Conseil de
l'Union européenne

Bruxelles, le 31 octobre 2022
(OR. en)

14128/22

Dossier interinstitutionnel:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

NOTE POINT "I/A"

Origine:	Secrétariat général du Conseil
Destinataire:	Comité des représentants permanents (2e partie)/Conseil
Nº doc. préc.:	10097/5/22 REV 5
N° doc. Cion:	7474/22 + ADD 1
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 - Orientation générale

INTRODUCTION

1. Le 22 mars 2022, la Commission a adopté la proposition de règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union. La proposition était l'une des mesures prévues dans la stratégie de cybersécurité de l'UE pour la décennie numérique[1], qui vise à renforcer la résilience collective de l'Union contre les cybermenaces.

[1] 14133/20.

Dans ses conclusions du 22 mars 2021 sur cette stratégie[2], le Conseil a souligné que la cybersécurité était essentielle au fonctionnement de l'administration et des institutions publiques, tant au niveau national qu'au niveau de l'UE, ainsi que pour notre société et l'économie dans son ensemble.

2. La proposition de la Commission, fondée sur l'article 298 du traité sur le fonctionnement de l'Union européenne, vise à améliorer le niveau de cybersécurité au sein des institutions, organes et organismes de l'Union en établissant un cadre commun, dans le respect de l'autonomie de chaque entité de l'Union. En particulier, les objectifs de la proposition sont les suivants:

   – renforcer le mandat et le financement de la CERT-UE (équipe interinstitutionnelle autonome d'intervention en cas d'urgence informatique pour les entités de l'Union);

   – mettre en place une structure interinstitutionnelle (conseil interinstitutionnel de cybersécurité - IICB) réunissant des représentants de toutes les entités de l'Union afin de s'assurer de la bonne mise en œuvre du règlement;

   – introduire l'obligation pour les entités de l'Union de partager avec la CERT-UE des informations (non classifiées) concernant les incidents et de notifier les menaces, vulnérabilités et incidents significatifs; et

   – promouvoir la coordination et la coopération dans le cadre de la réaction aux incidents significatifs.

3. Le Parlement européen a nommé Mme Henna Virkkunen (EPP) rapporteure de la commission ITRE, compétente au fond. Le projet de rapport a été rendu public le 7 octobre 2022.

4. Le Contrôleur européen de la protection des données a rendu son avis le 17 mai 2022[3].

[2] 6722/21.
[3] 9252/22.

5. Au Conseil, l'examen de la proposition au sein du groupe horizontal "Questions cyber" (GHQC) a débuté le 29 mars 2022, pendant la présidence française. La présidence française a élaboré un premier texte de compromis, qui a été examiné par le GHQC en juin 2022, et a présenté au Conseil un rapport sur l'état d'avancement des travaux[4] le 21 juin 2022.

6. Au cours de la présidence tchèque, le GHQC a consacré huit réunions[5] aux discussions sur la proposition et sur plusieurs textes de compromis consécutifs.

7. Le 23 mai 2022, la présidence a demandé au Comité de sécurité du Conseil de rendre un avis sur les aspects de la proposition relatifs à la sécurité de l'information et, en particulier, aux informations classifiées. Le comité a rendu son avis le 19 septembre 2022[6]. Comme l'a suggéré le comité, les informations classifiées de l'UE ont été explicitement exclues du champ d'application du règlement. Les dispositions relatives aux exemptions des obligations de partage et de déclaration liées aux informations reçues de l'extérieur des entités de l'Union ont été modifiées en conséquence.

8. Le 28 octobre 2022, le GHQC est parvenu à un accord sur le compromis de la présidence qui figure en annexe.

---

4 9719/22.
5 6 et 20 juillet, 13, 21 et 28 septembre, 5, 19 et 28 octobre 2022.
6 12603/22 + COR 1.

PRINCIPALES QUESTIONS

9. Les États membres se sont félicités que la proposition soit présentée en temps utile et en complément de la future directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2) et ont soutenu ses objectifs généraux. Toutefois, les États membres ont plaidé en faveur d'un alignement plus poussé sur la directive SRI 2 et d'une plus grande réciprocité dans l'échange d'informations entre les entités de l'Union et les États membres, et ont relevé le caractère excessivement volontaire de certaines des mesures proposées. Les États membres ont également indiqué qu'ils préféraient que les références à l'unité conjointe de cybersécurité (dont le mandat et la composition restent à définir) soient supprimées.

10. Sur la base des discussions menées au niveau du GHQC, les points suivants ont été identifiés comme constituant les principales questions politiques:

a) Alignement sur la future directive SRI 2

Comme l'ont demandé les États membres, l'alignement sur la future directive SRI 2 a été renforcé, notamment:

- un certain nombre de définitions (article 3) ont été alignées sur celles de la directive SRI 2;
- un nouvel article 7 *bis* a été inséré sur les examens volontaires par les pairs, conformément à la directive SRI 2, adaptés aux besoins des entités de l'Union;
- les obligations de déclaration prévues à l'article 20 ont été alignées sur celles de la directive SRI 2.

b) Composition du conseil interinstitutionnel de cybersécurité (IICB) (article 9)

À la suite de discussions sur la façon appropriée d'associer des représentants des États membres aux travaux de l'IICB, un compromis a été trouvé au moyen d'une déclaration du Conseil inscrite au procès-verbal.

c) Autonomie institutionnelle

Une approche équilibrée a été trouvée entre la volonté des États membres de renforcer les mécanismes de contrôle du respect et la nécessité de préserver le principe d'autonomie institutionnelle, notamment en ce qui concerne les audits et les mesures disciplinaires (article 11).

Enfin, la mention relative à un pourcentage spécifique du budget informatique consacré à la cybersécurité a été supprimée du considérant 8.

CONCLUSIONS

11. Le Comité des représentants permanents est invité à:

a) approuver le texte de compromis figurant en annexe, qui constituera ensuite le mandat de négociation avec le Parlement européen;

b) inviter le Conseil à approuver le texte de compromis qui figure en annexe lors de sa session du 18 novembre 2022 et à inscrire au procès-verbal la déclaration du Conseil qui figure dans l'addendum au présent document.

ANNEXE

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 [...] **entités** 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 [...] **entités** 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 [...] **entité** 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 [...] **entités de l'Union** 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. **Par ailleurs, les entités de l'Union traitent de grandes quantités d'informations souvent sensibles provenant des États membres, de sorte que les incidents pourraient également avoir des répercussions négatives sur les États membres. C'est pourquoi la cybersécurité des entités de l'Union revêt également une grande importance pour les États membres. Les informations concernant des incidents spécifiques peuvent également faciliter la détection de cybermenaces ou d'incidents similaires affectant les États membres.**

(4) Les [...] **entités** 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 cyberrésilience 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 [...] **entités** de l'Union atteignent un niveau élevé commun de cybersécurité grâce **à la mise en œuvre de mesures 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 [...] **entités** 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 [...] **entité** 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 [...]. **Le cadre devrait définir des politiques en matière de cybersécurité, y compris des procédures visant à évaluer l'efficacité des mesures de cybersécurité mises en œuvre. Le cadre devrait reposer sur une approche "tous risques", qui vise à protéger les réseaux et les systèmes d'information ainsi que l'environnement physique de ces systèmes contre des événements tels que les vols, les incendies, les inondations et les pannes d'électricité ou de télécommunications, contre l'accès physique non autorisé aux installations d'information et de traitement des informations de l'entité de l'Union, ainsi que contre les dommages à ces installations et les interférences avec ces installations, qui pourraient compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises, traitées ou accessibles par l'intermédiaire des réseaux et des systèmes d'information**. **Le cadre devrait intégrer les conclusions de l'analyse des risques, en tenant compte de l'ensemble des risques techniques, opérationnels et organisationnels pertinents pour la cybersécurité de l'entité de l'Union concernée.**

(6a) Pour gérer les risques recensés dans le cadre, chaque entité de l'Union devrait veiller à ce que des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées soient prises. Celles-ci devraient porter sur les domaines, y compris les mesures de cybersécurité énoncées dans le présent règlement afin de renforcer la cybersécurité de chaque entité de l'Union.

(6 *ter*) Les actifs et les risques recensés dans le cadre ainsi que les conclusions tirées des évaluations régulières de la maturité devraient être pris en compte dans le plan de cybersécurité établi par chaque entité de l'Union. Le plan de cybersécurité devrait inclure les mesures de cybersécurité adoptées, dans le but d'accroître la cybersécurité globale de l'entité de l'Union concernée.

(6 *quater*) Étant donné qu'assurer la cybersécurité est un processus continu, il conviendrait de réexaminer régulièrement l'adéquation et l'efficacité de toutes les mesures à la lumière de l'évolution des risques, des actifs et de la maturité des entités de l'Union. Le cadre devrait être réexaminé à intervalles réguliers et au moins tous les trois ans, tandis que le plan de cybersécurité devrait être révisé au moins tous les deux ans ou à la suite de chaque évaluation de la maturité ou de chaque réexamen du cadre.

(6 *quinquies*) Les entités de l'Union devraient échanger régulièrement les informations utiles, y compris en ce qui concerne les incidents et les cybermenaces pertinents, tout en garantissant la confidentialité et la protection appropriée des informations fournies par l'entité de l'Union qui les communique.

(6 *sexies*) Il convient de mettre en œuvre un mécanisme visant à garantir l'efficacité de l'échange d'informations, de la coordination et de la coopération entre les entités de l'Union en cas d'incidents majeurs, y compris une identification claire des rôles et des responsabilités des entités de l'Union concernées. Les informations échangées devraient être prises en compte par le point de contact désigné pour le réseau CyCLONe lorsque des informations pertinentes sont partagées avec ce réseau pour contribuer à l'appréciation commune de la situation.

(7) En raison des différences entre les [...] **entités** 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 [...] **entités** de l'Union ou qui empiètent sur leur autonomie institutionnelle. Il convient, par conséquent, que ces [...] **entités de l'Union** établissent leurs propres cadres de gestion, de gouvernance et de contrôle des risques de cybersécurité **ainsi que leurs propres plans de cybersécurité**, et adoptent des [...] **mesures** de cybersécurité [...]. **Lors de la mise en œuvre de ces mesures, il convient de tenir dûment compte des synergies existant entre les entités de l'Union, en vue d'une bonne gestion des ressources et d'une optimisation des coûts. Il convient également de veiller comme il se doit à ce que les mesures n'aient pas d'incidence négative sur l'efficacité de l'échange d'informations et des opérations menées par les entités de l'Union avec d'autres entités de l'Union et les autorités nationales compétentes.**

(8) Pour éviter que la charge financière et administrative imposée aux [...] **entités** 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 [...] **entité** de l'Union devrait s'efforcer d'allouer un pourcentage adéquat de son budget informatique à l'amélioration de son niveau de cybersécurité. [...] **L'évaluation de la maturité devrait également déterminer si les dépenses de cybersécurité de l'entité de l'Union sont proportionnées aux risques auxquels elle est confrontée.**

(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 [...] **entité** de l'Union. **[...] Le niveau hiérarchique le plus élevé devrait superviser la mise en œuvre du présent règlement, y compris l'établissement du cadre de gestion, de gouvernance et de contrôle des risques et des plans de cybersécurité, comprenant des mesures de cybersécurité.** La prise en compte de la culture de la cybersécurité, c'est-à-dire la pratique quotidienne de la cybersécurité, fait partie intégrante [...] **d'un cadre de** cybersécurité dans l'ensemble des [...] **entités** de l'Union.

(10) [...] [...] Ces mesures **de cybersécurité** devraient faire partie [...] **du plan de** cybersécurité et être précisées dans des documents d'orientation ou des recommandations publiés par la CERT-UE. Lors de la définition des mesures et des lignes directrices, il convient de tenir dûment compte **de l'état de la technique et, le cas échéant, des normes européennes et internationales applicables, ainsi que** 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. **Lorsque c'est approprié, la CERT-UE devrait coopérer avec l'ENISA.**

(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[7]. [...] **Le présent règlement devrait prévoir un ensemble complet de règles relatives à l'organisation et au fonctionnement de la CERT-UE**. **Les dispositions du présent règlement prévalent sur les dispositions de l'accord interinstitutionnel sur l'organisation et le fonctionnement de la CERT-UE conclu en décembre 2017**.

[...]

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

(13) De nombreuses cyberattaques s'inscrivent dans le cadre de campagnes plus larges qui ciblent des groupes [...] **d'entités** de l'Union ou de communautés d'intérêt auxquelles appartiennent les [...] **entités** de l'Union. Afin de permettre la détection proactive, la réaction en cas d'incident ou l'adoption de mesures d'atténuation, les [...] **entités** de l'Union devraient notifier à la CERT-UE les cybermenaces [...], les vulnérabilités [...], **les incidents évités ainsi que** les incidents [...] et partager les renseignements techniques appropriés permettant de détecter ou d'atténuer les cybermenaces, vulnérabilités**, incidents évités** et incidents similaires, ainsi que de réagir à ces menaces, vulnérabilités, **incidents évités** et incidents dans d'autres [...] **entités** de l'Union. Suivant la même approche que celle envisagée dans la directive [proposition SRI 2], lorsque les entités **de l'Union** ont connaissance d'un incident important, elles devraient être tenues de [...] **déclencher une alerte rapide auprès de la** CERT-UE dans un délai de 24 heures. Cet échange d'informations devrait permettre à la CERT-UE de communiquer les informations à d'autres [...] **entités** 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 [...] similaires.

(13 *bis*) Le présent règlement établit une approche en plusieurs étapes du signalement des incidents importants afin de trouver le juste équilibre entre, d'une part, le signalement rapide qui aide à atténuer la propagation potentielle des incidents importants et permet aux entités de l'Union de chercher de l'aide et, d'autre part, le signalement approfondi qui permet de tirer des leçons précieuses des incidents individuels et d'améliorer au fil du temps la cyberrésilience de chaque entité de l'Union. À cet égard, le présent règlement devrait inclure le signalement des incidents qui, sur la base d'une évaluation initiale effectuée par l'entité de l'Union, pourraient entraîner des perturbations opérationnelles graves du fonctionnement de l'entité de l'Union ou des pertes financières pour l'entité de l'Union concernée, ou nuire à d'autres personnes physiques ou morales en causant des préjudices matériels ou non matériels considérables. Cette évaluation initiale devrait tenir compte, entre autres, des réseaux et des systèmes d'information touchés et notamment de leur importance pour le fonctionnement de l'entité de l'Union, de la gravité et des caractéristiques techniques de la cybermenace et de toutes les vulnérabilités sous-jacentes qui sont exploitées ainsi que de l'expérience de l'entité de l'Union en matière d'incidents similaires. Des indicateurs tels que la mesure dans laquelle le fonctionnement de l'entité de l'Union est affecté, la durée d'un incident ou le nombre de personnes physiques ou morales touchées pourraient jouer un rôle important pour déterminer si la perturbation opérationnelle est grave.

(13 *ter*) Étant donné que les infrastructures et les réseaux de l'entité de l'Union concernée et de l'État membre dans lequel cette entité de l'Union est située sont interconnectés, il est essentiel que cet État membre soit informé sans retard injustifié de tout incident important survenu au sein de cette entité de l'Union. À cette fin, l'entité de l'Union touchée devrait notifier la contrepartie nationale de la CERT-UE, désignée par l'État membre conformément à la directive [proposition SRI 2], en respectant le même délai que pour le signalement d'un incident important à la CERT-UE. La CERT-UE devrait également informer cette contrepartie nationale lorsqu'elle a connaissance d'un incident important survenu dans l'État membre, à moins que l'entité de l'Union touchée ne l'ait déjà signalé.

(14) Outre l'extension des missions de la CERT-UE et l'élargissement de son rôle, il convient de créer un conseil interinstitutionnel de cybersécurité (IICB) qui [...] **devrait jouer**, **en vue de** faciliter l'instauration d'un niveau élevé commun de cybersécurité parmi les [...] **entités** de l'Union, **un rôle exclusif pour la surveillance de** [...] la mise en œuvre du présent règlement par les [...] **entités** de l'Union [...], **la supervision de** la mise en œuvre des priorités et des objectifs généraux par la CERT-UE et [...] **et la fourniture d'**orientations stratégiques à la CERT-UE. **Par conséquent,** 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. **L'organisation et le fonctionnement de l'IICB devraient également être régis par son règlement intérieur, qui pourrait inclure des précisions sur les réunions régulières de l'IICB, y compris les réunions annuelles au niveau politique, lors desquelles les représentants du niveau hiérarchique le plus élevé de chaque membre de l'IICB tiendraient des discussions stratégiques pour l'IICB et lui fourniraient des orientations stratégiques. En outre, l'IICB peut instituer un comité exécutif chargé de l'assister dans ses travaux et lui déléguer certaines de ses tâches et compétences, surtout en ce qui concerne les tâches nécessitant [...] une expertise spécifique chez ses membres, par exemple l'approbation du catalogue de services et de toute mise à jour ultérieure de celui-ci, ainsi que des modalités des accords sur le niveau de service, les évaluations des documents et rapports soumis par les entités de l'Union à l'IICB conformément au présent règlement ou les tâches liées à la préparation des décisions relatives aux mesures de contrôle du respect adoptées par l'IICB et au suivi de leur mise en œuvre. L'IICB devrait établir le règlement intérieur du comité exécutif, y compris ses tâches et pouvoirs.**

(15) La 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, la CERT-UE devrait lancer des appels à l'action décrivant les mesures de sécurité urgentes que les [...] **entités** de l'Union sont vivement encouragées à prendre dans un délai déterminé. **L'IICB peut donner instruction à la CERT-UE d'élaborer, de retirer ou de modifier une proposition de documents d'orientation ou de recommandation, ou un appel à l'action.**

(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 [...]. 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 la CERT-UE, les [...] **entités** de l'Union et d'autres parties prenantes, le cas échéant. **[...] Lorsque l'IICB constate que les entités de l'Union n'ont pas appliqué ou mis en œuvre le présent règlement, y compris les documents d'orientation, les recommandations ou les appels à l'action élaborés au titre du présent règlement, il peut, sans préjudice des procédures internes de l'entité de l'Union concernée, prendre des mesures de contrôle du respect. L'application du système de mesures de contrôle du respect devrait être d'une sévérité progressive, ce qui signifie que, lorsque l'IICB adopte les mesures de contrôle du respect, il devrait commencer par un avertissement, qui constitue la mesure la moins sévère, et, si nécessaire, aller jusqu'à la mesure la plus sévère, consistant à émettre un avis recommandant la suspension temporaire des flux de données vers l'entité de l'Union concernée, mesure qui serait appliquée dans des cas exceptionnels de non-respect persistant, délibéré et/ou grave par l'entité concernée de l'obligation qui lui incombe en vertu du présent règlement.**

(16 *bis*) L'avertissement, qui constitue la mesure de contrôle du respect la moins sévère, vise à remédier aux lacunes constatées de l'entité de l'Union et comprend des recommandations en vue de modifier les documents de cybersécurité de l'entité de l'Union dans un délai déterminé. L'avertissement devrait être à la disposition de toutes les entités de l'Union, sauf s'il fait l'objet de restrictions appropriées conformément au présent règlement.

(16 *ter*) L'IICB peut en outre recommander la réalisation d'un audit d'une entité de l'Union. L'entité de l'Union peut recourir à sa fonction d'audit interne à cette fin. L'IICB pourrait également demander qu'un audit soit effectué par un service d'audit tiers, y compris par un prestataire de services du secteur privé convenu d'un commun accord.

(16 *quater*) Sur la base des résultats d'un audit effectué sur sa recommandation ou à sa demande, l'IICB peut en outre demander à l'entité de l'Union de mettre la gestion, la gouvernance et le contrôle des risques de cybersécurité en conformité avec les dispositions du présent règlement.

(16 *quinquies*) Étant donné que les États membres partagent avec les entités de l'Union concernées des informations susceptibles d'être sensibles, la cybersécurité du destinataire de ces informations est essentielle pour les États membres. Par conséquent, dans des cas exceptionnels de non-respect persistant, délibéré, répété et/ou grave de l'obligation qui incombe à l'entité de l'Union, l'IICB peut émettre, en dernier ressort, un avis à l'intention de tous les États membres et entités de l'Union recommandant la suspension temporaire des flux de données à destination de l'entité de l'Union, qui devrait s'appliquer jusqu'à ce que le niveau de la cybersécurité dans cette entité se soit amélioré. Cet avis devrait être communiqué à tous les États membres et à toutes les entités de l'Union par des canaux de communication sécurisés appropriés.

(16 *sexies*) Afin de garantir la bonne mise en œuvre du présent règlement, l'IICB devrait, s'il estime qu'une violation persistante du présent règlement par une entité de l'Union est directement imputable aux actions ou omissions d'un membre de son personnel, y compris au niveau hiérarchique le plus élevé, demander à l'entité de l'Union concernée de prendre les mesures appropriées à l'encontre de ce membre du personnel, conformément au statut des fonctionnaires ainsi qu'aux autres règles équivalentes applicables dans certaines entités de l'Union. Ces mesures peuvent comprendre, par exemple, une procédure disciplinaire et, lorsqu'il y a lieu, dans le cas spécifique des agences de l'Union, une demande à l'autorité compétente de prendre les mesures nécessaires en vue d'une éventuelle révocation de la personne qui pourrait être responsable de la violation persistante du présent règlement.

(17) La CERT-UE devrait avoir pour mission de contribuer à la sécurité de l'environnement informatique de l'ensemble des [...] **entités** de l'Union. **Lorsqu'elle envisage, à la demande d'une entité de l'Union, de fournir des conseils ou des contributions techniques sur des questions politiques pertinentes, la CERT-UE devrait veiller à ce que cela n'entrave pas l'accomplissement de ses autres tâches énoncées dans le présent règlement.**

(17 *bis*) La CERT-UE devrait jouer un rôle équivalent à celui de coordinateur désigné pour les [...] **entités** 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] **et devrait élaborer une politique de gestion des vulnérabilités visant notamment à promouvoir et à faciliter la divulgation volontaire et coordonnée des vulnérabilités**.

[...]

(19) La 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 de la Commission[8], la 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, la CERT-UE devrait partager avec ses homologues nationaux des informations spécifiques aux incidents. Elle 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.

[8] 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).

(20) Pour soutenir la cybersécurité opérationnelle, la CERT-UE devrait faire appel à l'expertise disponible de l'Agence de l'Union européenne pour la cybersécurité (**ENISA**) dans le cadre de la coopération structurée prévue par le règlement (UE) 2019/881 du Parlement européen et du Conseil[9]. 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. La CERT-UE devrait coopérer avec [...] **l'ENISA** en ce qui concerne l'analyse des menaces et partager régulièrement son rapport sur le panorama des menaces avec l'Agence.

[...]

(22) **Les activités et la manipulation des informations effectuées par la CERT-UE au titre du présent règlement peuvent impliquer le traitement de données à caractère personnel.** 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[10]. **Lorsque des données à caractère personnel sont transmises, en vertu du présent règlement, à des destinataires établis dans l'Union autres que des entités de l'Union, cela devrait se faire conformément à l'article 9 du règlement (UE) 2018/1725.**

---

9 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).

10 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).

(23) Le traitement des informations par la CERT-UE et les [...] **entités** de l'Union devrait être conforme aux règles [...] **applicables en matière de** sécurité de l'information [...].

(23 *bis*) Aux fins du partage d'informations, des marquages visibles sont utilisés pour indiquer que les destinataires des informations doivent appliquer des limitations au partage sur la base, notamment, d'accords de confidentialité ou d'accords informels de non-divulgation tels que le "Traffic Light Protocol" ou d'autres indications claires données par la source. Par "Traffic Light Protocol", il faut entendre un moyen de communiquer des renseignements sur toute limitation applicable à la diffusion plus large des informations. Ce protocole est utilisé par la quasi-totalité des centres de réponse aux incidents de sécurité informatique (CSIRT) et par certains centres d'échange et d'analyse d'informations (ISAC).

(24) **Le présent règlement et les nouvelles tâches attribuées à la CERT-UE n'auront aucune incidence sur les dépenses totales au titre du cadre financier pluriannuel.** Étant donné que les services et les missions du CERT-UE sont dans l'intérêt de l'ensemble des [...] **entités** de l'Union, chaque [...] **entité** 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 [...] **entités** de l'Union. **Toutes les entités de l'Union et leurs administrations devraient veiller à optimiser leurs ressources au niveau actuel et renforcer les gains d'efficacité, notamment en approfondissant la coopération interinstitutionnelle dans le domaine de la cybersécurité. Par conséquent, une approche commune de la mutualisation des dépenses administratives devrait être privilégiée par rapport à des dépenses individualisées des entités de l'Union.**

(25) L'IICB, avec l'aide de la 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. **En outre, la Cour des comptes européenne est invitée à évaluer régulièrement le fonctionnement de la CERT-UE,**

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Chapitre I
DISPOSITIONS GÉNÉRALES

Article premier

Objet

1. Le présent règlement établit **des mesures visant à parvenir à un niveau élevé commun de cybersécurité au sein des entités de l'Union.** […]

2. À cette fin, le présent règlement définit:

c) les obligations incombant […] **à chaque entité** de l'Union en ce qui concerne l'établissement d'un cadre […] de gestion, de gouvernance et de contrôle des risques de cybersécurité;

d) les obligations incombant aux […] **entités** de l'Union en ce qui concerne la gestion des risques de cybersécurité […]**,** la communication **et le partage** d'informations;

e) les règles relatives à l'organisation […]**,** au fonctionnement **et à la gestion** […] **de l'équipe interinstitutionnelle autonome d'intervention en cas d'urgence informatique pour les entités** de l'Union (CERT-UE) et à l'organisation […]**,** au fonctionnement **et à la gestion** du conseil interinstitutionnel de cybersécurité **(IICB);**

f) les règles relatives au suivi de la mise en œuvre du présent règlement.

Article 2

Champ d'application

1. Le présent règlement s'applique à […] l'ensemble des […] **entités** de l'Union […] ainsi qu'à […] **la** CERT-UE et […] **au IICB**.

2. Le présent règlement s'applique sans préjudice de l'autonomie institutionnelle prévue par les traités.

3. À l'exception de l'article 12, paragraphe 7, le présent règlement ne s'applique pas aux réseaux et systèmes d'information traitant des informations classifiées de l'UE (ICUE).

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1) "[…] **entités** de l'Union": les institutions, organes**, bureaux** 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 […] **tel que défini à** 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 […] **telle que définie à** l'article 4, point 2), de la directive [proposition SRI 2];

4) "cybersécurité": la cybersécurité […] **telle que définie à l'article 2, point 1), du règlement (UE) 2019/881**;

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 **capable de prendre des décisions**, en fonction des dispositifs de gouvernance à haut niveau propres à chaque […] **entité** de l'Union;

5 *bis*) "incident évité": un incident évité tel que défini à l'article 4, point 4 *bis*, de la directive [proposition SRI 2];

6) "incident": un incident […] **tel que défini à** l'article 4, point 5), de la directive [proposition SRI 2];

[…]

8) "[…] **incident majeur**": tout incident […] **qui provoque des perturbations dépassant les capacités de réaction d'une entité de l'Union et de la CERT-UE ou qui a une incidence notable sur au moins deux entités de l'Union;** […]

9) "traitement des incidents": le traitement des incidents […] **tel que défini à** l'article 4, point 6), de la directive [proposition SRI 2];

10) "cybermenace": une cybermenace […] **telle que définie à** l'article 2, point 8), du règlement (UE) 2019/881;

[…]

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

[…]

14) "risque […]": […] **un risque au sens de l'article 4, point 7 *ter*), de la directive [proposition SRI 2]**.

[…]

[…]

Article 3 bis

Traitement des données à caractère personnel

1) Le traitement, par la CERT-UE, l'IICB ou les entités de l'Union, de données à caractère personnel au titre du présent règlement est effectué dans le respect du règlement (UE) 2018/1725.

2) La CERT-UE, l'IICB et les entités de l'Union traitent et échangent des données à caractère personnel dans la mesure nécessaire et dans le seul but de remplir leurs obligations respectives au titre du présent règlement.

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

Article 4

Cadre de gestion, de gouvernance et de contrôle des risques

1. Chaque […] **entité** de l'Union établit son propre cadre […] de gestion, de gouvernance et de contrôle des risques de cybersécurité (ci-après le "cadre"), à l'appui de sa mission […]**.** […] **Le cadre est placé** 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 **non classifié** de […] **l'entité de l'Union concernée**, y compris l'environnement informatique sur site, **le réseau de technologie opérationnelle,** 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 **repose sur une approche "tous risques" et sur une évaluation de la maturité conformément à l'article 6 couvrant l'ensemble des risques techniques, opérationnels et organisationnels pertinents susceptibles d'avoir une incidence sur la cybersécurité de l'entité de l'Union concernée** […].

2 *bis*. Le cadre définit des politiques en matière de cybersécurité, y compris des objectifs et des priorités en matière de sécurité des réseaux et des systèmes d'information, ainsi que des politiques et des procédures visant à évaluer l'efficacité des mesures de gestion des risques de cybersécurité mises en œuvre et à définir les rôles et responsabilités des membres du personnel.

2 *ter*. Le cadre est réexaminé régulièrement, et au moins tous les trois ans, à la lumière de l'évolution des risques, des actifs et de la maturité de l'entité de l'Union.

3. Le niveau hiérarchique le plus élevé de chaque […] **entité** de l'Union […] **contrôle le** respect, par son […] **organisation**, 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.

3 *bis*. Le cas échéant et sans préjudice de sa responsabilité dans la mise en œuvre du présent règlement, le niveau hiérarchique le plus élevé de chaque entité de l'Union peut déléguer des obligations spécifiques au titre du présent règlement à d'autres membres de l'encadrement supérieur au sein de l'entité concernée. Indépendamment d'une éventuelle délégation de ses obligations spécifiques, le niveau hiérarchique le plus élevé peut être tenu responsable du non-respect, par l'entité, des obligations prévues par le présent règlement.

3 *ter*. Le niveau hiérarchique le plus élevé de chaque entité de l'Union veille à ce que les entités de l'Union approuvent un plan de cybersécurité comprenant des mesures de gestion des risques de cybersécurité correspondant à leur analyse des risques, de sorte que le cadre soit mis en œuvre conformément au présent règlement.

[…]

5. Chaque […] **entité** 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.

Le responsable local de la cybersécurité facilite la mise en œuvre du présent règlement et rend directement et régulièrement compte au niveau hiérarchique le plus élevé de l'état d'avancement de la mise en œuvre.

Sans préjudice du fait que le responsable local de la cybersécurité soit un point de contact unique dans chaque entité de l'Union, une entité de l'Union peut déléguer certaines tâches du responsable local de la cybersécurité en ce qui concerne la mise en œuvre du présent règlement à la CERT-UE sur la base d'un accord de niveau de service conclu entre cette entité de l'Union et la CERT-UE. L'IICB décide si la fourniture de ce service fait partie des services de base de la CERT-UE, en tenant compte des ressources humaines et financières de l'entité de l'Union concernée. Chaque entité de l'Union informe la CERT-UE, dans les meilleurs délais, de la désignation du responsable local de cybersécurité, ainsi que de tout changement ultérieur. La CERT-UE tient et met régulièrement à jour la liste des responsables locaux de la cybersécurité désignés.

6. Le personnel d'encadrement supérieur au sens de l'article 29, paragraphe 2, du statut[11], ou d'autres fonctionnaires de niveau équivalent, de chaque entité 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'organisation.

11 Règlement nº 259/68 du Conseil, du 29 février 1968, fixant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, JO L 56 du 4.3.1968, p. 1.

7. Chaque entité de l'Union dispose de mécanismes efficaces pour garantir qu'un pourcentage adéquat du budget informatique est consacré à la cybersécurité. Lors de la définition de ce pourcentage, il est dûment tenu compte du cadre.

Article 5

[…] ***Mesures de gestion des risques*** *de cybersécurité*

1. […] **Chaque entité de l'Union veille, sous la supervision du niveau hiérarchique le plus élevé** […] **à ce que des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées soient prises afin de gérer les risques recensés dans le cadre visé à l'article 4, paragraphe 1, et de prévenir et/ou réduire les conséquences des incidents. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de sa taille et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.**

[…]

3. Les entités de l'Union abordent au moins les domaines spécifiques suivants dans le cadre de la mise en œuvre des mesures de gestion des risques de cybersécurité au sein de leurs plans de cybersécurité, conformément aux documents d'orientation et aux recommandations émanant de l'IICB:

a) la politique de cybersécurité, en ce qui concerne la spécification des outils et des mesures nécessaires pour atteindre les objectifs et priorités visés à l'article 4 et à l'article 5, paragraphe 4;

b) l'analyse des risques et les politiques de sécurité des systèmes d'information;

c) l'organisation de la cybersécurité, y compris la définition des rôles et des responsabilités;

d) la gestion des actifs, y compris l'inventaire des actifs informatiques et la cartographie des réseaux informatiques;

e) la sécurité des ressources humaines et le contrôle d'accès;

f) la sécurité des activités;

g) la sécurité des communications;

h) l'acquisition, le développement et la maintenance des systèmes, y compris le traitement et la divulgation des vulnérabilités;

i) la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité de l'Union et ses fournisseurs ou prestataires de services directs. Les entités de l'Union tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé;

j) le traitement des incidents et la coopération avec la CERT-UE, telles que la maintenance du suivi de la sécurité et de la journalisation;

k) la gestion de la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises; et

l) la promotion et le développement de programmes d'éducation, de renforcement des compétences, de sensibilisation, d'exercices et de formation en matière de cybersécurité.

4. Les entités de l'Union abordent au moins les mesures de gestion des risques de cybersécurité spécifiques suivantes dans le cadre de la mise en œuvre des mesures de gestion des risques de cybersécurité au sein de leurs plans de cybersécurité, conformément aux documents d'orientation et aux recommandations émanant de l'IICB:

a) les objectifs et les priorités en ce qui concerne l'utilisation des services d'informatique en nuage au sens de l'article 4, point 19, de la directive [proposition SRI 2] et les modalités techniques permettant le télétravail;

b) des mesures concrètes en vue de l'utilisation future des principes de vérification systématique, y compris un modèle de sécurité, et une stratégie coordonnée de cybersécurité et de gestion des systèmes fondée sur la reconnaissance de l'existence de menaces tant à l'intérieur qu'à l'extérieur des frontières traditionnelles du réseau;

c) l'adoption de l'authentification à facteurs multiples comme norme dans l'ensemble des réseaux et des systèmes d'information;

d) la sécurisation de la chaîne d'approvisionnement des logiciels au moyen de critères pour le développement et l'évaluation sécurisés des logiciels;

e) le renforcement des règles de passation des marchés publics afin de faciliter un niveau élevé commun de cybersécurité par:

i) la suppression des obstacles contractuels qui limitent le partage d'informations sur les incidents, les vulnérabilités et les cybermenaces entre les fournisseurs de services informatiques et la CERT-UE;

ii) l'obligation contractuelle de signaler les incidents, les vulnérabilités et les cybermenaces ainsi que de veiller à ce que des mesures appropriées de réaction et de suivi en cas d'incidents soient en place;

f) l'utilisation de la cryptographie et du chiffrement, et en particulier du chiffrement de bout en bout;

g) des systèmes de communication sécurisés au sein de l'organisation.

Article 6

Évaluations de la maturité

1. Chaque […] **entité** de l'Union**, au besoin avec l'aide d'un tiers spécialisé,** procède, au moins tous les trois ans, à une évaluation de la maturité […] 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.

2. Sur recommandation de la CERT-UE et après consultation de l'Agence de l'Union européenne pour la cybersécurité (ENISA), l'IICB adopte, dans un délai de 4 mois à compter de l'entrée en vigueur du présent règlement, des lignes directrices méthodologiques pour la réalisation des évaluations de maturité.

3. Lorsque […] **l'évaluation de la maturité est terminée, l'entité de l'Union la soumet à l'IICB. La première évaluation de la maturité est effectuée au plus tard le [12 mois après l'entrée en vigueur du présent règlement].**

Article 7

Plans de cybersécurité

1. Compte tenu des conclusions tirées de l'évaluation de la maturité et des actifs et des risques recensés conformément à l'article 4, le niveau hiérarchique le plus élevé de chaque […] **entité** de l'Union approuve un plan de cybersécurité dans les meilleurs délais après l'établissement du cadre […]**, l'adoption des mesures de gestion des risques de** cybersécurité […] **et la réalisation de l'évaluation de la maturité et au plus tard 21 mois après l'entrée en vigueur du présent règlement**. Le plan **de cybersécurité** vise à accroître la cybersécurité globale de l'entité **de l'Union** concernée et contribue ainsi à […] renforcer […] **le** niveau élevé commun de cybersécurité parmi l'ensemble des […] **entités** de l'Union […]. […] **Le** plan **de cybersécurité** comprend au moins les **mesures de gestion des risques de cybersécurité conformément à l'article 5** […]. Le plan **de cybersécurité** est révisé au moins tous les […] **deux** ans **ou** à la suite de […] **chaque évaluation** de la maturité effectuée […] conformément à l'article 6 **ou de chaque réexamen du cadre conformément à l'article 4**.

2. […]

3. Le plan de cybersécurité **prend en compte** […] tous les documents d'orientation et recommandations applicables émis **conformément à l'article 13** […].

4. **Une fois le plan de cybersécurité achevé, l'entité de l'Union le soumet à l'IICB.**

Article 7 bis

Évaluation par les pairs

1. Sur recommandation de la CERT-UE et après consultation de l'ENISA, et en utilisant la méthodologie relative aux évaluations par les pairs et la méthodologie d'autoévaluation conformément à l'article 16 de la directive [proposition SRI 2] adaptées, le cas échéant, aux besoins des entités de l'Union, l'IICB établit, au plus tard le … [24 mois après l'entrée en vigueur du présent règlement] la méthodologie et les aspects organisationnels des évaluations par les pairs en vue de tirer des enseignements des expériences partagées, de renforcer la confiance mutuelle, de parvenir à un niveau élevé commun de cybersécurité, ainsi que de renforcer les capacités et les politiques des entités de l'Union en matière de cybersécurité qui sont nécessaires à la mise en œuvre du présent règlement. La participation aux évaluations par les pairs a lieu sur une base volontaire. Des représentants des États membres peuvent participer à l'évaluation par les pairs en qualité d'observateurs. Les évaluations par les pairs sont menées par des experts en cybersécurité désignés par au moins deux entités de l'Union, différentes des entités de l'Union évaluées, et portent sur au moins l'un des éléments suivants:

i) le niveau de mise en œuvre des mesures de gestion des risques de cybersécurité et des obligations de déclaration visées aux articles 5 et 20;

ii) le niveau des capacités, y compris les ressources financières, techniques et humaines disponibles;

iii) le niveau de mise en œuvre du cadre de partage des informations visé à l'article 19;

iv) des questions spécifiques de nature transsectorielle.

2. Les entités de l'Union peuvent signaler sur quelles questions spécifiques visées au paragraphe 1, point iv), doit porter l'évaluation. La portée de l'évaluation, y compris les questions signalées, est communiquée aux entités de l'Union qui y participent avant le début de l'évaluation par les pairs.

3. Avant le début de l'évaluation par les pairs, les entités de l'Union peuvent procéder à une autoévaluation des aspects évalués et fournir celle-ci aux experts désignés.

4. Les évaluations par les pairs comportent des visites sur place physiques ou virtuelles et des échanges hors site. Conformément au principe de bonne coopération, les entités de l'Union faisant l'objet de l'évaluation par les pairs fournissent aux experts désignés les informations nécessaires à l'évaluation, sans préjudice du droit national ou du droit de l'Union concernant la protection des informations sensibles ou classifiées. Toute information obtenue durant le processus d'évaluation par les pairs n'est utilisée qu'à cet effet. Les experts participant à l'évaluation par les pairs ne divulguent à aucun tiers les informations sensibles ou classifiées obtenues au cours de cette évaluation.

5. Une fois qu'ils ont fait l'objet d'une évaluation par les pairs dans des entités de l'Union, les mêmes aspects ne font pas l'objet d'une nouvelle évaluation par les pairs dans ces entités de l'Union au cours des deux années suivant la conclusion de l'évaluation par les pairs, sauf si les entités de l'Union le demandent ou si une proposition en ce sens de l'IICB est approuvée.

6. Les entités de l'Union veillent à ce que tout risque de conflit d'intérêts concernant les experts désignés soit révélé aux autres entités de l'Union et à l'IICB, avant le début de l'évaluation par les pairs. Les entités de l'Union faisant l'objet de l'évaluation par les pairs peuvent s'opposer à la désignation de certains experts pour des raisons dûment justifiées communiquées aux entités de l'Union qui les ont désignés.

7. **Les experts participant aux évaluations par les pairs rédigent des rapports sur les résultats et les conclusions des évaluations. Les entités de l'Union sont autorisées à formuler des observations sur leurs projets de rapport respectifs, qui sont joints aux rapports. Les rapports contiennent des recommandations permettant d'améliorer les aspects sur lesquels l'évaluation par les pairs a porté. Les rapports sont présentés à l'IICB et au réseau des CSIRT, le cas échéant. Les entités de l'Union qui ont fait l'objet d'une évaluation par les pairs peuvent décider de rendre public le rapport les concernant ou une version expurgée de celui-ci.**

Article 8

Mise en œuvre

1. […]

2. Les documents d'orientation et les recommandations établis conformément à l'article 13 soutiennent la mise en œuvre des dispositions du présent chapitre.

3. **À la demande de l'IICB, les entités de l'Union font rapport sur des aspects spécifiques 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 **entités** [...] **de l'Union**;

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

3. L'IICB est composé**:**

   a) d'un représentant désigné par chacune des entités suivantes:

      i) le Parlement européen;

      ii) le Conseil européen;

      iii) le Conseil de l'Union européenne;

      iv) la Commission européenne;

      v) la Cour de justice de l'Union européenne;

      vi) la Banque centrale européenne;

vii) la Cour des comptes européenne;

viii) le service européen pour l'action extérieure;

ix) le Comité économique et social européen;

x) le Comité européen des régions;

xi) la Banque européenne d'investissement;

xii) le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité; et

xiii) l'Agence de l'Union européenne pour la cybersécurité;

b) trois représentants [...] **désignés** 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.
[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3 bis. Chaque membre peut être assisté d'un suppléant. D'autres représentants des **entités** [...] susmentionnées ou d'autres **entités** [...] 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 [...] **deux** ans. Son suppléant devient membre à part entière de l'IICB pour la même durée.

6. L'IICB se réunit **au moins trois fois par an** à l'initiative de son président **et/ou** à la demande de la CERT-UE **et/**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 de la CERT-UE**, le président du groupe de coopération SRI**, **le président du réseau EU-CyCLONe et le président du réseau des CSIRT,** ou **leurs** [...] suppléant**s** [...] **peuvent** participe**r** aux réunions de l'IICB **comme observateurs**, sauf décision contraire de l'IICB.

10. Le secrétariat de l'IICB est assuré par **l'ENISA** [...] **et rend compte au président de l'IICB**.

11. Les représentants nommés par l'EUAN sur proposition du comité consultatif sur les TIC transmettent les décisions de l'IICB aux **membres de l'EUAN** [...]. 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. [...]

13. L'IICB peut **instituer** [...] un comité exécutif pour l'assister dans ses travaux et lui déléguer certains de ses pouvoirs et tâches**, en particulier ceux visés à l'article 10, points c) et e)**. L'IICB établit le règlement intérieur du comité exécutif, y compris ses tâches et pouvoirs, ainsi que le mandat de ses membres.

14. L'IICB présente au Conseil, tous les 12 mois, un rapport détaillant les progrès réalisés dans la mise en œuvre du présent règlement et précisant notamment l'étendue de la coopération de la CERT-UE avec ses homologues nationaux dans chacun des États membres. Ce rapport constitue une contribution au rapport bisannuel sur l'état de la cybersécurité dans l'Union au cours de la même période, conformément à l'article 15 de la directive [proposition SRI 2].

Article 10

Tâches de l'IICB

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

(a) [...] **suivre et superviser efficacement l'application** du présent règlement [...] **et aider les** [...] **entités** de l'Union **à renforcer leur cybersécurité**; **à cette fin, l'IICB peut demander des rapports ad hoc à la CERT-UE et aux entités de l'Union;**

a *bis*) à la suite de discussions stratégiques, adopter une stratégie pluriannuelle visant à relever le niveau de cybersécurité dans les entités de l'Union et l'évaluer régulièrement et au moins tous les cinq ans et, le cas échéant, la modifier;

b) approuver, sur la base d'une proposition **présentée par le** [...] chef de la CERT-UE, le programme de travail annuel de la CERT-UE et en suivre la mise en œuvre;

c) approuver, sur la base d'une proposition du chef de la CERT-UE, le catalogue de services de la CERT-UE **et toute mise à jour ultérieure de celui-ci**;

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

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

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

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

h) approuver les accords de coopération et les **accords** [...] ou contrats de niveau de service conclus entre la CERT-UE et d'autres entités conformément à l'article 17;

i) créer **des** [...] groupes consultatifs techniques [...] afin d'assister l'IICB dans ses travaux, approuver leur mandat et désigner leurs présidents respectifs;

j) **adopter des documents d'orientation ou des recommandations sur proposition de la CERT-UE conformément à l'article 13 et donner instruction à la CERT-UE d'élaborer, de retirer ou de modifier une proposition de documents d'orientation ou de recommandations, ou un appel à l'action;**

k) recevoir et évaluer les documents et rapports présentés par les entités de l'Union au titre du présent règlement;

l) soutenir la mise en place d'un groupe informel réunissant les responsables locaux de la cybersécurité de toutes les entités et faciliter ainsi l'échange de bonnes pratiques et d'informations relatives à la mise en œuvre du présent règlement;

m) élaborer un plan de gestion des cybercrises afin de soutenir la gestion coordonnée des incidents majeurs au niveau opérationnel affectant des entités de l'Union et de contribuer à l'échange régulier d'informations pertinentes, notamment en ce qui concerne les incidences et la gravité des incidents majeurs et les moyens d'atténuation possibles.

Article 11

Contrôle du respect

1. L'IICB suit **efficacement, conformément à l'article 9, paragraphe 2 et à l'article 10,** la mise en œuvre du présent règlement et des documents d'orientation, recommandations et appels à l'action adoptés par les [...] **entités** de l'Union. **À cette fin, l'IICB peut demander les informations ou les documents nécessaires pour évaluer la bonne application des dispositions du règlement par les entités de l'Union. Aux fins de l'adoption de mesures de contrôle du respect au titre du présent article, l'entité de l'Union concernée ne dispose pas du droit de vote.**

2. Lorsque l'IICB constate que **des entités** [...] 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'**entité** [...] de l'Union concernée**, et après avoir donné à l'entité ou à la personne concernée la possibilité de présenter son point de vue**:

a) émettre un avertissement **pour remédier aux lacunes constatées dans un délai déterminé, y compris des recommandations visant à modifier les documents relatifs à la cybersécurité adoptés par les entités de l'Union sur la base du présent règlement**; lorsque cela s'avère nécessaire en raison d'un risque de cybersécurité impérieux, les destinataires de l'avertissement sont limités de manière appropriée;

a *bis*) transmettre une notification motivée à une entité de l'Union, au cas où il n'a pas été suffisamment remédié, dans un délai déterminé, aux lacunes constatées dans l'avertissement précédemment émis, et notifier formellement cet avis au Conseil, au Parlement européen et à la Commission;

b) **émettre, en particulier:** [...]

i. une recommandation de procéder à un audit d'une entité de l'Union;

ii. une demande visant à ce qu'un audit soit effectué par un service d'audit tiers.

c) demander à l'entité de l'Union de mettre la gestion, la gouvernance et le contrôle des risques en matière de cybersécurité en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé.

d) émettre un avis à l'intention de tous les États membres et toutes les entités de l'Union recommandant la suspension temporaire des flux de données vers l'entité de l'Union.

3. Lorsque l'IICB a adopté des mesures en vertu du paragraphe 2, points a) à d), l'entité de l'Union concernée fournit un compte rendu détaillé des mesures prises et des actions menées pour remédier aux lacunes alléguées constatées par l'IICB. L'entité de l'Union présente ce compte rendu dans un délai raisonnable à convenir avec l'IICB.

4. Lorsque l'IICB estime qu'il y a une violation persistante des dispositions du présent règlement par une entité de l'Union directement imputable aux actions ou omissions d'un fonctionnaire ou d'un autre agent de l'Union, y compris au niveau hiérarchique le plus élevé, l'IICB demande à l'entité concernée de prendre les mesures appropriées, y compris de nature disciplinaire, conformément, notamment, aux règles énoncées dans le statut des fonctionnaires et le régime applicable aux autres agents de l'Union européenne. À cette fin, l'IICB transfère les informations nécessaires à l'entité concernée.

Chapitre IV
CERT-UE

Article 12

Missions et tâches de la CERT-UE

1. [...] **La mission de la CERT-UE** est de contribuer à la sécurité de l'environnement informatique non classifié de l'ensemble des [...] **entités** 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.

1 *bis*. La CERT-UE recueille, gère, analyse et partage avec les entités de l'Union des informations sur les menaces, les vulnérabilités et les incidents relatifs aux infrastructures TIC non classifiées. Elle coordonne les réponses aux incidents au niveau interinstitutionnel et au niveau des entités de l'Union, y compris en assurant ou en coordonnant la fourniture d'une assistance opérationnelle spécialisée.

2. La CERT-UE accomplit les tâches suivantes pour les [...] **entités** 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 **dispositions** [...] énoncées à l'article 13, paragraphe 1, ou des rapports ad hoc demandés par l'IICB;

b) [...] **offrir des services CSIRT standard à toutes les entités de l'Union** 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) **sur la base des informations visées au paragraphe 1 *bis*,** [...] contribuer à la conscience situationnelle de la cybersécurité de l'UE **en étroite coopération avec l'ENISA**. **Ces informations sont partagées avec l'IICB, ainsi qu'avec le réseau des CSIRT et l'INTCEN;**

f) jouer un rôle équivalent à celui de coordinateur désigné pour les entités de l'Union, tel que visé à l'article 6 de la directive [proposition SRI 2].

[...]

[...]

[...]

[...]

[...]

4. **Dans le cadre de ses compétences, l**a CERT-UE mène une coopération structurée avec [....] **l'ENISA** 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. La 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 [...] **entités** 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 [...] **entités** 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 [...] **entités** de l'Union qui coopèrent étroitement avec les [...] **entités** 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. La CERT-UE peut organiser **ou participer à** des exercices de cybersécurité ou recommander la participation à des exercices existants, le cas échéant en étroite coopération avec [...] **l'ENISA**, afin de tester le niveau de cybersécurité des [...] **entités** de l'Union.

7. La CERT-UE peut fournir une assistance aux [...] **entités** de l'Union en ce qui concerne les incidents survenant dans des environnements informatiques classifiés s'il y est explicitement invité par [...] **les entités de l'Union** concernée**s, conformément à leurs procédures respectives**. **Dans ce cas, les dispositions des articles 19 à 21 du présent règlement ne s'appliquent pas. La fourniture d'une assistance par la CERT-UE en vertu du présent paragraphe est sans préjudice des règles applicables des États membres ou de l'Union en ce qui concerne la protection des informations sensibles ou classifiées.**

8. La CERT-UE informe les entités de l'Union de ses procédures et processus de gestion des incidents.

9. La CERT-UE peut surveiller le trafic sur les réseaux des entités de l'Union avec le consentement de l'entité de l'Union concernée.

10. La CERT-UE peut, si les services politiques des entités de l'Union en font expressément la demande, fournir des conseils ou des contributions techniques sur des questions politiques pertinentes.

11. La CERT-UE, en coopération avec le Contrôleur européen de la protection des données, apporte son soutien aux entités de l'Union concernées lorsqu'elles traitent des incidents donnant lieu à des violations de données à caractère personnel.

Article 13

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

1. La 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 [...] **entités** de l'Union sont instamment invité**e**s à prendre dans un délai déterminé. Dans les meilleurs délais après avoir reçu l'appel à l'action, l'entité de l'Union concernée informe la CERT-UE de la manière dont ces mesures ont été appliquées;

   b) des propositions soumises à l'IICB concernant des documents d'orientation destinés à l'ensemble ou à une partie des [...] **entités** de l'Union;

   c) des propositions soumises à l'IICB concernant des recommandations destinées à titre individuel aux [...] **entités** de l'Union.

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

   a) les modalités de la gestion des risques de cybersécurité [...] ou les améliorations à y apporter **et les mesures de gestion des risques en matière de** cybersécurité [...];

   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**, y compris une approche coordonnée de la sécurité de la chaîne d'approvisionnement**.

[...]

[...]

Article 14

Chef de la CERT-UE

1. La Commission, après avoir obtenu l'approbation des deux tiers des membres de l'IICB, désigne le chef de la CERT-UE. L'IICB est consulté à tous les stades de la procédure menant à la désignation du chef de la 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. Le chef de la CERT-UE est responsable du bon fonctionnement de celle-ci et agit dans le cadre de ses attributions, sous la direction de l'IICB. Il ou elle est responsable de la mise en œuvre de la direction stratégique, des orientations, des objectifs et des priorités définis par l'IICB, ainsi que de la gestion de la CERT- UE, y compris de ses ressources financières et humaines. Il ou elle rend compte régulièrement au président de l'IICB.

3. Le chef de la CERT-UE aide l'ordonnateur délégué compétent à élaborer le rapport annuel d'activités contenant des informations financières et de gestion, y compris les résultats des contrôles, établi conformément à l'article 74, paragraphe 9, du règlement financier, et lui rend régulièrement compte de la mise en œuvre des mesures pour lesquelles des pouvoirs lui ont été sous- délégués.

4. Le chef de la CERT-UE établit chaque année une planification financière des recettes et dépenses administratives pour ses activités, la proposition de programme de travail annuel, la proposition de catalogue de services de la CERT-UE et sa révision, la proposition de modalités des accords de niveau de service et la proposition d'indicateurs clés de performance relatifs à la CERT-UE en vue de leur approbation par l'IICB conformément à l'article 10.

Lors de la révision de la liste des services figurant dans le catalogue de services de la CERT-UE, le chef de la CERT-UE tient compte des ressources allouées à la CERT-UE.

5. Le chef de la CERT-UE présente [...] des rapports [...] **annuels** à l'IICB [...] sur les résultats obtenus par la 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, [...] **point a)**.

Article 15

Questions financières et de personnel

[...]

1 *bis*. Tout en étant établie comme un fournisseur interinstitutionnel autonome de services destinés à l'ensemble des entités de l'Union, la CERT-UE est intégrée à la structure administrative d'une direction générale de la Commission, afin de bénéficier des structures d'appui de la Commission en matière administrative, financière, de gestion et de comptabilité. La Commission informe l'IICB du siège administratif de la CERT- UE et de toute modification de celui-ci. Cette approche est évaluée régulièrement, au plus tard avant la fin de tout cadre financier pluriannuel établi conformément à l'article 312 du traité sur le fonctionnement de l'Union européenne, pour permettre l'adoption de mesures adéquates.

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

3. Les tâches et activités de la CERT-UE, y compris les services qu'elle fournit, conformément à l'article 12, paragraphes 2, [...] 4 et 6, et à l'article 13, paragraphe 1, aux [...] **entités** 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 à la CERT-UE sont détaillés dans une note de bas de page du tableau des effectifs de la Commission. Les postes réservés à la CERT-UE sont détaillés dans une note de bas de page du tableau des effectifs de la Commission.

4. Les [....] **entités** de l'Union autres que [...] **celles visées** au paragraphe 3 versent une contribution financière annuelle à la CERT-UE pour couvrir les services fournis par la 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 la 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[12].

5. Les coûts des tâches définies à l'article 12, paragraphe 5, sont recouvrés auprès des [...] **entités** de l'Union qui bénéficient des services de la CERT-UE. Les recettes sont affectées aux lignes budgétaires dont relèvent les coûts.

---

12 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) n° 1296/2013, (UE) n° 1301/2013, (UE) n° 1303/2013, (UE) n° 1304/2013, (UE) n° 1309/2013, (UE) n° 1316/2013, (UE) n° 223/2014, (UE) n° 283/2014 et la décision n° 541/2014/UE, et abrogeant le règlement (UE, Euratom) n° 966/2012 (JO L 193 du 30.7.2018, p. 1).

Article 16

Coopération de la CERT-UE avec les homologues des États membres

1. La CERT-UE coopère et échange**, dans les meilleurs délais,** des informations avec les homologues nationaux dans les États membres, **notamment** [...] les CSIRT **visés à l'article 9 de la directive [proposition SRI 2] et/ou, le cas échéant, les autorités nationales compétentes** 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 [...] **entités** de l'Union, y compris par l'intermédiaire du réseau des CSIRT visé à l'article 13 de la directive [proposition SRI 2].

1 *bis*. La CERT-UE avertit sans délai tout homologue national concerné visé au paragraphe 1 dans un État membre, lorsqu'elle prend connaissance d'incidents importants survenant sur le territoire de cet État membre, à moins que la CERT-UE ne dispose de l'information selon laquelle l'entité de l'Union touchée a déjà signalé l'incident conformément à l'article 20, paragraphe 2 bis.

2. La CERT-UE [...] **échange** [...]**, dans les meilleurs délais,** 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 **ou de contribuer à l'analyse d'un incident** sans **avoir besoin du** consentement de [...] **l'entité de l'Union** touchée. La CERT-UE [...] **n'échange pas d'**informations propres à un incident qui révèlent l'identité de la cible de l'incident de cybersécurité [...] **à moins:**

   a) que l'entité de l'Union touchée ait donné son consentement;

   b) que l'entité de l'Union touchée ait déjà révélé qu'elle l'était;

c) que l'entité de l'Union touchée n'ait pas donné son consentement, mais que la publication de son identité augmente la probabilité d'éviter ou d'atténuer d'autres incidents survenant par ailleurs. Ce genre de décisions nécessite l'approbation du chef de la CERT-UE. L'entité de l'Union touchée est informée avant la publication.

Article 17

Coopération de la CERT-UE avec* [....] *d'autres homologues

1. La CERT-UE peut coopérer avec les homologues [...] **dans l'Union européenne autres que ceux mentionnés à l'article 16**, 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, [...] la CERT-UE sollicite au préalable l'approbation de l'IICB **au cas par cas**. **La CERT-UE informe tous les homologues nationaux concernés visées à l'article 16, paragraphe 1 dans un État membre dans lequel l'homologue est situé, lorsque la CERT-UE met en place une coopération avec de tels homologues.**

2. La CERT-UE peut coopérer avec d'autres partenaires, tels que des entités commerciales, des organisations internationales, des entités nationales ou des experts 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, la CERT-UE sollicite au préalable l'approbation de l'IICB **au cas par cas**.

3. La CERT-UE peut**, sous réserve qu'un accord ou un contrat de non-divulgation ait été conclu avec le partenaire concerné et** avec le consentement de [...] **l'entité de l'Union** touchée par un incident, fournir des informations relatives à l'incident **spécifique** aux partenaires [...] **visés aux paragraphes 1 et 2 dans le seul but** de contribuer à son analyse. **La légalité de ces accords ou contrats de non- divulgation fait l'objet d'un contrôle selon les procédures internes applicables de la Commission. Les accords ou contrats de non- divulgation ne nécessitent pas l'approbation préalable de l'IICB, mais le président de celui-ci en est informé.**

4. **La CERT-UE peut exceptionnellement conclure des accords de niveau de service avec des entités autres que les entités de l'Union, avec l'approbation préalable de l'IICB.**

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

Article 18

Traitement des informations

1. La CERT-UE et les [...] **entités** 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[13] s'appliquent aux demandes d'accès du public aux documents détenus par la CERT-UE, y compris l'obligation, prévue par ledit règlement, de consulter les autres [...] **entités** de l'Union**, et le cas échéant les États membres,** dès lors qu'une demande concerne leurs documents.

[...]

4. Le traitement des informations par la CERT-UE et les [...] **entités** de l'Union est conforme aux règles [...] **applicables en matière de** sécurité de l'information[...].

[...]

Article 19

[...] ***Partage d'informations en matière de cybersécurité***

-1. Les entités de l'Union peuvent volontairement transmettre à la CERT-UE des informations relatives aux cybermenaces, aux incidents, aux incidents évités et aux vulnérabilités qui les touchent. La CERT-UE veille à ce que des moyens de communication efficaces soient disponibles pour faciliter le partage d'informations avec les entités de l'Union. La CERT-UE peut traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires.

[13] 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).

1. Afin [...] **d'accomplir sa mission et ses tâches définies à l'article 12**, la CERT-UE peut demander aux [...] **entités** de l'Union de lui fournir **des informations** à partir de leurs inventaires respectifs des systèmes informatiques, **y compris des informations relatives aux cybermenaces, aux incidents évités, aux indicateurs de compromission, des alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberincidents** [...]. L'**entité** [...] requis**e** transmet les informations demandées, ainsi que toute mise à jour ultérieure de celles-ci, dans les meilleurs délais.

2. Les [...] **entités** de l'Union fournissent à la 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 respectivement touchés. La CERT-UE peut préciser davantage les types d'informations numériques dont elle a besoin pour la conscience situationnelle et la réaction aux incidents.

3. La CERT-UE ne peut échanger **avec les entités de l'Union** des informations propres à un incident qui révèlent l'identité de [...] **l'entité** de l'Union touché**e** par cet incident qu'avec le consentement de cette entité. **Lorsque ce consentement n'est pas accordé, l'entité concernée en communique les motifs dûment justifiés à la CERT-EU.** [...]

4. Les obligations en matière de partage ne s'étendent pas aux informations classifiées de l'Union européenne (ICUE) ni aux informations **dont la distribution au-delà de l'entité de l'Union destinataire a été exclue par la source de l'information au moyen d'un marquage visible, sauf si la source de l'information autorise explicitement le partage de ladite information avec la CERT-UE.** [...]

Article 20

Obligations en matière de [...] ***communication d'informations***

-1. Un incident est considéré comme "important" si:

a) il a causé ou est susceptible de causer une perturbation opérationnelle grave au fonctionnement de l'entité de l'Union ou des pertes financières pour l'entité de l'Union concernée;

b) il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels ou non matériels considérables.

1. L'ensemble des [...] **entités** de l'Union transmettent [...] au CERT-EU [...]**:** [...]

[...].

a) sans retard injustifié et en tout cas dans les 24 heures après avoir eu connaissance de l'incident important, une alerte précoce, qui, le cas échéant, indique si l'incident important semble causé par des actes illicites ou malveillants et s'il a ou pourrait avoir une incidence transfrontière;

b) sans retard injustifié et en tout cas dans les 72 heures après avoir eu connaissance de l'incident important, une notification d'incident qui, le cas échéant, met à jour les informations visées au point a) et fournit une évaluation initiale de l'incident important, de sa gravité et de son incidence, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles;

c) à la demande de la CERT-UE, un rapport intermédiaire sur les mises à jour pertinentes de la situation;

d) un rapport final au plus tard un mois après la présentation de la notification d'incident important visée au point b), comprenant au moins les éléments suivants:

i) une description détaillée de l'incident important, de sa gravité et de son incidence;

ii) le type de menace ou la cause profonde qui a probablement déclenché l'incident important;

iii) les mesures d'atténuation appliquées et en cours.

iv) le cas échéant, l'incidence transfrontière de l'incident important;

e) en cas d'incident important en cours au moment de la présentation du rapport final visé au point d), un rapport d'avancement à ce moment-là puis un rapport final dans un délai d'un mois après que l'incident a été traité.

[...]

g) [...]

h) [...]

i) [...]

j) [...]

2 *bis*. Toute entité de l'Union partage les informations déclarées conformément au paragraphe 1 dans le même délai avec tous les homologues nationaux concernés visés à l'article 16, paragraphe 1, où elle se situe.

3. La CERT-UE soumet [...] **tous les trois mois à l'IICB, au Centre de situation et de renseignement de l'UE (INTCEN) et au réseau des CSIRT** un rapport de synthèse contenant des données anonymisées et agrégées sur les cybermenaces [...], les vulnérabilités [...] **conformément à l'article 19, les réponses des entités de l'Union aux appels à l'action conformément à l'article 13, paragraphe 1, point a),** et les incidents importants qui ont été notifiés conformément au paragraphe 1. **Ce rapport constitue une contribution au rapport bisannuel sur l'état de la cybersécurité dans l'Union au titre de l'article 15 de la directive [proposition SRI 2].**

4. L'IICB**, pour le [6 mois après la date d'entrée en vigueur du présent règlement] au plus tard,** [...] élabore[...] des documents d'orientation ou des recommandations [...] **précisant davantage** les modalités**, le format** et le contenu **du rapport** [...]. **Les documents d'orientation ou recommandations tiennent dûment compte des dispositions mises en œuvre par tout acte d'exécution conformément à l'article 20, paragraphe 11, de la directive [proposition SRI 2].** La CERT-UE diffuse les renseignements techniques appropriés pour permettre aux [...] **entités** 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 [...] **communication d'informations** ne s'étendent pas aux ICUE ni aux informations **dont la distribution au-delà de l'entité de l'Union destinataire a été exclue par la source de l'information au moyen d'un marquage visible, à moins que la source de l'information [...] ne permette explicitement que ladite information soit partagée avec la CERT-UE.** [...]

Article 21

Coordination des réponses aux incidents et coopération [...]

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

   a) les [...] **entités** de l'Union;

   b) les homologues visés aux articles 16 et 17.

2. La CERT-UE**,** [...] **le cas échéant en étroite coopération avec l'ENISA conformément à l'article 7, paragraphe 7, point d), du règlement sur la cybersécurité[14],** facilite la coordination entre les [...] **entités** de l'Union en matière de réaction aux incidents, notamment par les moyens suivants:

   a) contribution à une communication externe cohérente;

   [...]

   c) utilisation optimale des ressources opérationnelles;

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

3. La CERT-UE**, en étroite coopération avec l'ENISA,** soutient les [...] **entités** de l'Union en ce qui concerne la conscience situationnelle des cybermenaces, des vulnérabilités et des incidents.

---

14 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 des technologies de l'information et des communications en matière de cybersécurité et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité).

4. L'IICB**, le [12 mois après la date d'entrée en vigueur du présent règlement] au plus tard, sur la base d'une proposition du CERT-EU, adopte** [...] des **documents** d'orientation[...] **ou recommandations** 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, la CERT-UE conseille sur la manière de signaler l'incident aux autorités répressives.

Article 22

Gestion des incidents [...] majeurs

-1. Afin de soutenir la gestion coordonnée des incidents majeurs au niveau opérationnel affectant des entités de l'Union et de contribuer à l'échange régulier d'informations pertinentes entre les entités de l'Union et avec les États membres, l'IICB élabore un plan de gestion des cybercrises sur la base des activités détaillées à l'article 21, paragraphe 2, en étroite coopération avec la CERT-UE et l'ENISA, et qui comprend au moins les éléments suivants:

a) les modalités de coordination et de flux d'informations entre les entités de l'Union pour la gestion des incidents majeurs au niveau opérationnel;

b) les instructions permanentes communes;

c) une taxinomie commune de la gravité des incidents majeurs et des points déclencheurs de crise;

d) des exercices réguliers;

e) les canaux de communication sécurisés à utiliser;

f) un point de contact pour le réseau CyCLONe, qui partage les informations pertinentes avec le réseau CyCLONe pour contribuer à l'appréciation commune de la situation.

1. La CERT-UE coordonne les réactions aux [...] **incidents** majeurs[...] entre les [...] **entités** de l'Union. Elle tient à jour un inventaire de l'expertise technique qui serait nécessaire pour réagir aux incidents en cas d'**incidents majeurs** [...].

2. Les [...] **entités** 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. À la demande expresse d'un État membre dans lequel se situe l'entité de l'Union affectée et avec [...] l'accord de[...] **l'entité** de l'Union [...] **affectée**, la CERT-UE peut aussi faire appel à des experts figurant sur la liste visée au paragraphe 2 pour contribuer à la réaction à [...] **un incident** majeur[...] dans [...] **ladite entité de l'Union**.

Chapitre VI
DISPOSITIONS FINALES

Article 23

Réaffectation budgétaire initiale

La Commission propose la réaffectation du personnel et des ressources financières provenant des [...] **entités** de l'Union concernées 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 de la 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 **réexaminer le** [...] présent règlement.

2. La Commission fait rapport au Parlement européen et au Conseil sur la mise en œuvre du présent règlement au plus tard **36** [...] 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 **tard** [...] cinq ans après la date d'entrée en vigueur du présent règlement. **Le rapport est accompagné au besoin d'une proposition législative.**

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*
Le président	*Le président*

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

ANNEXE II

[...]

[...]

[...]

[...]

[...]

[...]

[...]