Journal officiel
de l'Union européenne

FR
Série L

2023/2841

18.12.2023

RÈGLEMENT (UE/Euratom) 2023/2841 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 décembre 2023

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

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 ([1]),

considérant ce qui suit:

(1) À l'ère numérique, les technologies de l'information et de la communication constituent l'un des piliers d'une administration européenne 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 les entités de l'Union plus vulnérables aux cybermenaces et aux incidents, ce qui met en péril la continuité de leurs activités et leur capacité à sécuriser leurs données. Alors que le recours accru aux services en nuage, l'utilisation généralisée des technologies de l'information et de la communication (TIC), le degré élevé de numérisation, le télétravail et l'évolution des technologies et de la connectivité sont des caractéristiques essentielles de toutes les activités des entités de l'Union, la résilience numérique n'est pas encore suffisamment intégrée.

(2) Le panorama des cybermenaces auxquelles sont confrontées 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. Les acteurs de la menace mènent leurs cyberattaques à un rythme croissant, tandis que leurs campagnes sont de plus en plus sophistiquées et automatisées, ciblent des surfaces d'attaque exposées qui ne cessent de s'étendre et exploitent rapidement les vulnérabilités.

(3) Les environnements TIC 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 seule 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 d'autres entités de l'Union. En outre, certains environnements TIC des entités de l'Union sont connectés aux environnements TIC des États membres, de sorte qu'un incident dans une entité de l'Union présente un risque de cybersécurité pour les environnements TIC des États membres et inversement. Le partage d'informations concernant des incidents spécifiques peut 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 des entités de l'Union, qu'elles atteignent un niveau élevé commun de cybersécurité grâce à la mise en œuvre de mesures de cybersécurité proportionnées aux risques de cybersécurité, à l'échange d'informations et à la collaboration.

([1]) Position du Parlement européen du 21 novembre 2023 (non encore parue au Journal officiel) et décision du Conseil du 8 décembre 2023.

(5) La directive (UE) 2022/2555 du Parlement européen et du Conseil ([2]) vise à améliorer encore la cyberrésilience et les capacités de réaction en cas d'incident des entités publiques et privées, des autorités et organismes compétents ainsi que de l'Union dans son ensemble. Il est donc nécessaire de veiller à ce que les entités de l'Union suivent cet exemple, en formulant des règles qui soient compatibles avec la directive (UE) 2022/2555 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 (ci-après dénommé «cadre») qui garantisse une gestion efficace et prudente de tous les risques de cybersécurité et tienne compte de la continuité des activités et de la gestion des crises. Le cadre devrait établir des politiques en matière de cybersécurité, notamment en définissant des objectifs et des priorités, aux fins de la sécurité des réseaux et des systèmes d'information englobant la totalité de l'environnement TIC non classifié. 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, les pannes d'électricité ou de télécommunications, l'accès physique non autorisé aux installations d'information et de traitement des informations de l'entité de l'Union, 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.

(7) Pour gérer les risques de cybersécurité identifiés dans le cadre, chaque entité de l'Union devrait prendre des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées. Ces mesures devraient porter sur les domaines et les mesures de gestion des risques de cybersécurité visés dans le présent règlement, afin de renforcer la cybersécurité de chaque entité de l'Union.

(8) Les actifs et les risques de cybersécurité identifiés dans le cadre ainsi que les conclusions tirées des évaluations régulières de la maturité en matière de cybersécurité devraient être reflétés dans le plan de cybersécurité établi par chaque entité de l'Union. Le plan de cybersécurité devrait inclure les mesures de gestion des risques de cybersécurité qui ont été adoptées.

(9) Étant donné qu'assurer la cybersécurité est un processus continu, il conviendrait de réexaminer régulièrement l'adéquation et l'efficacité des mesures prises au titre du présent règlement, à la lumière de l'évolution des risques de cybersécurité, des actifs et de la maturité en matière de cybersécurité des entités de l'Union. Le cadre devrait être révisé à intervalles réguliers et au moins tous les quatre ans, tandis que le plan de cybersécurité devrait être révisé tous les deux ans ou plus fréquemment, le cas échéant, à la suite des évaluations de la maturité en matière de cybersécurité ou de toute révision substantielle du cadre.

(10) Les mesures de gestion des risques de cybersécurité prises par les entités de l'Union devraient inclure des politiques visant, lorsque c'est possible, à rendre le code source transparent, tout en tenant compte des garanties qui protègent les droits des tiers et des entités de l'Union. Ces politiques devraient être proportionnées aux risques de cybersécurité et chercher à faciliter l'analyse des cybermenaces, sans créer d'obligation de divulguer le code d'un tiers ni de droit d'accès à ce même code qui aille outre les conditions contractuelles applicables.

(11) Les outils et applications de cybersécurité dont le code source est ouvert peuvent contribuer à augmenter le degré d'ouverture. Les normes ouvertes facilitent l'interopérabilité entre les outils de sécurité, ce qui profite à la sécurité des acteurs. Les outils et applications de cybersécurité en sources ouvertes peuvent mobiliser la communauté des développeurs au sens large, ce qui permet de diversifier les fournisseurs. Les sources ouvertes peuvent conduire à un processus de vérification plus transparent des outils liés à la cybersécurité et à un processus de détection des vulnérabilités mené par la communauté. Les entités de l'Union devraient donc être en mesure de promouvoir l'utilisation de logiciels libres et de normes ouvertes, en appliquant des politiques relatives à l'utilisation de données ouvertes et de codes sources ouverts dans le cadre de la sécurité par la transparence.

([2]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

(12) En raison des différences entre les entités de l'Union, il y a lieu de faire preuve de souplesse dans la mise en œuvre du présent règlement. Les mesures en faveur d'un niveau élevé commun de cybersécurité prévu dans le présent règlement 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 établissent leurs propres cadres et adoptent leurs propres mesures de gestion des risques de cybersécurité et plans 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 de la coopération entre les entités de l'Union et entre les entités de l'Union et les homologues des États membres.

(13) En vue d'une utilisation optimale des ressources, le présent règlement devrait prévoir la possibilité que deux ou plusieurs entités de l'Union dotées de structures similaires coopèrent pour réaliser les évaluations de la maturité en matière de cybersécurité de leurs entités respectives.

(14) Pour éviter d'imposer une charge financière et administrative excessive aux entités de l'Union, il convient que les exigences en matière de gestion des risques de cybersécurité soient proportionnées aux risques de cybersécurité pesant sur le réseau et les systèmes d'information concernés, compte tenu de l'état 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 TIC à l'amélioration de son niveau de cybersécurité. À plus long terme, un objectif indicatif de l'ordre de 10 % au minimum devrait être poursuivi. L'évaluation de la maturité en matière de cybersécurité devrait déterminer si les dépenses de cybersécurité de l'entité de l'Union sont proportionnées aux risques de cybersécurité auxquels elle est confrontée. Sans préjudice des règles des traités relatives au budget annuel de l'Union, la Commission devrait tenir compte, lorsqu'elle présente sa proposition de premier budget annuel à la suite de l'entrée en vigueur du présent règlement, des obligations découlant du présent règlement lorsqu'elle évalue les besoins en matière de budget et de personnel des entités de l'Union tels qu'ils ressortent de leurs estimations de dépenses.

(15) 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. La responsabilité de l'application du présent règlement, y compris la mise en place du cadre et des mesures de gestion des risques de cybersécurité ainsi que l'approbation du plan de cybersécurité, devrait incomber au plus haut niveau hiérarchique de l'entité de l'Union. La prise en compte de la culture de la cybersécurité, c'est-à-dire la pratique quotidienne de la cybersécurité, fait partie intégrante du cadre et des mesures correspondantes de gestion des risques de cybersécurité dans l'ensemble des entités de l'Union.

(16) La sécurité des réseaux et des systèmes d'information traitant des informations classifiées de l'UE (ICUE) est essentielle. Les entités de l'Union traitant des ICUE doivent appliquer les cadres réglementaires exhaustifs en vigueur pour protéger ces informations, en suivant notamment une gouvernance spécifique, des stratégies spécifiques et des procédures spécifiques de gestion des risques. Les réseaux et les systèmes d'information traitant des ICUE doivent respecter des normes de sécurité plus contraignantes que les réseaux et les systèmes d'information non classifiés. Par conséquent, les réseaux et les systèmes d'information traitant des ICUE sont plus résilients face aux cybermenaces et aux incidents. Ainsi, le présent règlement ne devrait pas s'appliquer aux réseaux et aux systèmes d'information traitant des ICUE, bien qu'un cadre commun soit nécessaire à cet égard. Toutefois, si une entité de l'Union le requiert expressément, l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-UE) devrait être en mesure de fournir une assistance à cette entité de l'Union pour les incidents survenant dans des environnements TIC classifiés.

(17) Les entités de l'Union devraient évaluer les risques liés aux relations avec les fournisseurs et les fournisseurs de services, y compris les fournisseurs de services de stockage et de traitement des données ou de services de sécurité gérés, et prendre les mesures appropriées pour y faire face. Ces mesures de cybersécurité devraient être précisées dans des orientations ou des recommandations publiées 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'Union, notamment des évaluations des risques de cybersécurité et des recommandations formulées par le groupe de coopération institué par l'article 14 de la directive (UE) 2022/2555, telles que l'évaluation coordonnée pour l'UE des risques concernant la cybersécurité des réseaux 5G et la boîte à outils de l'UE pour la cybersécurité 5G. En outre,

compte tenu de l'éventail des cybermenaces et de l'importance, pour les entités de l'Union, de renforcer la cyberrésilience, la certification des produits TIC, services TIC et processus TIC pertinents pourrait être requise, dans le cadre de schémas européens de certification de cybersécurité spécifiques adoptés en vertu de l'article 49 du règlement (UE) 2019/881 du Parlement européen et du Conseil ([3]).

(18) En mai 2011, les secrétaires généraux des institutions et organes de l'Union ont décidé de mettre en place d'une équipe de préconfiguration pour la 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'Union. 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 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 ([4]). Le présent règlement devrait prévoir un ensemble complet de règles relatives à l'organisation, au fonctionnement et à la gestion 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.

(19) La CERT-UE devrait désormais être dénommée «service de cybersécurité pour les institutions, organes et organismes de l'Union» (le CERT-UE). La dénomination abrégée «CERT-UE» devrait toutefois être conservée en raison de sa notoriété.

(20) Indépendamment de l'extension des missions du CERT-UE et de l'élargissement de son rôle, le présent règlement institue le conseil interinstitutionnel de cybersécurité (IICB), en vue de faciliter l'instauration d'un niveau élevé commun de cybersécurité parmi les entités de l'Union. L'IICB devrait jouer un rôle exclusif pour surveiller et soutenir la mise en œuvre du présent règlement par les entités de l'Union, superviser la mise en œuvre des priorités et des objectifs généraux du CERT-UE et fournir des orientations stratégiques au CERT-UE. Par conséquent, l'IICB devrait assurer la représentation des institutions de l'Union et inclure des représentants des organes et organismes de l'Union par l'intermédiaire du réseau des agences de l'Union (EUAN). L'organisation et le fonctionnement de l'IICB devraient également être régis par un 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 devrait pouvoir instituer un comité exécutif chargé de l'assister dans ses travaux et lui déléguer certaines de ses tâches et compétences, notamment 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 de 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 conformité 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 compétences.

(21) L'IICB a pour but d'aider les entités de l'Union à améliorer leur posture de cybersécurité respective grâce à la mise en œuvre du présent règlement. Afin d'aider les entités de l'Union, l'IICB devrait fournir des orientations au chef du CERT-UE, adopter une stratégie pluriannuelle visant à relever le niveau de cybersécurité dans les entités de l'Union, mettre au point la méthode et les autres aspects relatifs aux évaluations volontaires par les pairs, et faciliter la création d'un groupe informel de responsables locaux de la cybersécurité, soutenu par l'Agence de l'Union européenne pour la cybersécurité (ENISA), afin d'échanger de bonnes pratiques et des informations relatives à la mise en œuvre du présent règlement.

([3]) 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) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

([4]) Accord interinstitutionnel entre le Parlement européen, le Conseil européen, le Conseil de l'Union européenne, la Commission européenne, la Cour de justice de l'Union européenne, la Banque centrale européenne, la Cour des comptes européenne, le Service européen pour l'action extérieure, le Comité économique et social européen, le Comité européen des régions et la Banque européenne d'investissement relatif à l'organisation et au fonctionnement d'une équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union (CERT-UE) (JO C 12 du 13.1.2018, p. 1).

(22) Afin de parvenir à un niveau élevé de cybersécurité dans toutes les entités de l'Union, trois représentants désignés par l'EUAN devraient représenter au sein de l'IICB les intérêts des organes et organismes de l'Union qui gèrent leur propre environnement TIC. La sécurité du traitement des données à caractère personnel et la cybersécurité de celles-ci sont essentielles à la protection des données. Compte tenu des synergies entre la protection des données et la cybersécurité, le Contrôleur européen de la protection des données devrait être représenté au sein de l'IICB, en tant qu'entité de l'Union soumise au présent règlement et disposant d'une compétence spécifique en matière de protection des données, y compris pour la sécurité des réseaux de communications électroniques. L'innovation et la compétitivité étant cruciales en matière de cybersécurité, le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité devrait être représenté au sein de l'IICB. Compte tenu du rôle et des compétences de l'ENISA en matière de cybersécurité, du soutien qu'elle apporte et de l'importance de la cybersécurité des infrastructures et des services spatiaux de l'Union, l'ENISA et l'Agence de l'Union européenne pour le programme spatial devraient être représentées au sein de l'IICB. Vu le rôle que le présent règlement confie au CERT-UE, le président de l'IICB devrait inviter le chef du CERT-UE à toutes les réunions de l'IICB, sauf lorsque ce dernier examine des questions directement liées au chef du CERT-UE.

(23) L'IICB devrait contrôler le respect du présent règlement ainsi que la mise en œuvre des orientations, des recommandations et des injonctions. Sur les questions techniques, l'IICB devrait être assisté de groupes consultatifs techniques composés comme il l'estime opportun. Ces groupes consultatifs techniques devraient travailler en étroite coopération avec le CERT-UE, les entités de l'Union et d'autres parties prenantes, le cas échéant.

(24) Lorsque l'IICB constate qu'une entité de l'Union n'a pas réellement mis en œuvre le présent règlement ou les orientations, recommandations ou injonctions élaborées au titre du présent règlement, l'IICB devrait être habilité à prendre des mesures de conformité, sans préjudice des procédures internes de l'entité de l'Union concernée. L'IICB devrait appliquer les mesures de conformité de manière progressive; en d'autres termes, il devrait prendre d'abord la mesure la moins sévère, à savoir un avis motivé, puis, si nécessaire uniquement, des mesures de plus en plus sévères, jusqu'à la recommandation de suspension temporaire des flux de données vers l'entité de l'Union concernée, ce qui constitue la mesure la plus sévère. Une telle recommandation ne devrait être appliquée que dans des cas exceptionnels, lorsque l'entité de l'Union concernée viole le présent règlement de manière persistante, délibérée, répétée ou grave.

(25) L'avis motivé constitue la mesure de conformité la moins sévère face à des lacunes observées dans la mise en œuvre du présent règlement. L'IICB devrait être habilité à faire suivre un avis motivé d'orientations visant à aider l'entité de l'Union à veiller à ce que son cadre, ses mesures de gestion des risques de cybersécurité, son plan de cybersécurité et sa communication d'information respectent le présent règlement, puis d'un avertissement exhortant l'entité de l'Union concernée à remédier aux lacunes constatées dans un délai déterminé. S'il n'a pas suffisamment été remédié aux lacunes visées par l'avertissement, l'IICB devrait être habilité à transmettre une notification motivée.

(26) L'IICB devrait pouvoir recommander la réalisation d'un audit d'une entité de l'Union. L'entité de l'Union devrait pouvoir recourir à sa fonction d'audit interne à cette fin. L'IICB devrait également être habilité à 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.

(27) Dans des cas exceptionnels où une entité de l'Union viole le présent règlement de manière persistante, délibérée, répétée ou grave, l'IICB devrait pouvoir, en dernier ressort, recommander à tous les États membres et à toutes les entités de l'Union la suspension temporaire des flux de données à destination de l'entité de l'Union, qui devrait s'appliquer jusqu'à ce que celle-ci mette fin à la violation. Une telle recommandation devrait être communiquée par des canaux de communication sécurisés et appropriés.

(28) Pour veiller à la bonne application du présent règlement, si l'IICB considère qu'une violation persistante de celui-ci est directement imputable aux actions ou aux omissions d'un membre du personnel d'une entité de l'Union, y compris au niveau hiérarchique le plus élevé, l'IICB devrait demander à l'entité de l'Union concernée de prendre les mesures appropriées, voire d'envisager des mesures de nature disciplinaire, conformément aux règles et aux procédures énoncées dans le statut des fonctionnaires de l'Union européenne et le régime applicable aux autres agents de l'Union européenne, fixés par le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil ([5]) (ci-après dénommé «statut») et à toutes les autres règles et procédures applicables.

(29) Le CERT-UE devrait contribuer à la sécurité de l'environnement TIC de l'ensemble des entités de l'Union. Lorsqu'il envisage, à la demande d'une entité de l'Union, de fournir des conseils ou des contributions techniques sur des questions politiques pertinentes, le CERT-UE devrait veiller à ce que cela n'entrave pas l'accomplissement des autres tâches qui lui incombent au titre du présent règlement. Le CERT-UE devrait jouer, pour les entités de l'Union, un rôle équivalent à celui de coordinateur désigné aux fins de la divulgation coordonnée des vulnérabilités conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555.

(30) Le CERT-UE devrait soutenir la mise en œuvre de mesures visant à assurer un niveau élevé commun de cybersécurité, en proposant des orientations et des recommandations à l'intention de l'IICB ou en émettant des injonctions. Ces orientations et recommandations devraient être approuvées par l'IICB. Le cas échéant, le CERT-UE devrait émettre des injonctions décrivant les mesures de sécurité urgentes que les entités de l'Union sont vivement encouragées à prendre dans un délai déterminé. L'IICB devrait donner instruction au CERT-UE d'élaborer, de retirer ou de modifier une proposition d'orientation ou de recommandation, ou une injonction.

(31) Le CERT-UE devrait également remplir le rôle qui lui est assigné dans la directive (UE) 2022/2555 en ce qui concerne la coopération et l'échange d'informations avec le réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT) institué en vertu de l'article 15 de ladite directive. En outre, conformément à la recommandation (UE) 2017/1584 de la Commission ([6]), le CERT-UE devrait, en ce qui concerne la réaction, assurer la coopération et la coordination avec les parties prenantes concernées. Afin de contribuer à un niveau élevé de cybersécurité dans l'ensemble de l'Union, le CERT-UE devrait partager avec ses homologues des États membres des informations spécifiques aux incidents. Il devrait également collaborer avec d'autres homologues publics et privés, y compris au sein de l'Organisation du traité de l'Atlantique Nord, sous réserve de l'approbation préalable de l'IICB.

(32) Pour soutenir la cybersécurité opérationnelle, le CERT-UE devrait faire appel à l'expertise disponible de l'ENISA dans le cadre de la coopération structurée prévue par le règlement (UE) 2019/881 du Parlement européen et du Conseil. Le cas échéant, les deux entités devraient conclure des accords spécifiques afin de définir les modalités pratiques de cette coopération et d'éviter la duplication des activités. Le CERT-UE devrait coopérer avec l'ENISA en ce qui concerne l'analyse des cybermenaces et lui transmettre régulièrement son rapport sur le panorama des menaces.

(33) Le CERT-UE devrait être en mesure de coopérer et d'échanger des informations avec les communautés de cybersécurité pertinentes au sein de l'Union et de ses États membres, afin de promouvoir la coopération opérationnelle et de permettre aux réseaux existants de réaliser pleinement leur potentiel de protection de l'Union.

(34) Étant donné que les services et les missions du CERT-UE sont dans l'intérêt des entités de l'Union, chaque entité de l'Union engageant des dépenses TIC devrait contribuer équitablement à ces services et missions. Ces contributions sont sans préjudice de l'autonomie budgétaire des entités de l'Union.

([5]) Règlement (CEE, Euratom, CECA) n° 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, et instituant des mesures particulières temporairement applicables aux fonctionnaires de la Commission (JO L 56 du 4.3.1968, p. 1).

([6]) 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).

(35) De nombreuses cyberattaques s'inscrivent dans le cadre de campagnes plus larges qui ciblent des groupes d'entités de l'Union ou des communautés d'intérêt auxquelles appartiennent les entités de l'Union. Afin de permettre la détection proactive, la réaction en cas d'incident, l'adoption de mesures d'atténuation et le rétablissement à la suite d'un incident, les entités de l'Union devraient être en mesure de notifier au CERT-UE les incidents, cybermenaces, vulnérabilités et incidents évités, et partager les renseignements techniques appropriés permettant de détecter ou d'atténuer de tels incidents, cybermenaces, vulnérabilités et incidents évités, ainsi que d'y réagir, dans d'autres entités de l'Union. Suivant la même approche que dans la directive (UE) 2022/2555, les entités de l'Union devraient être tenues de soumettre une alerte précoce au CERT-UE dans un délai de vingt-quatre heures après avoir eu connaissance d'un incident important. Cet échange d'informations devrait permettre au CERT-UE d'informer les autres entités de l'Union et leurs homologues concernés, afin de contribuer à protéger les environnements TIC des entités de l'Union et de leurs homologues contre des incidents similaires.

(36) Le présent règlement définit une approche de la notification des incidents importants en plusieurs étapes, afin de trouver le juste équilibre entre, d'une part, la notification rapide qui aide à atténuer la propagation potentielle des incidents importants et permet aux entités de l'Union de demander une assistance et, d'autre part, la notification approfondie qui permet de tirer des leçons précieuses des incidents individuels et d'améliorer au fil du temps la cyberrésilience des diverses entités de l'Union ainsi que de contribuer à améliorer de manière générale leur posture de cybersécurité. 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 concernée, pourraient entraîner des perturbations opérationnelles graves du fonctionnement de l'entité de l'Union concernée ou des pertes financières pour celle-ci, ou nuire à d'autres personnes physiques ou morales en causant des préjudices considérables, matériels ou non. Cette évaluation initiale devrait tenir compte, entre autres, des réseaux et des systèmes d'information touchés, 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 doit être qualifiée de grave.

(37) Étant donné que l'infrastructure, les réseaux et les systèmes d'information de l'entité de l'Union concernée et ceux 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 informer les homologues concernés des États membres désignés ou établis en vertu des articles 8 et 10 de la directive (UE) 2022/2555 qu'un incident important s'est produit et qu'elle va le signaler au CERT-UE. Lorsque le CERT-UE apprend qu'un incident important s'est produit dans un État membre, il devrait informer tout homologue concerné dans ledit État membre.

(38) 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, qui délimite clairement les rôles et les responsabilités des entités de l'Union concernées. Conformément au plan de gestion des crises de cybersécurité, le représentant de la Commission à l'IICB devrait faire office de point de contact pour faciliter le partage des informations pertinentes relatives aux incidents majeurs avec le réseau européen d'organisations de liaison en cas de crises de cybersécurité (EU-CyCLONe), afin de contribuer à l'appréciation commune de la situation. Le rôle du représentant de la Commission à l'IICB en tant que point de contact devrait être sans préjudice du rôle distinct de la Commission au sein d'EU-CyCLONe, en vertu de l'article 16, paragraphe 2, de la directive (UE) 2022/2555.

(39) Le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([7]) s'applique à tout traitement des données à caractère personnel effectué au titre du présent règlement. Des données à caractère personnel pourraient subir un traitement au titre de mesures adoptées dans le cadre de la gestion des risques de cybersécurité, de la vulnérabilité et des incidents, du partage d'informations sur les incidents, les cybermenaces et les vulnérabilités, ainsi que de la coordination de la réaction aux incidents et de la coopération. Ces mesures pourraient nécessiter le traitement de certaines catégories de données à caractère personnel, telles que les adresses IP, les localisateurs de ressources

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

uniformes (URL), les noms de domaine, les adresses électroniques, le rôle des personnes concernées dans l'organisation, les horodatages, les objets de courriers électroniques ou les noms de fichiers. Toute mesure prise au titre du présent règlement devrait respecter le cadre réglementaire en matière de protection des données et de la vie privée. Les entités de l'Union, le CERT-UE et, le cas échéant, l'IICB devraient prendre toutes les garanties techniques et organisationnelles utiles pour garantir ce respect de manière responsable.

(40) Le présent règlement constitue la base juridique du traitement de données à caractère personnel par les entités de l'Union, le CERT-UE et, le cas échéant, l'IICB aux fins de l'exécution de leurs tâches et de leurs obligations au titre du présent règlement, conformément à l'article 5, paragraphe 1, point b), du règlement (UE) 2018/1725. Le CERT-UE peut jouer le rôle de sous-traitant ou de responsable du traitement, en fonction de la tâche qu'il exécute au titre du règlement (UE) 2018/1725.

(41) Dans certains cas, pour s'acquitter des obligations, qui leur incombent au titre du présent règlement, de garantir un niveau élevé de cybersécurité, en particulier dans le cadre de la gestion de la vulnérabilité et des incidents, les entités de l'Union et le CERT-UE peuvent se voir obligés de traiter des catégories particulières de données à caractère personnel, visées à l'article 10, paragraphe 1, du règlement (UE) 2018/1725. Le présent règlement constitue la base juridique du traitement des catégories particulières de données à caractère personnel par les entités de l'Union et le CERT-UE, conformément à l'article 10, paragraphe 2, point g), du règlement (UE) 2018/1725. Le traitement de catégories particulières de données à caractère personnel au titre du présent règlement devrait être strictement proportionné au but poursuivi. Sous réserve des conditions fixées à l'article 10, paragraphe 2, point g), du règlement susmentionné, les entités de l'Union et le CERT-UE ne devraient être habilités à traiter de telles données que dans la mesure de ce qui est nécessaire, et uniquement lorsque le présent règlement le prévoit explicitement. Lors du traitement de catégories particulières de données à caractère personnel, les entités de l'Union et le CERT-UE devraient respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour protéger les droits fondamentaux et les intérêts des personnes concernées.

(42) Conformément à l'article 33 du règlement (UE) 2018/1725 et compte tenu de l'état de la technique, des coûts de mise en œuvre, de la nature, de l'objet, du contexte et des finalités du traitement, ainsi que de la probabilité et de la gravité des risques d'atteinte aux droits et aux libertés des personnes physiques, les entités de l'Union et le CERT-UE devraient prendre des mesures techniques et organisationnelles appropriées pour garantir un niveau adéquat de sécurité des données à caractère personnel, par exemple accorder des droits d'accès restreints fondés sur le besoin d'en connaître, appliquer des principes de piste d'audit, adopter une chaîne de contrôle, conserver les données au repos dans un environnement contrôlé et susceptible de faire l'objet d'un audit, suivre des procédures opérationnelles normalisées et adopter des mesures de protection de la vie privée, comme la pseudonymisation ou le chiffrement. La mise en œuvre de ces mesures ne devrait pas affecter les finalités du traitement des incidents ni l'intégrité des preuves. Lorsqu'une entité de l'Union ou le CERT-UE transfèrent des données à caractère personnel liées à un incident, y compris des catégories particulières de données à caractère personnel, à un homologue ou à un partenaire aux fins du présent règlement, le transfert devrait respecter le règlement (UE) 2018/1725. Lorsque des catégories particulières de données à caractère personnel sont transférées à un tiers, les entités de l'Union et le CERT-UE devraient veiller à ce que ce tiers applique des mesures de protection des données à caractère personnel à un niveau équivalent à celui du règlement (UE) 2018/1725.

(43) Les données à caractère personnel traitées aux fins du présent règlement ne devraient être conservées que le temps nécessaire conformément au règlement (UE) 2018/1725. Les entités de l'Union et, le cas échéant, le CERT-UE agissant en qualité de responsable du traitement devraient fixer des durées de conservation limitées à ce qui est nécessaire pour atteindre les objectifs poursuivis. En ce qui concerne en particulier les données à caractère personnel collectées aux fins du traitement des incidents, les entités de l'Union et le CERT-UE devraient établir une distinction entre les données à caractère personnel qui sont collectées aux fins de la détection d'une cybermenace dans leur environnement TIC pour prévenir un incident et les données à caractère personnel qui sont collectées aux fins de l'atténuation d'un incident et de la réaction et du rétablissement à la suite de celui-ci. Aux fins de la détection d'une cybermenace, il importe de tenir compte du temps pendant lequel un acteur de la menace peut rester dans un système sans être détecté. Aux fins de l'atténuation d'un incident et de la réaction et du rétablissement à la suite d'un incident, il est important d'examiner si les données à caractère personnel sont nécessaires pour localiser et traiter un incident récurrent ou un incident de nature similaire pour lequel une corrélation pourrait être démontrée.

(44) Le traitement des informations par les entités de l'Union et le CERT-UE devrait être conforme aux règles applicables en matière de sécurité de l'information. L'inclusion de la sécurité des ressources humaines en tant que mesure de gestion des risques de cybersécurité devrait également être conforme aux règles applicables.

(45) Aux fins du partage d'informations, des marquages visibles sont utilisés pour indiquer que les destinataires d'informations doivent appliquer des limitations au partage sur la base, notamment, d'accords de non-divulgation 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 CSIRT et par certains centres d'échange et d'analyse d'informations.

(46) Le présent règlement devrait être évalué régulièrement à la lumière des futures négociations sur les cadres financiers pluriannuels afin que de nouvelles décisions puissent être prises en ce qui concerne le fonctionnement et le rôle institutionnel du CERT-UE, y compris la transformation éventuelle du CERT-UE en organisme de l'Union.

(47) L'IICB, avec l'aide du CERT-UE, devrait examiner et évaluer la mise en œuvre du présent règlement et faire part de ses conclusions à la Commission. La Commission devrait s'appuyer sur ces conclusions pour faire rapport au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Ce rapport, contenant les conclusions de l'IICB, devrait évaluer l'opportunité d'inclure les réseaux et systèmes d'information traitant des ICUE dans le champ d'application du présent règlement, en particulier en l'absence de règles en matière de sécurité de l'information communes aux entités de l'Union.

(48) Conformément au principe de proportionnalité, il est nécessaire et approprié, pour réaliser l'objectif fondamental consistant à parvenir à un niveau élevé commun de cybersécurité au sein des entités de l'Union, de fixer des règles régissant la cybersécurité pour les entités de l'Union. Le présent règlement n'excède pas ce qui est nécessaire pour atteindre l'objectif poursuivi, conformément à l'article 5, paragraphe 4, du traité sur l'Union européenne.

(49) Le présent règlement reflète le fait que les entités de l'Union diffèrent par leur taille et leur capacité, y compris en ce qui concerne leurs ressources financières et humaines.

(50) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu un avis le 17 mai 2022 ([8]),

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GENERALES

Article premier

Objet

Le présent règlement établit des mesures visant à parvenir à un niveau élevé commun de cybersécurité au sein des entités de l'Union en ce qui concerne:

a) l'établissement par chaque entité de l'Union d'un cadre interne de gestion, de gouvernance et de contrôle des risques de cybersécurité en vertu de l'article 6;

b) la gestion des risques de cybersécurité, la communication et le partage d'informations;

c) l'organisation, le fonctionnement et la gestion du conseil interinstitutionnel de cybersécurité institué en vertu de l'article 10, ainsi que l'organisation, le fonctionnement et la gestion du service de cybersécurité pour les institutions, organes et organismes de l'Union (CERT-UE);

d) le suivi de la mise en œuvre du présent règlement.

([8]) JO C 258 du 5.7.2022, p. 10.

Article 2

Champ d'application

1. Le présent règlement s'applique aux entités de l'Union, au conseil interinstitutionnel de cybersécurité institué en vertu de l'article 10 et au CERT-UE.

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

3. À l'exception de l'article 13, paragraphe 8, 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 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 conformément à ces traités;

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

3) «sécurité des réseaux et des systèmes d'information», la sécurité des réseaux et des systèmes d'information telle qu'elle est définie à l'article 6, point 2), de la directive (UE) 2022/2555;

4) «cybersécurité», la cybersécurité telle qu'elle est définie 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 chargés du fonctionnement d'une entité de l'Union au niveau administratif le plus élevé, ayant pour mandat d'adopter ou d'autoriser des décisions conformément aux dispositifs de gouvernance à haut niveau de cette entité, sans préjudice des responsabilités formelles incombant aux autres niveaux hiérarchiques en matière de conformité et en ce qui concerne la gestion des risques de cybersécurité dans leurs domaines de compétence respectifs;

6) «incident évité», un incident évité tel qu'il est défini à l'article 6, point 5), de la directive (UE) 2022/2555;

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

8) «incident majeur», un incident qui provoque des perturbations dépassant les capacités de réaction d'une entité de l'Union et du CERT-UE ou qui a une incidence notable sur au moins deux entités de l'Union;

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

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

11) «cybermenace», une cybermenace telle qu'elle est définie à l'article 2, point 8), du règlement (UE) 2019/881;

12) «cybermenace importante», une cybermenace importante telle qu'elle est définie à l'article 6, point 11), de la directive (UE) 2022/2555;

13) «vulnérabilité», une vulnérabilité telle qu'elle est définie à l'article 6, point 15), de la directive (UE) 2022/2555;

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

15) «service d'informatique en nuage», un service d'informatique en nuage tel qu'il est défini à l'article 6, point 30), de la directive (UE) 2022/2555.

Article 4

Traitement des données à caractère personnel

1. Le traitement, par le CERT-UE, le conseil interinstitutionnel de cybersécurité institué en vertu de l'article 10 et les entités de l'Union, de données à caractère personnel au titre du présent règlement est effectué conformément au règlement (UE) 2018/1725.

2. Lorsqu'ils exécutent des tâches ou remplissent des obligations en vertu du présent règlement, le CERT-UE, le conseil interinstitutionnel de cybersécurité institué en vertu de l'article 10 et les entités de l'Union ne traitent et n'échangent des données à caractère personnel que dans la mesure nécessaire et dans le seul but d'exécuter ces tâches ou de remplir ces obligations.

3. Le traitement de catégories particulières de données à caractère personnel visées à l'article 10, paragraphe 1, du règlement (UE) 2018/1725 est considéré comme nécessaire pour des raisons d'intérêt public important conformément à l'article 10, paragraphe 2, point g), dudit règlement. Ces données ne peuvent être traitées que dans la mesure nécessaire à la mise en œuvre des mesures de gestion des risques de cybersécurité visées aux articles 6 et 8, à la fourniture de services par le CERT-UE au titre de l'article 13, au partage d'informations propres à un incident au titre de l'article 17, paragraphe 3, et de l'article 18, paragraphe 3, au partage d'informations au titre de l'article 20, aux obligations en matière de communication d'informations prévues à l'article 21, à la coordination de la réaction aux incidents et à la coopération au titre de l'article 22 et à la gestion des incidents majeurs au titre de l'article 23 du présent règlement. Les entités de l'Union et le CERT-UE, lorsqu'ils agissent en qualité de responsables du traitement, appliquent des mesures techniques pour empêcher le traitement des catégories particulières de données à caractère personnel à d'autres fins et prévoient des mesures appropriées et spécifiques pour protéger les droits fondamentaux et les intérêts des personnes concernées.

CHAPITRE II

MESURES DESTINEES A ASSURER UN NIVEAU ELEVE COMMUN DE CYBERSECURITE

Article 5

Mise en œuvre des mesures

1. Au plus tard le 8 septembre 2024, le conseil interinstitutionnel de cybersécurité institué en vertu de l'article 10 publie, après consultation de l'Agence de l'Union européenne pour la cybersécurité (ENISA) et après avoir reçu des orientations du CERT-UE, des lignes directrices à l'intention des entités de l'Union aux fins de procéder à un examen initial de la cybersécurité et d'établir un cadre interne de gestion, de gouvernance et de contrôle des risques de cybersécurité conformément à l'article 6, de procéder à des évaluations de la maturité en matière de cybersécurité conformément à l'article 7, de prendre des mesures de gestion des risques de cybersécurité conformément à l'article 8 et d'adopter le plan de cybersécurité conformément à l'article 9.

2. Lorsqu'elles mettent en œuvre les articles 6 à 9, les entités de l'Union tiennent compte des lignes directrices visées au paragraphe 1 du présent article, ainsi que des lignes directrices et recommandations pertinentes adoptées en vertu des articles 11 et 14.

Article 6

Cadre de gestion, de gouvernance et de contrôle des risques de cybersécurité

1. Au plus tard le 8 avril 2025, chaque entité de l'Union établit, après avoir procédé à un examen initial de la cybersécurité, tel qu'un audit, un cadre interne de gestion, de gouvernance et de contrôle des risques de cybersécurité (ci-après dénommé «cadre»). L'établissement du cadre est placé sous la supervision et la responsabilité du niveau hiérarchique le plus élevé de l'entité de l'Union.

2. Le cadre couvre l'ensemble de l'environnement TIC non classifié de l'entité de l'Union concernée, y compris l'environnement TIC sur sites, 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 ces environnements (ci-après dénommé «environnement TIC»). Le cadre est fondé sur une approche «tous risques».

3. Le cadre garantit un niveau élevé de cybersécurité. Le cadre établit des politiques internes de cybersécurité, y compris des objectifs et des priorités, pour la sécurité des réseaux et des systèmes d'information, ainsi que les rôles et les responsabilités du personnel de l'entité de l'Union chargé d'assurer la mise en œuvre effective du présent règlement. Le cadre comprend également des mécanismes visant à mesurer l'efficacité de la mise en œuvre.

4. Le cadre fait régulièrement l'objet d'une révision, compte tenu de l'évolution des risques de cybersécurité, et au moins tous les quatre ans. Le cas échéant et à la suite d'une demande du conseil interinstitutionnel de cybersécurité institué en vertu de l'article 10, le cadre d'une entité de l'Union peut être mis à jour sur la base des orientations données par le CERT-UE sur les incidents identifiés ou les lacunes éventuelles observées dans la mise en œuvre du présent règlement.

5. Le niveau hiérarchique le plus élevé de chaque entité de l'Union est responsable de la mise en œuvre du présent règlement et contrôle le respect, par son entité, des obligations liées au cadre.

6. 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 des membres du personnel d'encadrement supérieur au sens de l'article 29, paragraphe 2, du statut ou à d'autres fonctionnaires de niveau équivalent, au sein de l'entité de l'Union concernée. Indépendamment d'une telle délégation, le niveau hiérarchique le plus élevé peut être tenu pour responsable des infractions au présent règlement commises par l'entité de l'Union concernée.

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

8. 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 le 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 au CERT-UE sur la base d'un accord de niveau de service conclu entre cette entité de l'Union et le CERT-UE, ou ces tâches peuvent être partagées entre plusieurs entités de l'Union. Lorsque ces tâches sont déléguées au CERT-UE, le conseil interinstitutionnel de cybersécurité institué en vertu de l'article 10 décide si la fourniture de ce service fait partie des services de base du CERT-UE, en tenant compte des ressources humaines et financières de l'entité de l'Union concernée. Chaque entité de l'Union informe le CERT-UE, dans les meilleurs délais, de la désignation du responsable local de cybersécurité, ainsi que de tout changement ultérieur.

Le CERT-UE établit et tient à jour une liste des responsables locaux de la cybersécurité désignés.

9. Les membres de l'encadrement supérieur au sens de l'article 29, paragraphe 2, du statut ou d'autres fonctionnaires de niveau équivalent de chaque entité de l'Union ainsi que tous les membres du personnel pertinents chargés de la mise en œuvre des mesures et de l'exécution des obligations de gestion des risques de cybersécurité définies par le présent règlement suivent régulièrement une formation spécifique afin d'acquérir des connaissances et des compétences suffisantes pour appréhender et évaluer les pratiques en matière de gestion des risques et de gestion de la cybersécurité et leur incidence sur les activités de l'entité de l'Union.

Article 7

Évaluations de la maturité en matière de cybersécurité

1. Au plus tard le 8 juillet 2025 et au moins tous les deux ans par la suite, chaque entité de l'Union procède à une évaluation de la maturité en matière de cybersécurité portant sur l'ensemble des éléments de son environnement TIC.

2. Les évaluations de la maturité en matière de cybersécurité sont effectuées, le cas échéant, avec l'aide d'un tiers spécialisé.

3. Les entités de l'Union ayant des structures similaires peuvent coopérer à la réalisation d'évaluations de la maturité en matière de cybersécurité pour leurs entités respectives.

4. Sur la base d'une demande du conseil interinstitutionnel de cybersécurité institué en vertu de l'article 10 et avec le consentement explicite de l'entité de l'Union concernée, les résultats d'une évaluation de la maturité en matière de cybersécurité peuvent être discutés au sein dudit conseil ou du groupe informel de responsables locaux de la cybersécurité afin de tirer les leçons des expériences et de partager les bonnes pratiques.

Article 8

Mesures de gestion des risques de cybersécurité

1. Dans les meilleurs délais et en tout état de cause au plus tard le 8 septembre 2025, chaque entité de l'Union prend, sous la supervision du niveau hiérarchique le plus élevé, des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées afin de gérer les risques de cybersécurité identifiés dans le cadre et de prévenir et réduire les conséquences des incidents. Ces mesures garantissent, pour les réseaux et les systèmes d'information de la totalité de l'environnement TIC, un niveau de sécurité adapté aux risques de cybersécurité encourus, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables. Lors de l'évaluation de la proportionnalité de ces mesures, il est tenu dûment compte du degré d'exposition de l'entité de l'Union aux risques de cybersécurité, de sa taille et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales, économiques et interinstitutionnelles.

2. Les entités de l'Union tiennent compte au moins des domaines suivants dans la mise en œuvre des mesures de gestion des risques de cybersécurité:

a) la politique de cybersécurité, y compris les mesures nécessaires pour atteindre les objectifs et les priorités visés à l'article 6 et au paragraphe 3 du présent article;

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

c) les objectifs stratégiques concernant l'utilisation des services d'informatique en nuage;

d) un audit de cybersécurité, le cas échéant, qui peut inclure une évaluation des risques de cybersécurité, de la vulnérabilité et des cybermenaces, et des tests d'intrusion effectués régulièrement par un fournisseur privé de confiance;

e) la mise en œuvre des recommandations découlant des audits de cybersécurité visés au point d) au moyen de mises à jour de la cybersécurité et des politiques;

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

g) la gestion des actifs, y compris l'inventaire des actifs TIC et la cartographie des réseaux TIC;

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

i) la sécurité des activités;

j) la sécurité des communications;

k) l'acquisition, le développement et la maintenance des systèmes, y compris les politiques de traitement et de divulgation des vulnérabilités;

l) dans la mesure du possible, les politiques en matière de transparence du code source des systèmes;

m) 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;

n) le traitement des incidents et la coopération avec le CERT-UE, par exemple la maintenance du suivi de la sécurité et de la journalisation;

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

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

Aux fins du premier alinéa, point m), 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.

3. Les entités de l'Union prennent au moins les mesures spécifiques suivantes en matière de gestion des risques de cybersécurité:

a) les modalités techniques visant à permettre le télétravail et à en assurer la pérennité;

b) des mesures concrètes pour progresser vers les principes de vérification systématique;

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

d) l'utilisation de la cryptographie et du chiffrement, en particulier le chiffrement de bout en bout, ainsi que les signatures numériques sécurisées;

e) le cas échéant, des communications vocales, vidéo et textuelles sécurisées, et des systèmes de communication d'urgence sécurisés au sein de l'entité de l'Union;

f) des mesures préventives de détection et de suppression des logiciels malveillants et des logiciels espions;

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

h) l'élaboration et l'adoption de programmes de formation à la cybersécurité en fonction des missions confiées et des capacités escomptées à l'intention du niveau hiérarchique le plus élevé et des membres du personnel de l'entité de l'Union chargés d'assurer la mise en œuvre effective du présent règlement;

i) la formation régulière des membres du personnel à la cybersécurité;

j) le cas échéant, la participation à des analyses des risques que présente l'interconnexion entre les entités de l'Union;

k) 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 TIC et le CERT-UE;

   ii) l'obligation contractuelle de signaler les incidents, les vulnérabilités et les cybermenaces ainsi que de veiller à ce que des mécanismes appropriés de réaction et de suivi en cas d'incident soient en place.

Article 9

Plans de cybersécurité

1. Compte tenu de la conclusion de l'évaluation de la maturité en matière de cybersécurité effectuée conformément à l'article 7 et des actifs et des risques de cybersécurité identifiés dans le cadre, ainsi que des mesures de gestion des risques de cybersécurité prises conformément à l'article 8, le niveau hiérarchique le plus élevé de chaque entité de l'Union approuve un plan de cybersécurité dans les meilleurs délais et en tout état de cause au plus tard le 8 janvier 2026. Le plan de cybersécurité vise à accroître la cybersécurité globale de l'entité de l'Union et contribue ainsi à renforcer le niveau élevé commun de cybersécurité au sein des entités de l'Union. Le plan de cybersécurité comprend au moins les mesures de gestion des risques de cybersécurité prises conformément à l'article 8. Le plan de cybersécurité est révisé tous les deux ans ou plus fréquemment, le cas échéant, à la suite des évaluations de la maturité en matière de cybersécurité effectuées conformément à l'article 7 ou de toute révision substantielle du cadre.

2. Le plan de cybersécurité comprend le plan de gestion des crises de cybersécurité de l'entité de l'Union en cas d'incidents majeurs.

3. L'entité de l'Union soumet le plan de cybersécurité complet au conseil interinstitutionnel de cybersécurité institué en vertu de l'article 10.

CHAPITRE III

CONSEIL INTERINSTITUTIONNEL DE CYBERSECURITE

Article 10

Conseil interinstitutionnel de cybersécurité

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

2. L'IICB est chargé:

a) de suivre et de soutenir 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 le 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;

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;

xiii) l'ENISA;

xiv) le Contrôleur européen de la protection des données (CEPD);

xv) l'Agence de l'Union européenne pour le programme spatial.

b) de 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 de l'Union qui gèrent leur propre environnement TIC, autres que ceux visés au point a).

Les entités de l'Union représentées au sein de l'IICB s'efforcent de parvenir à un équilibre entre les femmes et les hommes parmi les représentants désignés.

4. Chaque membre de l'IICB peut être assisté d'un suppléant. D'autres représentants des entités de l'Union visées au paragraphe 3 ou d'autres entités de l'Union peuvent être invités par le président à assister aux réunions de l'IICB sans droit de vote.

5. Le chef du CERT-UE et les présidents du groupe de coopération, du réseau des CSIRT et de EU-CyCLONe établis, respectivement, en vertu des articles 14, 15 et 16 de la directive (UE) 2022/2555, ou leurs suppléants, peuvent participer aux réunions de l'IICB en tant qu'observateurs. Dans des circonstances exceptionnelles, l'IICB peut, conformément à son règlement intérieur, en décider autrement.

6. L'IICB adopte son règlement intérieur.

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

8. L'IICB se réunit au moins trois fois par an à l'initiative de son président, à la demande du CERT-UE ou à la demande de l'un de ses membres.

9. 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 de l'IICB ne peut voter qu'en cas d'égalité, sa voix pouvant alors être décisive.

10. L'IICB peut statuer par la voie d'une procédure écrite simplifiée lancée conformément à son règlement intérieur. Dans le cadre de cette procédure, la décision concernée est réputée approuvée dans le délai fixé par le président, sauf objection d'un membre.

11. Le secrétariat de l'IICB est assuré par la Commission et rend compte au président de l'IICB.

12. Les représentants nommés par l'EUAN transmettent les décisions de l'IICB aux membres de l'EUAN. Tout membre de l'EUAN a le droit de soulever auprès de ces représentants ou du président de l'IICB toute question qu'il estime devoir être portée à l'attention de l'IICB.

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

14. Au plus tard le 8 janvier 2025, puis sur une base annuelle, l'IICB présente au Parlement européen et au Conseil un rapport détaillant les progrès réalisés dans la mise en œuvre du présent règlement et précisant notamment l'étendue de la coopération du CERT-UE avec ses homologues des États membres dans chacun d'entre eux. Le rapport constitue une contribution au rapport bisannuel sur l'état de la cybersécurité dans l'Union adopté en vertu de l'article 18 de la directive (UE) 2022/2555.

Article 11

Tâches de l'IICB

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

a) fournir des orientations au chef du CERT-UE;

b) suivre et superviser efficacement la mise en œuvre du présent règlement et aider les entités de l'Union à renforcer leur cybersécurité, y compris, le cas échéant, en demandant des rapports ad hoc aux entités de l'Union et au CERT-UE;

c) à la suite de discussions stratégiques, adopter une stratégie pluriannuelle visant à relever le niveau de cybersécurité dans les entités de l'Union, l'évaluer régulièrement et en tout état de cause tous les cinq ans et, le cas échéant, la modifier;

d) mettre au point la méthodologie et les aspects organisationnels concernant la réalisation d'évaluations volontaires par les pairs par les entités de l'Union, en vue de tirer les enseignements des expériences partagées, de renforcer la confiance mutuelle, d'atteindre un niveau élevé commun de cybersécurité et de renforcer les capacités des entités de l'Union en matière de cybersécurité, en veillant à ce que ces évaluations par les pairs soient menées par des experts en cybersécurité désignés par une entité de l'Union différente de celle qui en fait l'objet et à ce que la méthodologie soit fondée sur l'article 19 de la directive (UE) 2022/2555 et soit, le cas échéant, adaptée aux entités de l'Union;

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

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

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

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

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

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

k) approuver les accords de coopération et les accords ou contrats de niveau de service conclus entre le CERT-UE et d'autres entités conformément à l'article 18;

l) adopter des orientations et des recommandations sur proposition du CERT-UE conformément à l'article 14 et donner instruction au CERT-UE d'élaborer, de retirer ou de modifier une proposition d'orientations ou de recommandations, ou une injonction;

m) créer des groupes consultatifs techniques chargés de missions spécifiques afin d'assister l'IICB dans ses travaux, approuver leur mandat et désigner leurs présidents respectifs;

n) recevoir et évaluer les documents et rapports présentés par les entités de l'Union au titre du présent règlement, tels que les évaluations de la maturité en matière de cybersécurité;

o) faciliter la mise en place d'un groupe informel de responsables locaux de la cybersécurité des entités de l'Union, soutenu par l'ENISA, dans le but d'échanger de bonnes pratiques et des informations relatives à la mise en œuvre du présent règlement;

p) compte tenu des informations fournies par le CERT-UE sur les risques de cybersécurité identifiés et les enseignements tirés, contrôler l'adéquation des dispositifs d'interconnexion entre les environnements TIC des entités de l'Union et donner des conseils sur les améliorations possibles;

q) établir un plan de gestion des crises de cybersécurité en vue de soutenir, au niveau opérationnel, la gestion coordonnée des incidents majeurs affectant les entités de l'Union et de contribuer à l'échange régulier d'informations pertinentes, en particulier en ce qui concerne les conséquences et la gravité des incidents majeurs et les moyens possibles d'en atténuer les effets;

r) coordonner l'adoption des plans individuels de gestion des crises de cybersécurité des entités de l'Union visés à l'article 9, paragraphe 2;

s) adopter des recommandations concernant la sécurité des chaînes d'approvisionnement visée à l'article 8, paragraphe 2, premier alinéa, point m), compte tenu des résultats des évaluations coordonnées au niveau de l'Union des risques pour la sécurité des chaînes d'approvisionnement critiques visées à l'article 22 de la directive (UE) 2022/2555, afin d'aider les entités de l'Union à adopter des mesures efficaces et proportionnées en matière de gestion des risques de cybersécurité;

Article 12

Respect

1. L'IICB suit efficacement, conformément à l'article 10, paragraphe 2, et à l'article 11, la mise en œuvre du présent règlement et des orientations, recommandations et injonctions adoptées par les entités de l'Union. L'IICB peut demander aux entités de l'Union les informations ou les documents nécessaires à cette fin. Aux fins de l'adoption de mesures de conformité au titre du présent article, lorsque l'entité de l'Union concernée est directement représentée au sein de l'IICB, cette entité de l'Union ne dispose pas du droit de vote.

2. Lorsque l'IICB constate qu'une entité de l'Union n'a pas effectivement mis en œuvre le présent règlement ou les orientations, recommandations ou injonctions élaborées 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 concernée la possibilité de présenter ses observations:

a) faire part à l'entité de l'Union concernée de son avis motivé relatif aux lacunes observées dans la mise en œuvre du présent règlement;

b) après consultation du CERT-UE, fournir des orientations à l'entité de l'Union concernée afin que son cadre, ses mesures de gestion des risques de cybersécurité, son plan de cybersécurité et ses rapports soient conformes au présent règlement, dans un délai déterminé;

c) émettre un avertissement pour remédier aux lacunes constatées dans un délai déterminé, y compris des recommandations visant à modifier les mesures adoptées par l'entité de l'Union concernée au titre du présent règlement;

d) transmettre une notification motivée à l'entité de l'Union concernée, dans le cas où il n'a pas été suffisamment remédié, dans le délai imparti, aux lacunes constatées dans un avertissement émis conformément au point c);

e) formuler:

i) une recommandation de procéder à un audit; ou

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

f) le cas échéant, informer la Cour des comptes, dans le cadre de son mandat, du non-respect présumé;

g) émettre une recommandation à l'intention de tous les États membres et toutes les entités de l'Union de suspendre temporairement les flux de données vers l'entité de l'Union concernée.

Aux fins du premier alinéa, point c), les destinataires d'un avertissement sont limités de manière appropriée, lorsque cela s'avère nécessaire en raison du risque de cybersécurité.

Les avertissements et recommandations émis au titre du premier alinéa sont adressés au niveau hiérarchique le plus élevé de l'entité de l'Union concernée.

3. Lorsque l'IICB a adopté des mesures en vertu du paragraphe 2, premier alinéa, points a) à g), l'entité de l'Union concernée fournit des informations détaillées sur les mesures prises et les actions menées pour remédier aux lacunes alléguées constatées par l'IICB. L'entité de l'Union communique ces informations détaillées dans un délai raisonnable à convenir avec l'IICB.

4. Lorsque l'IICB estime qu'il y a une violation persistante 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 de l'Union concernée de prendre les mesures appropriées, y compris en lui demandant d'envisager des mesures de nature disciplinaire, conformément aux règles et procédures énoncées dans le statut des fonctionnaires et à toutes autres règles et procédures applicables. À cette fin, l'IICB transfère les informations nécessaires à l'entité de l'Union concernée.

5. Lorsque des entités de l'Union indiquent être incapables de respecter les délais visés à l'article 6, paragraphe 1, et à l'article 8, paragraphe 1, l'IICB peut, dans des cas dûment motivés, compte tenu de la taille de l'entité de l'Union, autoriser la prolongation de ces délais.

CHAPITRE IV

CERT-UE

Article 13

Mission et tâches du CERT-UE

1. La mission du CERT-UE est de contribuer à la sécurité de l'environnement TIC non classifié des entités de l'Union en leur fournissant des conseils concernant la cybersécurité, en les aidant à prévenir, à détecter et à traiter les incidents, ainsi qu'à en atténuer les effets, à y répondre et à s'en remettre, et en faisant office de pôle d'échange d'informations sur la cybersécurité et de coordination des réponses aux incidents.

2. Le CERT-UE recueille, gère, analyse et partage avec les entités de l'Union des informations sur les cybermenaces, les vulnérabilités et les incidents relatifs aux infrastructures TIC non classifiées. Il 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.

3. Le 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 mesures énoncées à l'article 14, paragraphe 1, ou des rapports ad hoc demandés par l'IICB;

b) offrir des services CSIRT standard aux entités de l'Union au moyen d'un ensemble de services de cybersécurité décrits dans son catalogue de services (ci-après dénommés «services de base»);

c) gérer un réseau de pairs et de partenaires pour soutenir les services visés aux articles 17 et 18;

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 orientations, recommandations et injonctions;

e) sur la base des informations visées au paragraphe 2, contribuer à la conscience situationnelle de la cybersécurité de l'Union en étroite coopération avec l'ENISA;

f) coordonner la gestion des incidents majeurs;

g) jouer, pour les entités de l'Union, un rôle équivalent à celui de coordinateur désigné aux fins de la divulgation coordonnée des vulnérabilités conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555;

h) réaliser, à la demande d'une entité de l'Union, un scan proactif et non intrusif des réseaux et des systèmes d'information accessibles au public de ladite entité de l'Union.

Les informations visées au premier alinéa, point e), sont partagées avec l'IICB, le réseau des CSIRT et le Centre de situation et du renseignement de l'Union européenne (INTCEN), le cas échéant et selon le cas, et sont soumises à des conditions de confidentialité appropriées.

4. Le CERT-UE peut, conformément à l'article 17 ou à l'article 18 selon le cas, coopérer avec les communautés de cybersécurité pertinentes au sein de l'Union et de ses États membres, notamment dans les domaines suivants:

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

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

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

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

5. Dans la limite de ses compétences, le 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. Le CERT-UE peut coopérer et échanger des informations avec le Centre européen de lutte contre la cybercriminalité d'Europol.

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

a) des services soutenant la cybersécurité de l'environnement TIC des entités de l'Union, autres que ceux visés au paragraphe 3, sur la base d'accords de niveau de service et sous réserve des ressources disponibles, notamment une surveillance des réseaux à large spectre, y compris la surveillance 24 heures sur 24, 7 jours sur 7 de première ligne des cybermenaces d'une gravité élevée;

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

c) sur demande, un scan proactif des réseaux et des systèmes d'information de l'entité de l'Union concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important;

d) des services soutenant la sécurité de l'environnement TIC 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.

En ce qui concerne le premier alinéa, point d), le CERT-UE peut, à titre exceptionnel, conclure des accords de niveau de service avec des entités autres que les entités de l'Union, avec l'approbation préalable de l'IICB.

7. Le CERT-UE organise et peut 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.

8. Le CERT-UE peut fournir une assistance aux entités de l'Union en ce qui concerne les incidents survenant dans des réseaux et systèmes d'information traitant des ICUE s'il y est explicitement invité par les entités de l'Union concernées, conformément à leurs procédures respectives. La fourniture d'une assistance par le CERT-UE en vertu du présent paragraphe est sans préjudice des règles applicables en ce qui concerne la protection des informations classifiées.

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

10. Le CERT-UE fournit, avec un niveau de confidentialité et de fiabilité élevé, au moyen des mécanismes de coopération et des lignes hiérarchiques appropriées, des informations pertinentes et anonymisées sur les incidents majeurs et la façon dont ils ont été traités. Ces informations sont intégrées dans le rapport visé à l'article 10, paragraphe 14.

11. Pour traiter des incidents donnant lieu à des violations de données à caractère personnel, le CERT-UE, en coopération avec le CEPD, soutient les entités de l'Union concernées, sans préjudice de la compétence et des missions du CEPD en tant qu'autorité de contrôle au titre du règlement (UE) 2018/1725.

12. Le 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.

Article 14

Orientations, recommandations et injonctions

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

a) des injonctions décrivant les mesures de sécurité urgentes que les entités de l'Union sont instamment invitées à prendre dans un délai déterminé;

b) des propositions soumises à l'IICB concernant des orientations destinées 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.

En ce qui concerne le premier alinéa, point a), l'entité de l'Union concernée informe le CERT-UE, dans les meilleurs délais après avoir reçu l'injonction, de la manière dont les mesures de sécurité urgentes ont été appliquées.

2. Les orientations et les recommandations peuvent inclure:

a) des méthodes communes et un modèle d'évaluation de la maturité des entités de l'Union en matière de cybersécurité, y compris les barèmes ou les IPC correspondants, destinés à servir de référence pour soutenir l'amélioration continue de la cybersécurité dans toutes les entités de l'Union et à faciliter la hiérarchisation des domaines et des mesures de cybersécurité en tenant compte de la posture de cybersécurité des entités;

b) les modalités de la gestion des risques de cybersécurité et les mesures de gestion des risques en matière de cybersécurité, ou les améliorations à y apporter;

c) les modalités des évaluations du niveau de maturité en matière de cybersécurité et des plans de cybersécurité;

d) le cas échéant, l'utilisation d'une technologie, d'une architecture et de pratiques de sources ouvertes 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;

e) le cas échéant, des informations permettant de faciliter l'utilisation d'instruments d'acquisition conjointe pour l'acquisition de produits et services de cybersécurité pertinents auprès de prestataires tiers;

f) des modalités de partage d'informations conformément à l'article 20.

Article 15

Chef du CERT-UE

1. La Commission, après avoir obtenu l'approbation d'une majorité des deux tiers des membres de l'IICB, désigne le chef du CERT-UE. L'IICB est consulté à tous les stades de la procédure de désignation, notamment en ce qui concerne l'établissement des avis de vacance, l'examen des candidatures et la désignation des comités de sélection relatifs au poste. La procédure de sélection, y compris la liste restreinte finale des candidats à partir de laquelle le chef du CERT-UE sera désigné, garantit une représentation juste de chaque sexe en tenant compte des candidatures présentées.

2. Le chef du CERT-UE est responsable du bon fonctionnement de celui-ci et agit dans le cadre de ses attributions et sous la direction de l'IICB. Le chef du CERT-UE communique régulièrement des rapports au président de l'IICB et présente des rapports ponctuels à l'IICB à sa demande.

3. Le chef du 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 (UE, Euratom) 2018/1046 du Parlement européen et du Conseil ([9]), et rend régulièrement compte à l'ordonnateur délégué de la mise en œuvre des mesures pour lesquelles des pouvoirs ont été sous-délégués au chef du CERT-UE.

4. Le chef du CERT-UE établit chaque année une planification financière des recettes et dépenses administratives pour ses activités, une proposition de programme de travail annuel, une proposition de catalogue de services du CERT-UE, des propositions de révision du catalogue de services, une proposition de modalités des accords de niveau de service et une proposition d'IPC relatifs au CERT-UE en vue de leur approbation par l'IICB conformément à l'article 11. Lors de la révision de la liste des services figurant dans le catalogue de services du CERT-UE, le chef du CERT-UE tient compte des ressources allouées au CERT-UE.

5. Le chef du CERT-UE présente au moins une fois par an des rapports à l'IICB et au président de l'IICB sur les activités exercées et les résultats obtenus par le CERT-UE pendant la période de référence, notamment en ce qui concerne 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 11. Ces rapports comprennent un programme de travail pour la période suivante, la planification financière des recettes et des dépenses, y compris en matière d'effectifs, les mises à jour prévues du catalogue des services du CERT-UE et une évaluation de l'incidence attendue de ces mises à jour pour les ressources financières et humaines.

Article 16

Questions financières et de personnel

1. Le CERT-UE est intégré à la structure administrative d'une direction générale de la Commission afin de bénéficier des structures d'appui de la Commission en matière administrative, de gestion financière et de comptabilité tout en préservant son statut de fournisseur interinstitutionnel autonome de services destinés à l'ensemble des entités de l'Union. La Commission informe l'IICB du siège administratif du CERT-UE et de toute modification de celui-ci. La Commission procède régulièrement au réexamen des modalités administratives relatives au CERT-UE et, en tout état de cause, avant l'établissement de tout cadre financier pluriannuel conformément à l'article 312 du traité sur le fonctionnement de l'Union européenne, pour permettre l'adoption de mesures adéquates. Le réexamen prévoit la possibilité de faire du CERT-UE un organisme de l'Union.

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

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

3. Les tâches et activités du CERT-UE, y compris les services qu'il fournit, conformément à l'article 13, paragraphes 3, 4, 5 et 7, et à l'article 14, 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 au 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 du présent article versent une contribution financière annuelle au CERT-UE pour couvrir les services fournis par le CERT-UE en vertu dudit paragraphe 3. Les contributions sont fondées sur les orientations données par l'IICB et convenues entre chaque entité de l'Union et le CERT-UE dans les accords de niveau de service. Les contributions représentent une part équitable et proportionnée de l'ensemble des coûts des services fournis. Elles sont affectées à la ligne budgétaire distincte visée au paragraphe 3 du présent article en tant que recettes affectées internes comme prévu à l'article 21, paragraphe 3, point c), du règlement (UE, Euratom) 2018/1046.

5. Les coûts des services prévus à l'article 13, paragraphe 6, sont recouvrés auprès des entités de l'Union qui bénéficient des services du CERT-UE. Les recettes sont affectées aux lignes budgétaires dont relèvent les coûts.

Article 17

Coopération du CERT-UE avec les homologues des États membres

1. Le CERT-UE coopère et échange des informations dans les meilleurs délais avec les homologues des États membres, y compris les CSIRT désignés ou établis en vertu de l'article 10 de la directive (UE) 2022/2555 ou, le cas échéant, les autorités compétentes et les points de contact uniques désignés ou établis en vertu de l'article 8 de ladite directive, en ce qui concerne les incidents, les cybermenaces, les vulnérabilités, les incidents évités, les éventuelles contre-mesures et les bonnes pratiques et toutes les questions pertinentes pour améliorer la protection des environnements TIC des entités de l'Union, y compris par l'intermédiaire du réseau des CSIRT établi en vertu de l'article 15 de la directive (UE) 2022/2555. Le CERT-UE soutient la Commission au sein du réseau EU-CyCLONe établi en vertu de l'article 16 de la directive (UE) 2022/2555 pour ce qui est de la gestion coordonnée des incidents et crises de cybersécurité majeurs.

2. Lorsque le CERT-UE prend connaissance d'un incident important survenant sur le territoire d'un État membre, il avertit sans tarder tout homologue concerné dans ledit État membre conformément au paragraphe 1.

3. À condition que des données à caractère personnel soient protégées conformément au droit de l'Union applicable en matière de protection des données, le CERT-UE échange, sans retard inutile, des informations pertinentes propres à un incident avec les homologues des États membres afin de faciliter la détection de cybermenaces ou d'incidents similaires ou de contribuer à l'analyse d'un incident sans l'autorisation de l'entité de l'Union touchée. Le CERT-UE n'échange des informations propres à un incident qui révèlent l'identité de la cible de l'incident qu'en cas de survenance de l'un des événements suivants:

a) l'entité de l'Union touchée donne son consentement;

b) l'entité de l'Union touchée ne donne pas son consentement comme le prévoit le point a), mais la divulgation de l'identité de l'entité de l'Union touchée augmente la probabilité d'éviter ou d'atténuer d'autres incidents survenant par ailleurs;

c) l'entité de l'Union touchée a déjà fait savoir publiquement qu'elle a été touchée.

Les décisions d'échanger des informations propres à un incident qui révèlent l'identité de la cible de l'incident en vertu du premier alinéa, point b), sont approuvées par le chef du CERT-UE. Avant de prendre une telle décision, le CERT-UE contacte l'entité de l'Union touchée par écrit en expliquant précisément la façon dont la divulgation de son identité permettra d'éviter ou d'atténue d'autres incidents survenant par ailleurs. Le chef du CERT-UE fournit l'explication en demandant explicitement à l'entité de l'Union d'indiquer dans un délai déterminé si elle donne son consentement. Le chef du CERT-UE fait également savoir à l'entité de l'Union que, compte tenu de l'explication fournie, il se réserve le droit de divulguer l'information même sans son consentement. L'entité de l'Union touchée est informée avant la divulgation de l'information.

Article 18

Coopération du CERT-UE avec d'autres homologues

1. Le CERT-UE peut coopérer avec des homologues dans l'Union, autres que ceux visés à l'article 17, qui sont soumis aux exigences de l'Union en matière de cybersécurité, 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, le CERT-UE sollicite au préalable l'approbation de l'IICB au cas par cas. Lorsque le CERT-UE met en place une coopération avec de tels homologues, il informe tous les homologues des États membres concernés visés à l'article 17, paragraphe 1, dans l'État membre dans lequel l'homologue est situé. Le cas échéant et selon le cas, cette coopération et les conditions de celle-ci, y compris en ce qui concerne la cybersécurité, la protection des données et le traitement des informations, sont établis dans des modalités spécifiques de confidentialité tels que des contrats ou des arrangements administratifs. Les modalités de confidentialité ne nécessitent pas l'approbation préalable de l'IICB, mais le président de celui-ci en est informé. En cas de besoin urgent et imminent d'échanger des informations en matière de cybersécurité dans l'intérêt d'entités de l'Union ou d'une autre partie, le CERT-UE peut y procéder avec une entité dont la compétence, la capacité et l'expertise spécifiques sont indispensables à juste titre pour aider à répondre à ce besoin urgent et imminent, même si le CERT-UE ne dispose pas de modalités de confidentialité avec cette entité. Dans ce cas, le CERT-UE en informe immédiatement le président de l'IICB et fait rapport à l'IICB par l'intermédiaire de rapports réguliers ou de réunions.

2. Le CERT-UE peut coopérer avec d'autres partenaires, tels que des entités commerciales, y compris des entités de secteurs spécifiques de l'industrie, 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 incidents évités, des vulnérabilités et d'éventuelles contre-mesures. Pour pouvoir élargir la coopération avec ces partenaires, le CERT-UE sollicite au préalable l'approbation de l'IICB au cas par cas.

3. Le CERT-UE peut, avec le consentement de l'entité de l'Union touchée par un incident et à condition que des modalités ou un contrat de non-divulgation aient été conclus avec l'homologue ou le partenaire concerné, fournir des informations relatives à l'incident spécifique aux homologues ou partenaires visés aux paragraphes 1 et 2 à la seule fin de contribuer à son analyse.

CHAPITRE V

OBLIGATIONS EN MATIERE DE COOPERATION ET DE COMMUNICATION D'INFORMATIONS

Article 19

Traitement des informations

1. Les entités de l'Union et le CERT-UE 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. Le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil ([10]) s'applique aux demandes d'accès du public aux documents détenus par le CERT-UE, y compris l'obligation, prévue par ledit règlement, de consulter les autres entités de l'Union ou, le cas échéant, les États membres, dès lors qu'une demande concerne leurs documents.

3. Le traitement des informations par les entités de l'Union et le CERT-UE est conforme aux règles applicables en matière de sécurité de l'information.

([10]) Règlement (CE) n° 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).

Article 20

Modalités de partage d'informations en matière de cybersécurité

1. Les entités de l'Union peuvent volontairement faire part au CERT-UE des incidents, cybermenaces, incidents évités et vulnérabilités qui les touchent et lui transmettre des informations à leur propos. Le CERT-UE veille à ce que des moyens de communication efficaces, avec un niveau de traçabilité, de confidentialité et de fiabilité élevé, soient disponibles pour faciliter le partage d'informations avec les entités de l'Union. Lors du traitement des notifications, le CERT-UE peut traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Sans préjudice de l'article 12, une notification volontaire n'a pas pour effet d'imposer à l'entité de l'Union qui en est à l'origine des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis ladite notification.

2. Afin d'accomplir sa mission et les tâches qui lui sont confiées en vertu de l'article 13, le CERT-UE peut demander aux entités de l'Union de lui fournir des informations à partir de leurs inventaires respectifs des systèmes TIC, notamment des informations relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, aux indicateurs de compromission et aux alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les incidents. L'entité de l'Union requise transmet les informations demandées, ainsi que toute mise à jour ultérieure de celles-ci, dans les meilleurs délais.

3. Le CERT-UE peut échanger avec les entités de l'Union des informations propres à un incident qui révèlent l'identité de l'entité de l'Union touchée par cet incident sous réserve du consentement de l'entité de l'Union touchée. Lorsqu'une entité de l'Union n'accorde pas son consentement, elle fournit au CERT-UE les motifs de cette décision.

4. Les entités de l'Union partagent avec le Parlement européen et le Conseil, à leur demande, des informations sur l'achèvement des plans de cybersécurité.

5. L'IICB ou le CERT-UE, selon le cas, partage les orientations, les recommandations et les injonctions avec le Parlement européen et le Conseil, à leur demande.

6. Les obligations en matière de partage énoncées au présent article ne s'étendent pas:

a) aux ICUE;

b) aux informations dont la distribution ultérieure a été exclue au moyen d'un marquage visible, à moins que le partage de celles-ci avec le CERT-UE ait été explicitement autorisé.

Article 21

Obligations d'information

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 concernée ou des pertes financières pour celle-ci;

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

2. Les entités de l'Union transmettent au CERT-UE:

a) sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance de l'incident important, une alerte précoce qui, le cas échéant, indique que l'on suspecte l'incident important d'avoir été causé par des actes illicites ou malveillants ou qu'il pourrait avoir un impact inter-entités ou transfrontière;

b) sans retard injustifié et en tout état de cause 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, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles;

c) à la demande du 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 visée au point b), comprenant les éléments suivants:

i) une description détaillée de l'incident, y compris de sa gravité et de son impact;

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

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

iv) le cas échéant, l'impact transfrontière ou inter-entités de l'incident;

e) en cas d'incident 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 à compter du traitement de l'incident.

3. Une entité de l'Union informe, sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance d'un incident important, tous les homologues des États membres concernés visés à l'article 17, paragraphe 1, dans l'État membre dans lequel il est situé qu'un incident important est survenu.

4. Les entités de l'Union notifient, entre autres, toute information qui permet au CERT-UE de déterminer tout impact inter-entités, tout impact pour l'État membre hôte ou tout impact transfrontière de l'incident important. Sans préjudice de l'article 12, le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité de l'Union.

5. Le cas échéant, les entités de l'Union communiquent sans retard injustifié aux utilisateurs des réseaux et des systèmes d'information touchés, ou d'autres composants de l'environnement TIC, qui sont potentiellement touchés par un incident important ou une cybermenace importante et qui, le cas échéant, doivent prendre des mesures d'atténuation, toutes les mesures ou corrections qu'ils peuvent appliquer en réponse à cet incident ou à cette menace. Le cas échéant, les entités de l'Union informent ces utilisateurs de la cybermenace importante elle-même.

6. Lorsqu'un incident important ou une cybermenace importante touche un réseau et un système d'information, ou un composant de l'environnement TIC d'une entité de l'Union qui est réputé être connecté à l'environnement TIC d'une autre entité de l'Union, le CERT-UE émet une alerte de cybersécurité.

7. Les entités de l'Union fournissent au CERT-UE, à sa demande et dans les meilleurs délais, les informations numériques générées par l'utilisation de dispositifs électroniques impliqués dans les incidents qui les ont respectivement touchés. Le CERT-UE peut fournir davantage de détails sur les types d'informations dont il a besoin pour la conscience situationnelle et la réaction aux incidents.

8. Le CERT-UE soumet tous les trois mois à l'IICB, à l'ENISA, à l'INTCEN et au réseau des CSIRT un rapport de synthèse contenant des données anonymisées et agrégées sur les incidents importants, les incidents, les cybermenaces, les incidents évités et les vulnérabilités conformément à l'article 20 et sur les incidents importants qui ont été notifiés conformément au paragraphe 2 du présent article. Le rapport de synthèse constitue une contribution au rapport bisannuel sur l'état de la cybersécurité dans l'Union adopté en vertu de l'article 18 de la directive (UE) 2022/2555.

9. Au plus tard le 8 juillet 2024, l'IICB élabore des orientations ou des recommandations précisant davantage les modalités, le format et le contenu du rapport conformément au présent article. Lors de la préparation de ces orientations ou de ces recommandations, l'IICB tient compte de tout acte d'exécution adopté en vertu de l'article 23, paragraphe 11, de la directive (UE) 2022/2555 en vue de préciser le type d'informations, le format et la procédure des notifications. Le 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.

10. Les obligations d'information énoncées au présent article ne s'étendent pas:

a) aux ICUE;

b) aux informations dont la distribution ultérieure a été exclue au moyen d'un marquage visible, à moins que le partage de celles-ci avec le CERT-UE ait été explicitement autorisé.

Article 22

Coordination de la réaction aux incidents et coopération

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

a) les entités de l'Union;

b) les homologues visés aux articles 17 et 18.

2. Le CERT-UE, le cas échéant en étroite coopération avec l'ENISA, 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;

b) soutien mutuel, comme le partage d'informations pertinentes avec les entités de l'Union, ou fourniture d'une assistance, le cas échéant directement sur site;

c) utilisation optimale des ressources opérationnelles;

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

3. Le CERT-UE, en étroite coopération avec l'ENISA, soutient les entités de l'Union en ce qui concerne la conscience situationnelle des incidents, des cybermenaces, des vulnérabilités et des incidents évités ainsi qu'en ce qui concerne le partage des évolutions pertinentes dans le domaine de la cybersécurité.

4. Au plus tard le 8 janvier 2025, sur la base d'une proposition du CERT-UE, l'IICB adopte des orientations ou des 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, le CERT-UE conseille sur la manière de signaler l'incident aux autorités répressives sans retard injustifié.

5. À la demande spécifique d'un État membre et moyennant l'approbation des entités de l'Union concernées, le CERT-UE peut inviter des experts figurant sur la liste visée à l'article 23, paragraphe 4, à contribuer à la réaction à un incident majeur qui a un impact dans cet État membre ou à un incident de cybersécurité majeur conformément à l'article 15, paragraphe 3, point g), de la directive (UE) 2022/2555. Des règles spécifiques relatives à l'accès et au recours à des experts techniques issus des entités de l'Union sont approuvées par l'IICB sur la base d'une proposition du CERT-UE.

Article 23

Gestion des incidents majeurs

1. Afin de soutenir au niveau opérationnel la gestion coordonnée des incidents majeurs 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 définit, conformément à l'article 11, point q), un plan de gestion des crises de cybersécurité sur la base des activités visées à l'article 22, paragraphe 2, en étroite coopération avec le CERT-UE et l'ENISA. Le plan de gestion des crises de cybersécurité 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.

2. Sous réserve du plan de gestion des crises de cybersécurité défini en vertu du paragraphe 1 du présent article et sans préjudice de l'article 16, paragraphe 2, premier alinéa, de la directive (UE) 2022/2555, le représentant de la Commission à l'IICB fait office de point de contact pour le partage des informations pertinentes relatives aux incidents majeurs avec EU-CyCLONe.

3. Le CERT-UE coordonne la gestion des incidents majeurs entre les entités de l'Union. Il tient à jour un inventaire de l'expertise technique disponible qui serait nécessaire pour réagir aux incidents en cas d'incidents majeurs et assiste l'IICB dans la coordination des plans de gestion des crises de cybersécurité des entités de l'Union en cas d'incidents majeurs visés à l'article 9, paragraphe 2.

4. 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.

CHAPITRE VI

DISPOSITIONS FINALES

Article 24

Réaffectation budgétaire initiale

Afin d'assurer un fonctionnement adapté et stable du CERT-UE, la Commission peut proposer la réaffectation de personnel et de ressources financières vers le budget de la Commission à destination des activités du CERT-UE. La réaffectation prend effet à la même date que le premier budget annuel de l'Union adopté après l'entrée en vigueur du présent règlement.

Article 25

Réexamen

1. Au plus tard le 8 janvier 2025, puis sur une base annuelle, l'IICB, avec l'aide du CERT-UE, fait rapport à la Commission sur la mise en œuvre du présent règlement. L'IICB peut adresser des recommandations à la Commission en vue de réexaminer le présent règlement.

2. Au plus tard le 8 janvier 2027, puis tous les deux ans, la Commission évalue et fait rapport au Parlement européen et au Conseil sur la mise en œuvre du présent règlement et sur l'expérience acquise au niveau stratégique et opérationnel.

Le rapport visé au premier alinéa du présent paragraphe comprend le réexamen visé à l'article 16, paragraphe 1, relatif à la possibilité de faire du CERT-UE un organisme de l'Union.

3. Au plus tard le 8 janvier 2029, 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. La Commission évalue également l'opportunité d'inclure les réseaux et systèmes d'information traitant des ICUE dans le champ d'application du présent règlement, en tenant compte des autres actes législatifs de l'Union applicables à ces systèmes. Le rapport est accompagné au besoin d'une proposition législative.

Article 26

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 Strasbourg, le 13 décembre 2023.

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
R. METSOLA	P. NAVARRO RÍOS