les modalités des évaluations du niveau de maturité et des plans de cybersécurité; et

(c) le cas échéant, l'utilisation d'une technologie et d'une architecture communes, ainsi que des meilleures pratiques qui y sont associées, dans le but de parvenir à l'interopérabilité et à des normes communes au sens de l'article 4, point (10), de la directive [proposition SRI 2].

3. L'IICB peut adopter des documents d'orientation ou des recommandations sur proposition du CERT-UE.

4. L'IICB peut donner instruction au CERT-UE d'élaborer, de retirer ou de modifier une proposition de documents d'orientation ou de recommandations, ou un appel à l'action.

Article 14
Chef du CERT-UE

Le chef du CERT-UE présente régulièrement des rapports à l'IICB et au président de l'IICB sur les résultats obtenus par le CERT-UE, la planification financière, les recettes, l'exécution du budget, les accords de niveau de service et les accords écrits conclus, la coopération avec les homologues et les partenaires, ainsi que les missions effectuées par le personnel, y compris les rapports visés à l'article 10, paragraphe 1.

Article 15
Questions financières et de personnel

1. La Commission, après avoir obtenu, à l'unanimité, l'approbation de l'IICB, désigne le chef du CERT-UE. L'IICB est consulté à tous les stades de la procédure menant à la désignation du chef du CERT-UE, notamment lorsqu'il s'agit d'établir les avis de vacance, d'examiner les candidatures et de désigner les comités de sélection relatifs à ce poste.

2. Pour l'application des procédures administratives et financières, le chef du CERT-UE agit sous l'autorité de la Commission.

3. Les tâches et activités du CERT-UE, y compris les services qu'il fournit, conformément à l'article 12, paragraphes 2, 3, 4 et 6, et à l'article 13, paragraphe 1, aux institutions, organes et organismes de l'Union et qui sont financés au titre de la rubrique du cadre financier pluriannuel consacrée à l'administration publique européenne, sont financées par une ligne budgétaire distincte du budget de la Commission. Les postes réservés au CERT-UE sont détaillés dans une note de bas de page du tableau des effectifs de la Commission.

4. Les institutions, organes et organismes de l'Union autres que ceux visés au paragraphe 3 versent une contribution financière annuelle au CERT-UE pour couvrir les services fournis par le CERT-UE en vertu dudit paragraphe 3. Les contributions respectives sont fondées sur les orientations données par l'IICB et convenues entre chaque entité et le CERT-UE dans les accords de niveau de service. Les contributions représentent une part équitable et proportionnée de l'ensemble des coûts des services fournis. Elles sont affectées à la ligne budgétaire distincte visée au paragraphe 3 en tant que recettes affectées comme prévu à l'article 21, paragraphe 3, point c), du règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil[8].

5. Les coûts des tâches définies à l'article 12, paragraphe 5, sont recouvrés auprès des institutions, organes et organismes de l'Union qui bénéficient des services du CERT-UE. Les recettes sont affectées aux lignes budgétaires dont relèvent les coûts.

Article 16

Coopération du CERT-UE avec les homologues des États membres

1. Le CERT-UE coopère et échange des informations avec les homologues nationaux dans les États membres, y compris les CERT, les centres nationaux de cybersécurité, les CSIRT et les points de contact uniques visés à l'article 8 de la directive [proposition SRI 2], sur les cybermenaces, les vulnérabilités et les incidents, sur d'éventuelles contre-mesures et sur toutes les questions pertinentes pour améliorer la protection des environnements informatiques des institutions, organes et organismes de l'Union, y compris par l'intermédiaire du réseau des CSIRT visé à l'article 13 de la directive [proposition SRI 2].

2. Le CERT-UE peut échanger des informations propres à un incident avec les homologues nationaux dans les États membres afin de faciliter la détection de cybermenaces ou d'incidents similaires sans le consentement de la partie touchée. Le CERT-UE ne peut échanger des informations propres à un incident qui révèlent l'identité de la cible de l'incident de cybersécurité qu'avec le consentement de la partie touchée.

Article 17

Coopération du CERT-UE avec les homologues des pays tiers

1. Le CERT-UE peut coopérer avec les homologues des pays tiers, y compris les homologues de secteurs spécifiques de l'industrie, en ce qui concerne les outils et méthodes, tels que les techniques, les tactiques, les procédures et les meilleures pratiques, et en ce qui concerne les cybermenaces et les vulnérabilités. Pour toute coopération avec lesdits homologues, y compris dans des configurations où les homologues de pays tiers coopèrent avec des homologues nationaux des États membres, le CERT-UE sollicite au préalable l'approbation de l'IICB.

2. Le CERT-UE peut coopérer avec d'autres partenaires, tels que des entités commerciales, des organisations internationales, des entités nationales ou des experts

[8] Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) nº 1296/2013, (UE) nº 1301/2013, (UE) nº 1303/2013, (UE) nº 1304/2013, (UE) nº 1309/2013, (UE) nº 1316/2013, (UE) nº 223/2014, (UE) nº 283/2014 et la décision nº 541/2014/UE, et abrogeant le règlement (UE, Euratom) nº 966/2012 (JO L 193 du 30.7.2018, p. 1).

individuels de pays tiers, afin de recueillir des informations sur des cybermenaces générales et spécifiques, des vulnérabilités et d'éventuelles contre-mesures. Pour pouvoir élargir la coopération avec ces partenaires, le CERT-UE sollicite au préalable l'approbation de l'IICB.

3. Le CERT-UE peut, avec le consentement de la partie touchée par un incident, fournir des informations relatives à l'incident aux partenaires susceptibles de contribuer à son analyse.

Chapitre V
OBLIGATIONS EN MATIÈRE DE COOPÉRATION ET DE COMMUNICATION D'INFORMATIONS

Article 18
Traitement des informations

1. Le CERT-UE et les institutions, organes et organismes de l'Union respectent l'obligation de secret professionnel conformément à l'article 339 du traité sur le fonctionnement de l'Union européenne ou à des cadres applicables équivalents.

2. Les dispositions du règlement (CE) nº 1049/2001 du Parlement européen et du Conseil[9] s'appliquent aux demandes d'accès du public aux documents détenus par le CERT-UE, y compris l'obligation, prévue par ledit règlement, de consulter les autres institutions, organes et organismes de l'Union dès lors qu'une demande concerne leurs documents.

3. Le traitement de données à caractère personnel dans le cadre du présent règlement est régi par le règlement (UE) 2018/1725 du Parlement européen et du Conseil.

4. Le traitement des informations par le CERT-UE et les institutions, organes et organismes de l'Union est conforme aux règles énoncées dans [la proposition de règlement sur la sécurité de l'information].

5. Tout contact que les services nationaux de sécurité ou de renseignement établissent ou tentent d'établir avec le CERT-UE est communiqué dans les meilleurs délais à la direction de la sécurité de la Commission et au président de l'IICB.

Article 19
Obligations en matière de partage

1. Afin de coordonner la gestion des vulnérabilités et la réaction aux incidents, le CERT-UE peut demander aux institutions, organes et organismes de l'Union de lui fournir, à partir de leurs inventaires respectifs des systèmes informatiques, des informations pertinentes pour le soutien de ses activités. L'institution, l'organe ou l'organisme requis transmet les informations demandées, ainsi que toute mise à jour ultérieure de celles-ci, dans les meilleurs délais.

2. Les institutions, organes et organismes de l'Union fournissent au CERT-UE, à sa demande et dans les meilleurs délais, les informations numériques générées par l'utilisation de dispositifs électroniques impliqués dans les incidents qui les ont

[9] 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).

respectivement touchés. Le CERT-UE peut préciser davantage les types d'informations numériques dont il a besoin pour la conscience situationnelle et la réaction aux incidents.

3. Le CERT-UE ne peut échanger des informations propres à un incident qui révèlent l'identité de l'institution, l'organe ou l'organisme de l'Union touché par cet incident qu'avec le consentement de cette entité. Le CERT-UE ne peut échanger des informations spécifiques à un incident qui révèlent l'identité de la cible de l'incident de cybersécurité qu'avec le consentement de l'entité touchée par cet incident.

4. Les obligations en matière de partage ne s'étendent pas aux informations classifiées de l'Union européenne (ICUE) ni aux informations qu'une institution, un organe ou un organisme de l'Union a reçues d'un service de sécurité ou de renseignement ou d'un service répressif d'un État membre à la condition expresse qu'elles ne soient pas partagées avec le CERT-UE.

Article 20
Obligations en matière de notification

1. L'ensemble des institutions, organes et organismes de l'Union transmettent une première notification au CERT-UE concernant les cybermenaces importantes, les vulnérabilités importantes et les incidents importants, dans les meilleurs délais et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance.

   Dans des cas dûment justifiés et en accord avec le CERT-UE, l'institution, l'organe ou l'organisme de l'Union concerné peut s'écarter du délai fixé au paragraphe précédent.

2. Les institutions, organes et organismes de l'Union notifient également au CERT-UE, dans les meilleurs délais, les renseignements techniques appropriés concernant les cybermenaces, vulnérabilités et incidents afin de pouvoir prendre des mesures de détection, de réaction aux incidents ou d'atténuation de ceux-ci. La notification inclut, s'ils sont disponibles:

   (a) les indicateurs de compromission pertinents;

   (b) les mécanismes de détection pertinents;

   (c) l'impact potentiel;

   (d) les mesures d'atténuation pertinentes.

3. Le CERT-UE soumet mensuellement à l'ENISA un rapport de synthèse contenant des données anonymisées et agrégées sur les cybermenaces importantes, les vulnérabilités importantes et les incidents importants qui ont été notifiés conformément au paragraphe 1.

4. L'IICB peut élaborer des documents d'orientation ou des recommandations concernant les modalités et le contenu de la notification. Le CERT-UE diffuse les renseignements techniques appropriés pour permettre aux institutions, organes et organismes de l'Union de prendre des mesures proactives de détection, de réaction aux incidents ou d'atténuation de ceux-ci.

5. Les obligations en matière de notification ne s'étendent pas aux ICUE ni aux informations qu'une institution, un organe ou un organisme de l'Union a reçues d'un service de sécurité ou de renseignement ou d'un service répressif d'un État membre à la condition expresse qu'elles ne soient pas partagées avec le CERT-UE.

Article 21

Coordination de la réaction aux incidents et coopération en cas d'incidents importants

1. En faisant office de pôle d'échange d'informations sur la cybersécurité et de coordination des réponses aux incidents, le CERT-UE facilite l'échange d'informations en ce qui concerne les cybermenaces, les vulnérabilités et les incidents entre:

   (a) les institutions, organes et organismes de l'Union;

   (b) les homologues visés aux articles 16 et 17.

2. Le CERT-UE facilite la coordination entre les institutions, organes et organismes de l'Union en matière de réaction aux incidents, notamment par les moyens suivants:

   (a) contribution à une communication externe cohérente;

   (b) assistance mutuelle;

   (c) utilisation optimale des ressources opérationnelles;

   (d) coordination avec d'autres mécanismes de réaction aux crises au niveau de l'Union.

3. Le CERT-UE soutient les institutions, organes et organismes de l'Union en ce qui concerne la conscience situationnelle des cybermenaces, des vulnérabilités et des incidents.

4. L'IICB élabore des orientations sur la coordination de la réaction aux incidents et la coopération en cas d'incident important. Lorsqu'il est suspecté qu'un incident est de nature criminelle, le CERT-UE conseille sur la manière de signaler l'incident aux autorités répressives.

Article 22

Attaques majeures

1. Le CERT-UE coordonne les réactions aux attaques majeures entre les institutions, organes et organismes de l'Union. Il tient à jour un inventaire de l'expertise technique qui serait nécessaire pour réagir aux incidents en cas d'attaques de ce type.

2. Les institutions, organes et organismes de l'Union contribuent à l'inventaire de l'expertise technique en fournissant une liste des experts disponibles au sein de leurs entités respectives, qui est mise à jour chaque année et détaille les compétences techniques spécifiques de ces experts.

3. Avec l'accord des institutions, organes et organismes de l'Union concernés, le CERT-UE peut aussi faire appel à des experts figurant sur la liste visée au paragraphe 2 pour contribuer à la réaction à une attaque majeure dans un État membre, conformément aux procédures opératoires de l'unité conjointe de cybersécurité.

Chapitre VI
DISPOSITIONS FINALES

Article 23
Réaffectation budgétaire initiale

La Commission propose la réaffectation du personnel et des ressources financières provenant des institutions, organes et organismes de l'Union concernés vers le budget de la Commission. La réaffectation prend effet à la même date que le premier budget adopté après l'entrée en vigueur du présent règlement.

Article 24
Réexamen

1. L'IICB, avec l'aide du CERT-UE, fait périodiquement rapport à la Commission sur la mise en œuvre du présent règlement. L'IICB peut également adresser des recommandations à la Commission en vue de proposer des modifications du présent règlement.
2. La Commission fait rapport au Parlement européen et au Conseil sur la mise en œuvre du présent règlement au plus tard 48 mois après l'entrée en vigueur du présent règlement, puis tous les trois ans.
3. La Commission évalue le fonctionnement du présent règlement et fait rapport au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions au plus tôt cinq ans après la date d'entrée en vigueur du présent règlement.

Article 25
Entrée en vigueur

Le présent règlement entre en vigueur le vingtième 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 Bruxelles, le

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaine(s) politique(s) concerné(s)

1.3. La proposition/l'initiative est relative à:

1.4. Objectif(s)

1.4.1. Objectif général/objectifs généraux

1.4.2. Objectif(s) spécifique(s)

1.4.3. Résultat(s) et incidence(s) attendus

1.4.4. Indicateurs de performance

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

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs: gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres

1.5.3. Leçons tirées d'expériences similaires

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

1.6. Durée et incidence financière de la proposition/de l'initiative

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre des financements, des modalités de paiement et de la stratégie de contrôle proposée

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

2.2.3. Estimation et justification du rapport coût-efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

2.3. Mesures de prévention des fraudes et irrégularités

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)

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

FICHE FINANCIÈRE 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 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité au sein des institutions, organes et organismes de l'Union

1.2. Domaine(s) politique(s) concerné(s)

Administration publique européenne

La proposition concerne des mesures destinées à assurer un niveau élevé commun de cybersécurité au sein des institutions, organes et organismes de l'Union

1.3. La proposition/l'initiative est relative à:

☑une action nouvelle

☐ une action nouvelle suite à un projet pilote/une action préparatoire[10]

☐ la prolongation d'une action existante

☑ une fusion ou une réorientation d'une ou de plusieurs actions vers une autre action/une action nouvelle

1.4. Objectif(s)

1.4.1. Objectif général/objectifs généraux

– Établir un cadre destiné à assurer un niveau élevé commun de cybersécurité au sein des institutions, organes et organismes de l'Union

– Fournir une nouvelle base juridique pour le CERT-UE afin de renforcer son mandat et son financement

1.4.2. Objectif(s) spécifique(s)

(1) Obliger les institutions, organes et organismes de l'Union à établir un cadre interne pour la gestion, la gouvernance et le contrôle des risques de cybersécurité

(2) Fixer les obligations incombant aux institutions, organes et organismes de l'Union en ce qui concerne la communication d'informations sur leur cadre de gestion, de gouvernance et de contrôle des risques de cybersécurité ainsi que sur les incidents de cybersécurité;

(3) Établir des règles concernant l'organisation et le fonctionnement du Centre pour la cybersécurité des institutions, organes et organismes de l'Union (CERT-UE), et concernant l'organisation et le fonctionnement du conseil interinstitutionnel de cybersécurité

(4) Contribuer à l'unité conjointe de cybersécurité

[10] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

1.4.3. Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée

– Cadres internes pour la gestion, la gouvernance et le contrôle des risques de cybersécurité, bases de référence en cybersécurité, évaluations régulières de la maturité et plans de cybersécurité au sein des institutions, organes et organismes de l'Union – Amélioration de la résilience en matière de cybersécurité et des capacités de réaction aux incidents des institutions, organes et organismes de l'Union – Modernisation du CERT-UE – Contribution à l'unité conjointe de cybersécurité

1.4.4. Indicateurs de performance

Préciser les indicateurs permettant de suivre l'avancement et les réalisations

– Cadres et bases de référence mis en place, réalisation d'évaluations régulières de la maturité et adoption de plans de cybersécurité au sein des institutions, organes et organismes de l'Union – Amélioration du traitement des incidents – Renforcement de la connaissance des risques de cybersécurité au niveau de l'encadrement supérieur des institutions, organes et organismes de l'Union – Harmonisation des dépenses en matière de sécurité informatique en pourcentage des dépenses informatiques totales – Rôle moteur renforcé du conseil interinstitutionnel de cybersécurité et du CERT-UE – Renforcement de l'échange d'informations entre les institutions, organes et organismes de l'Union et avec les organismes et parties prenantes concernés dans l'Union – Renforcement de la coopération en matière de cybersécurité avec les organismes et parties prenantes concernés dans l'Union, par l'intermédiaire du CERT-UE et de l'ENISA

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

La proposition vise à améliorer le niveau de résilience informatique des institutions, organes et organismes de l'Union, à réduire les incohérences en matière de résilience au sein de ces entités et à améliorer la conscience situationnelle et la capacité collective à se préparer et à réagir. La proposition est pleinement compatible et cohérente avec d'autres initiatives connexes, notamment la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 [proposition de directive SRI 2]. La proposition constitue un élément essentiel de la stratégie de l'UE pour l'union de la sécurité et de la stratégie de cybersécurité de l'UE pour la décennie numérique.

Il est prévu que le règlement soit proposé par la Commission européenne en octobre 2021, qu'il soit adopté par le Parlement européen et le Conseil en 2022 et que ses dispositions soient applicables à partir de son entrée en vigueur. L'incidence sur le plan des ressources humaines et financières décrite dans la présente fiche financière législative devrait commencer en 2023. Une période préparatoire a déjà commencé en 2021, mais les activités préparatoires de 2021 et 2022 ne sont pas liées à l'incidence financière de la proposition.

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs: gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres

Justification de l'action au niveau européen (ex ante)

Entre 2019 et 2021, le nombre d'incidents importants touchant des institutions, organes et organismes de l'Union et perpétrés par des acteurs de menaces persistantes avancées a considérablement augmenté. Au cours du premier semestre de 2021, on a enregistré autant d'incidents importants que sur l'ensemble de l'année 2020. Cette évolution est également visible dans le nombre de copies-images (instantanés du contenu des systèmes ou dispositifs concernés) analysées en 2020 par la CERT-UE, qui a triplé par rapport à 2019, tandis que le nombre d'incidents importants a été multiplié par plus de dix depuis 2018.

Les niveaux de maturité en matière de cybersécurité varient considérablement d'une entité à l'autre[11]. Le présent règlement garantit que l'ensemble des institutions, organes et organismes de l'Union mettent en œuvre un socle de mesures de sécurité et coopèrent en vue d'un fonctionnement ouvert et efficace de l'administration de l'Union.

Les systèmes à préserver relèvent de l'autonomie des institutions, organes et organismes de l'Union et sont gérés par ceux-ci; les actions proposées ne pourraient pas être menées par les États membres.

1.5.3. Leçons tirées d'expériences similaires

La directive SRI a été le premier instrument horizontal du marché intérieur visant à améliorer la résilience des réseaux et des systèmes dans l'Union face aux risques liés à la cybersécurité. Depuis son entrée en vigueur en 2016, elle a grandement contribué à accroître le niveau commun de cybersécurité parmi les États membres. La proposition de directive SRI 2 vise à améliorer davantage encore ces mesures.

Le règlement vise à établir des mesures similaires pour les institutions, organes et organismes de l'Union.

[11] Référence: [rapport spécial de la Cour des comptes européenne sur la cybersécurité au sein des institutions, organes et organismes de l'Union].

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

La proposition est compatible avec le cadre financier pluriannuel et constitue un élément essentiel de la stratégie de l'UE pour l'union de la sécurité et de la stratégie de cybersécurité de l'UE pour la décennie numérique.

La proposition envisage l'application de mesures destinées à assurer un niveau élevé commun de cybersécurité au sein des institutions, organes et organismes de l'Union La proposition est cohérente avec la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 [proposition de directive SRI 2].

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

La gestion des tâches par le CERT-UE requiert des profils spécifiques et implique une charge de travail supplémentaire qui ne peut pas être absorbée sans une augmentation des ressources humaines et financières.

1.6. Durée et incidence financière de la proposition/de l'initiative

☐ **durée limitée**

– ☐ En vigueur à partir de [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**

– L'incidence financière devrait commencer avec le premier budget adopté après l'entrée en vigueur du règlement. Une réaffectation de ressources des institutions et des principaux organismes de l'Union vers la Commission aurait lieu au cours de la première année, considérée comme une année de transition; cette réaffectation de ressources ainsi que d'autres (ré)affectations auront lieu dans le cadre des budgets annuels. Si le règlement est adopté en 2022, l'exercice 2023 constituera la période transitoire et l'exercice 2024 sera celui du fonctionnement à grande échelle.

1.7. Mode(s) de gestion prévu(s)[12]

☑ **Gestion directe** par la Commission et par chaque institution, organe et organisme de l'Union

– ☑ 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 aux organismes qu'ils ont désignés;

– ☐ à des organisations internationales et à leurs agences (à préciser);

– ☐ à la BEI et au Fonds européen d'investissement;

– ☐ aux organismes visés aux articles 70 et 71 du règlement financier;

– ☐ à des organismes de droit public;

– ☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

– ☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

– ☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné

– *Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

Remarques

[12] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/FR/man/budgmanag/Pages/budgmanag.aspx

Pour l'application des procédures administratives et financières, le CERT-UE agit sous l'autorité de la Commission.

Ressources supplémentaires découlant du projet de règlement:

La mise en œuvre des articles 12 et 13 du projet de règlement conduit à un catalogue de services élargi avec des services de base supplémentaires. Lors du fonctionnement à grande échelle, les ressources supplémentaires suivantes seront nécessaires (jusqu'à la fin du cadre financier pluriannuel à la fin de 2027): 21 ETP et 14,05 millions d'EUR.

La ventilation des ressources supplémentaires du budget entre les différentes tâches est la suivante:

(a) pour l'exécution des tâches pour les institutions, organes et organismes de l'Union détaillées à l'article 12, paragraphe 2, points a), b), c) et e): 13,75 ETP et 11,275 millions d'EUR;

(b) pour l'exécution des tâches détaillées à l'article 12, paragraphe 3 (contribution à l'unité conjointe de cybersécurité): 2 ETP et 381 000 EUR;

(c) pour l'exécution des tâches détaillées à l'article 12, paragraphe 4 (coopération structurée avec l'ENISA): 0,25 ETP et 236 000 EUR;

(d) pour l'exécution des tâches détaillées à l'article 12, paragraphe 6 (exercices dans le domaine de la cybersécurité): 0,25 ETP et 79 000 EUR;

(e) pour l'exécution des tâches détaillées à l'article 12, paragraphe 2, point d), et à l'article 13 (analyse et rapports sur la mise en œuvre du règlement, préparation des documents d'orientation, des recommandations et des appels à l'action): 3,75 ETP et 2,079 millions d'EUR;

(f) pour l'exécution des tâches d'appui au secrétariat du conseil interinstitutionnel de cybersécurité: 1 ETP.

Vue d'ensemble des ressources actuelles et de la transition vers le fonctionnement à pleine échelle:

En septembre 2021, la CERT-UE fonctionnait avec les ressources suivantes:

- emplois permanents et détachés: 14 ETP;

- agents contractuels financés dans le cadre d'accords de niveau de service: 24 ETP;

- total: 38 ETP.

Le budget de la CERT-UE en 2020 était le suivant: 250 000 EUR provenant du budget de la Commission et 3,5 millions d'EUR au titre de recettes affectées dans le cadre d'accords de niveau de service. Total: 3,75 millions d'EUR. Ce montant représentait l'ensemble du budget de la CERT-UE, couvrant les formations, le matériel informatique, les logiciels, les missions, le soutien, les agents contractuels et les conférences.

Après l'entrée en vigueur du règlement, les ressources futures du CERT-UE devraient être les suivantes:

- emplois permanents: 34 ETP;

- agents contractuels: 15 ETP;

- total: 49 ETP, soit une augmentation nette de 11 ETP.

Le changement de ratio entre les emplois permanents et les agents contractuels vise à remédier aux difficultés persistantes rencontrées pour recruter et conserver des professionnels de la cybersécurité de haut niveau en raison de leur rareté sur le marché du travail.

En outre, un agent contractuel ETP sera requis au sein de la direction générale de l'informatique de la Commission pour soutenir le conseil interinstitutionnel de cybersécurité.

En tout, 21 ETP supplémentaires seront donc nécessaires pour mettre en œuvre le règlement (20 ETP pour le CERT-UE et 1 ETP pour la direction générale de l'informatique de la Commission). Ces recrutements seront compensés par une suppression parallèle, au sein du CERT-UE, de 9 postes d'agents contractuels ETP, qui étaient auparavant financés par des recettes affectées dans le cadre d'accords de niveau de service.

Le budget des ressources non humaines du CERT-UE en 2024 après la période de transition couvrira les tâches visées aux points a) à e) ci-dessus et devrait être financé comme suit:

- 8,921 millions d'EUR par an provenant des institutions de l'Union, au titre de la rubrique 7 du budget de l'Union;

- 2,459 millions d'EUR provenant des institutions, organes et organismes de l'Union, au titre des rubriques 1 à 6 du budget de l'Union;

- 2,670 millions d'EUR provenant des institutions, organes et organismes de l'Union autofinancés;

- budget total du CERT-UE: 14,05 millions d'EUR.

Les tâches visées à l'article 12, paragraphe 5, ne sont pas décrites dans le catalogue de services du CERT-UE; il s'agit de services payants. Il s'agit de services accessoires, pour des montants relativement faibles, pour la plupart temporaires, et leurs coûts seront récupérés auprès des bénéficiaires des services au moyen d'accords de niveau de service ou d'accords écrits.

En ce qui concerne les contributions au personnel du CERT-UE: les institutions et principaux organismes de l'Union contribuent à hauteur d'une part équitable qui est proportionnelle à la part respective des postes permanents AD de l'organisation. Il faut voir si la BCE et la BEI peuvent également apporter une contribution équitable en détachant du personnel permanent.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions

La Commission, avec l'aide du conseil interinstitutionnel de cybersécurité et du CERT-UE, réexaminera périodiquement le fonctionnement du règlement et fera rapport au Parlement européen et au Conseil, la première fois au plus tard 48 mois après l'entrée en vigueur du présent règlement, et tous les trois ans par la suite.

Les sources de données utilisées pour les réexamens proviendront principalement du conseil interinstitutionnel de cybersécurité et du CERT-UE. En outre, des outils spécifiques de collecte de données (enquêtes auprès des institutions, organes et organismes de l'Union, de l'ENISA ou du réseau des CSIRT, par exemple) pourraient être utilisés si nécessaire.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre des financements, des modalités de paiement et de la stratégie de contrôle proposée

Les actions découlant du règlement seront gérées au sein de chaque institution, organe et organisme de l'Union conformément à ses règles et réglementations applicables en la matière.

La gestion administrative et financière des activités du CERT-UE est intégrée à l'administration de la Commission et suit les mécanismes de gestion et de mise en œuvre, les modalités de paiement et les contrôles applicables de celle-ci.

L'auditeur interne de la Commission exerce à l'égard du CERT-UE les mêmes pouvoirs que ceux qui lui sont attribués à l'égard des services de la Commission.

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

Risque très faible, étant donné que la CERT-UE est déjà rattachée administrativement, en tant qu'équipe spéciale de la Commission, au directeur général de l'informatique et que le conseil interinstitutionnel de cybersécurité suit le modèle de l'actuel comité de pilotage de la CERT-UE. L'écosystème de gestion financière et de contrôle interne est donc déjà en place.

2.2.3. Estimation et justification du rapport coût-efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

Des procédures bien éprouvées de passation de marchés, de gestion financière et de contrôle sont déjà en place. Le rapport coût-efficacité des contrôles et les niveaux de risque d'erreur correspondent à ceux de chaque institution, organe et organisme de l'Union et à ceux de la Commission pour les activités de la CERT-UE.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple

Les systèmes de gestion financière et de contrôle interne de la Commission s'appliquent aux activités du CERT-UE.

Aux fins de la lutte contre la fraude, la corruption et les autres actes illégaux, les dispositions du 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) 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 financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro	CD/CND[13]	de pays AELE[14]	de pays candidats[15]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
1 à 6	Lignes budgétaires couvrant les contributions de l'Union aux agences et organismes décentralisés	CD	NON	NON	NON	NON
7	Lignes budgétaires couvrant les rémunérations du personnel, les dépenses informatiques et les autres dépenses administratives dans les différentes sections du budget de l'UE	CND	NON	NON	NON	NON

- Nouvelles lignes budgétaires, dont la création est demandée

Dans l'ordre 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	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
	Néant		OUI/NON	OUI/NON	OUI/NON	OUI/NON

[13] CD = crédits dissociés / CND = crédits non dissociés.
[14] AELE: Association européenne de libre-échange.
[15] 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:

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	1 à 6	Rubriques couvrant les contributions aux agences et organismes décentralisés

DG: plusieurs			Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
○ Crédits opérationnels								
Lignes budgétaires couvrant les contributions de l'Union aux agences décentralisées (xx 10 xx xx)[16]	Engagements	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Paiements	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[17]								
Ligne budgétaire		(3)						
TOTAL des crédits pour la DG: plusieurs	Engagements	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Paiements	=2a+2b +3	2,459	2,459	2,459	2,459	2,459	12,293

16 Selon la nomenclature budgétaire officielle.

17 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'Union (anciennes lignes «BA»), recherche indirecte, recherche directe.

○ TOTAL des crédits opérationnels	Engagements	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Paiements	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		(6)						
TOTAL des crédits pour les RUBRIQUES 1 à 6 du cadre financier pluriannuel	Engagements	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Paiements	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Si plusieurs rubriques opérationnelles sont concernées par la proposition/l'initiative, dupliquer la section qui précède:

○ TOTAL des crédits opérationnels (toutes les rubriques opérationnelles)	Engagements	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Paiements	(5)	2,459	2,459	2,459	2,459	2,459	12,293
TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques (toutes les rubriques opérationnelles)		(6)						
TOTAL des crédits pour les RUBRIQUES 1 à 6 du cadre financier pluriannuel (Montant de référence)	Engagements	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Paiements	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Rubrique du cadre financier pluriannuel	7	«Dépenses administratives»

Cette partie est à compléter en utilisant les «données budgétaires de nature administrative», à introduire d'abord dans l'annexe de la fiche financière législative (annexe V des règles internes), à charger dans DECIDE pour les besoins de la consultation interservices.

En Mio EUR (à la 3e décimale)

		Année **2023**	Année **2024**	Année **2025**	Année **2026**	**Année 2027**	**TOTAL**
DG: DIGIT (CERT-UE)							
○ Ressources humaines		1,184	2,126	2,754	3,225	3,225	12,514
○ Autres dépenses administratives		7,938	8,921	8,921	8,921	8,921	43,622
TOTAL DG DIGIT (CERT-UE)	Crédits	9,122	11,047	11,675	12,146	12,146	56,136

TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel	(Total des engagements = Total des paiements)	9,122	11,047	11,675	12,146	12,146	**56,136**

En Mio EUR (à la 3e décimale)

		Année 2023	Année 2024	Année 2025	Année 2026	Année 20 27	**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 7 du cadre financier pluriannuel (*)	Engagements	11,581	13,506	14,134	14,605	14,605	68,429
	Paiements	11,581	13,506	14,134	14,605	14,605	68,429

(*) Les contributions des institutions, organes et organismes de l'Union autofinancés sont estimées à 2,670 millions d'EUR par an (soit un total de 13,350 millions d'EUR pour les cinq années). Ces contributions constitueront des recettes affectées au CERT-UE. Les tableaux ci-dessus n'incluent que l'incidence totale estimée sur le budget de l'Union et n'incluent pas ces contributions.

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations ⇩			Année **N**		Année **N+1**		Année **N+2**		Année **N+3**		Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)						**TOTAL**	
			RÉALISATIONS															
	Type[18]	Coût moyen	Nbre	Coût	Non	Coût	Non	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[19]…																		
- Réalisation																		
- Réalisation																		
- Réalisation																		
Sous-total objectif spécifique nº 1																		
OBJECTIF SPÉCIFIQUE nº 2…																		
- Réalisation																		
Sous-total objectif spécifique nº 2																		
TOTAUX																		

[18] 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.).

[19] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

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:

En Mio EUR (à la 3e décimale)

	Année 2023	Année 2024	Année 2025	Année 2026	Année 2027	**TOTAL**
RUBRIQUE 7 du cadre financier pluriannuel						
Ressources humaines						
Personnel permanent (grades AD)	1,099	2,041	2,669	3,14	3,14	12,089
Agents contractuels	0,085	0,085	0,085	0,085	0,085	0,425
Autres dépenses administratives	7,938	8,921	8,921	8,921	8,921	43,622
Sous-total RUBRIQUE 7 du cadre financier pluriannuel	9,122	11,047	11,675	12,146	12,146	56,136

Hors RUBRIQUE 7[20] du cadre financier pluriannuel						
Ressources humaines						
Autres dépenses de nature administrative						
Sous-total hors RUBRIQUE 7 du cadre financier pluriannuel						

TOTAL	9,122	11,047	11,675	12,146	12,146	56,136

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

[20] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'Union (anciennes lignes «BA»), recherche indirecte, recherche directe.

3.2.3.1. Besoins estimés en ressources humaines

– ☐ 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:

Estimation à exprimer en équivalents temps plein

		Année 2023	Année 2024	Année 2025	Année 2026	Année 2027		
O Emplois du tableau des effectifs (fonctionnaires et agents temporaires)								
20 01 02 01 (au siège et dans les bureaux de représentation de la Commission)		7	13	17	20	20		
20 01 02 03 (en délégation)								
01 01 01 01 (recherche indirecte)								
01 01 01 11 (recherche directe)								
Autres lignes budgétaires (à préciser)								
O Personnel externe (en équivalent temps plein: ETP)[21]								
20 02 01 (AC, END, INT de l'«enveloppe globale»)		1	1	1	1	1		
20 02 03 (AC, AL, END, INT et JPD dans les délégations)								
XX 01 xx **yy zz** [22]	- au siège							
	- en délégation							
01 01 01 02 (AC, END, INT sur recherche indirecte)								
01 01 01 12 (AC, END, INT sur recherche directe)								
Autres lignes budgétaires (à préciser)								
TOTAL		**8**	**14**	**18**	**21**	**21**		

XX est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Les fonctionnaires exécuteront les tâches et activités du CERT-UE conformément au règlement, en particulier aux chapitres IV et V.
Personnel externe	L'agent contractuel appuiera les fonctions de secrétariat du conseil interinstitutionnel de cybersécurité.

[21] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

[22] Sous-plafond de personnel externe financé sur crédits opérationnels (anciennes lignes «BA»).

3.2.4. 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).

Expliquez la reprogrammation requise, en précisant les lignes budgétaires concernées et les montants correspondants. Veuillez fournir un tableau Excel en cas de reprogrammation de grande envergure.

– ☐ 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.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées, les montants correspondants et les instruments dont le recours est proposé.

– ☐ nécessite une révision du CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants.

3.2.5. Participation de tiers au financement

La proposition/l'initiative:

– ☑ ne prévoit pas de cofinancement par des tierces parties[23]

– ☐ prévoit le cofinancement par des tierces parties estimé ci-après:

Crédits en Mio EUR (à la 3e décimale)

	Année **N**[24]	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			Total
Préciser l'organisme de cofinancement								
TOTAL des crédits cofinancés								

[23] Les recettes affectées provenant de la fourniture sporadique de services à des organisations non parties au titre de l'article 12, paragraphe 5, point c), n'ont pas été estimées parce qu'elles devraient être marginales.

[24] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

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[25]						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)		
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).

[25] 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.