Journal officiel
de l'Union européenne

FR
Série L

2024/1366

24.5.2024

RÈGLEMENT DÉLÉGUÉ (UE) 2024/1366 DE LA COMMISSION

du 11 mars 2024

complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil en établissant un code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité

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

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité ([1]), et notamment son article 59, paragraphe 2, point e),

considérant ce qui suit:

(1) La gestion des risques de cybersécurité est essentielle pour maintenir la sécurité de l'approvisionnement en électricité et garantir un niveau élevé de cybersécurité dans le secteur de l'électricité.

(2) La numérisation et la cybersécurité sont décisives pour fournir des services essentiels et revêtent donc une importance stratégique pour les infrastructures énergétiques critiques.

(3) La directive (UE) 2022/2555 du Parlement européen et du Conseil ([2]) définit des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. Le règlement (UE) 2019/941 du Parlement européen et du Conseil ([3]) complète la directive (UE) 2022/2555 en veillant à ce que les incidents de cybersécurité dans le secteur de l'électricité soient correctement identifiés comme un risque et à ce que les mesures prises pour y remédier soient dûment prises en compte dans les plans de préparation aux risques. Le règlement (UE) 2019/943 complète la directive (UE) 2022/2555 et le règlement (UE) 2019/941 en établissant des règles spécifiques pour le secteur de l'électricité au niveau de l'Union. En outre, le présent règlement délégué complète les dispositions de la directive (UE) 2022/2555 en ce qui concerne le secteur de l'électricité, chaque fois que des flux transfrontaliers d'électricité sont concernés.

(4) Dans un contexte de systèmes d'électricité numérisés interconnectés, la prévention et la gestion des crises électriques liées aux cyberattaques ne peuvent être considérées comme constituant une tâche exclusivement nationale. Il convient de développer pleinement le potentiel de mesures plus efficaces et moins coûteuses grâce à la coopération aux niveaux régional et de l'Union. Dès lors, un cadre commun de règles et des procédures mieux coordonnées sont nécessaires pour que les États membres et les autres acteurs soient en mesure de coopérer efficacement par-delà les frontières dans un esprit de transparence, de confiance et de solidarité accrues entre les États membres et les autorités compétentes chargées de l'électricité et de la cybersécurité.

(5) La gestion des risques de cybersécurité relevant du champ d'application du présent règlement nécessite un processus structuré comprenant, entre autres, l'identification des risques pour les flux transfrontaliers d'électricité découlant des cyberattaques, les processus opérationnels et périmètres connexes, les contrôles de cybersécurité et les mécanismes de vérification correspondants. Si le calendrier de l'ensemble du processus est réparti sur plusieurs années, chaque étape de ce processus devrait contribuer à un niveau commun élevé de cybersécurité dans le secteur et à l'atténuation des risques de cybersécurité. Tous les participants au processus devraient faire tout leur possible pour élaborer et convenir des méthodes dès que possible, sans retard et, en tout état de cause, au plus tard dans les délais fixés dans le présent règlement.

([1]) JO L 158 du 14.6.2019, p. 54.

([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).

([3]) Règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin 2019 sur la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE (JO L 158 du 14.6.2019, p. 1).

(6) Les évaluations des risques de cybersécurité au niveau de l'Union, des États membres, des régions et des entités prévues par le présent règlement peuvent être limitées à celles résultant de cyberattaques telles que définies dans le règlement (UE) 2022/2554 du Parlement européen et du Conseil ([4]), en excluant donc, par exemple, les attaques physiques, les catastrophes naturelles et les indisponibilités dues à la perte d'installations ou de ressources humaines. Les risques régionaux et à l'échelle de l'Union liés aux attaques physiques ou aux catastrophes naturelles dans le domaine de l'électricité sont déjà couverts par d'autres actes législatifs de l'Union, notamment l'article 5 du règlement (UE) 2019/941, ou le règlement (UE) 2017/1485 de la Commission ([5]) établissant une ligne directrice sur la gestion du réseau de transport de l'électricité. De même, la directive (UE) 2022/2557 du Parlement européen et du Conseil ([6]) sur la résilience des entités critiques vise à réduire les vulnérabilités et à renforcer la résilience physique des entités critiques et couvre tous les risques naturels et d'origine humaine pertinents susceptibles d'affecter la fourniture de services essentiels, y compris les accidents, les catastrophes naturelles, les urgences de santé publique telles que les pandémies, les menaces hybrides ou d'autres menaces antagonistes, y compris les infractions terroristes, l'infiltration criminelle et le sabotage.

(7) La notion d'«entités à fort impact ou à impact critique» figurant dans le présent règlement est fondamentale pour définir le champ d'application des entités qui seront soumises aux obligations décrites dans le présent règlement. L'approche fondée sur les risques décrite dans les différentes dispositions vise à recenser les processus, les ressources d'appui et les entités qui les exploitent qui ont un impact sur les flux transfrontaliers d'électricité. En fonction du degré d'impact d'éventuelles cyberattaques sur leurs opérations de flux transfrontaliers d'électricité, ces entités peuvent être considérées comme «à fort impact» ou «à impact critique». L'article 3 de la directive (UE) 2022/2555 définit les notions d'entités essentielles et importantes ainsi que les critères permettant d'identifier les entités appartenant à ces catégories. Bon nombre d'entre elles seront considérées et identifiées simultanément comme «essentielles» au sens de l'article 3 de la directive (UE) 2022/2555 et comme à fort impact ou à impact critique conformément à l'article 24 du présent règlement, mais les critères établis dans le présent règlement se réfèrent uniquement à leur rôle et à leur impact dans les processus en matière d'électricité ayant une incidence sur les flux transfrontaliers, sans tenir compte des critères définis à l'article 3 de la directive (UE) 2022/2555.

(8) Les entités relevant du champ d'application du présent règlement, considérées à fort impact ou à impact critique conformément à l'article 24 du présent règlement et soumises aux obligations qui y sont énoncées, sont principalement celles qui ont un impact direct sur les flux transfrontaliers d'électricité dans l'Union.

(9) Le présent règlement utilise les mécanismes et instruments existants, déjà établis dans d'autres législations, afin de garantir l'efficacité et d'éviter les doubles emplois dans la réalisation des objectifs.

(10) Lorsqu'ils appliquent le présent règlement, les États membres, les autorités compétentes et les gestionnaires de réseau devraient tenir compte des normes et spécifications techniques européennes convenues des organisations européennes de normalisation et agir conformément à la législation de l'Union relative à la mise sur le marché ou à la mise en service de produits couverts par cette législation de l'Union.

([4]) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).

([5]) Règlement (UE) 2017/1485 de la Commission du 2 août 2017 établissant une ligne directrice sur la gestion du réseau de transport de l'électricité (JO L 220 du 25.8.2017, p. 1).

([6]) Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164).

(11) En vue d'atténuer les risques de cybersécurité, il est nécessaire d'établir un corpus réglementaire détaillé régissant les actions et la coopération entre les parties prenantes concernées, dont les activités concernent les aspects liés à la cybersécurité des flux transfrontaliers d'électricité, dans le but de garantir la sécurité du système. Ces règles organisationnelles et techniques devraient garantir que la plupart des incidents liés à l'électricité ayant des causes profondes liées à la cybersécurité soient traités de manière efficace au niveau opérationnel. Il est nécessaire de préciser ce que les États membres devraient faire pour prévenir de telles crises et les mesures qu'ils peuvent prendre dans l'hypothèse où les règles d'exploitation du système ne seraient plus suffisantes. Dès lors, il y a lieu d'établir un cadre commun de règles sur la manière de prévenir, de préparer et de gérer les crises électriques simultanées ayant une cause profonde liée à la cybersécurité. Cela renforce la transparence dans la phase de préparation et au cours d'une crise de l'électricité simultanée et garantit que des mesures sont prises de manière coordonnée et efficace avec les autorités compétentes en matière de cybersécurité dans les États membres. Les États membres et les entités concernées devraient être tenus de coopérer, au niveau régional et, s'il y a lieu, de manière bilatérale, dans un esprit de solidarité. Cette coopération et ces règles visent à améliorer la préparation aux risques de cybersécurité à moindre coût, également en conformité aux objectifs de la directive (UE) 2022/2555. Il semble en outre nécessaire de renforcer le marché intérieur de l'électricité en renforçant la confiance entre les États membres, en particulier en atténuant le risque de réduction indue des flux transfrontaliers d'électricité, réduisant ainsi le risque d'effets de contagion négatifs sur les États membres voisins.

(12) La sécurité d'approvisionnement en électricité implique une coopération efficace entre les États membres, les institutions, organes et organismes de l'Union, et les parties prenantes concernées. Les gestionnaires de réseau de distribution et les gestionnaires de réseau de transport jouent un rôle clé pour garantir un système électrique sûr, fiable et efficace conformément aux articles 31 et 40 de la directive (UE) 2019/944 du Parlement européen et du Conseil ([7]). Les diverses autorités de régulation et les autres autorités nationales compétentes jouent également un rôle important pour garantir et surveiller la cybersécurité dans l'approvisionnement en électricité, dans le cadre des missions dont elles sont investies par les directives (UE) 2019/944 et (UE) 2022/2555. Les États membres devraient désigner une entité existante ou nouvelle en tant qu'autorité nationale compétente pour la mise en œuvre du présent règlement, dans le but de garantir la participation transparente et inclusive de tous les acteurs concernés, la préparation efficace et la bonne mise en œuvre dudit règlement, la coopération entre les différentes parties prenantes concernées et les autorités compétentes dans les domaines de l'électricité et de la cybersécurité, ainsi que de faciliter la prévention et l'évaluation ex post des crises électriques ayant des causes profondes liées à la cybersécurité et les échanges d'informations y afférents.

(13) Lorsqu'une entité à fort impact ou à impact critique fournit des services dans plus d'un État membre, a son siège ou un autre établissement ou un représentant dans un État membre, mais que son réseau et ses systèmes d'information sont situés dans un ou plusieurs autres États membres, ces États membres devraient encourager leurs autorités compétentes respectives à tout mettre en œuvre pour coopérer et se prêter mutuellement assistance si nécessaire.

(14) Les États membres devraient veiller à ce que les autorités compétentes disposent des pouvoirs nécessaires, en ce qui concerne les entités à fort impact et à impact critique, pour promouvoir le respect du présent règlement. Ces pouvoirs devraient permettre aux autorités compétentes d'effectuer des inspections sur place et une surveillance hors site. Cela peut inclure des contrôles aléatoires, la réalisation d'audits réguliers, des audits de sécurité ciblés fondés sur des évaluations des risques ou des informations disponibles liées aux risques et des analyses de sécurité fondées sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, et incluant les demandes d'informations nécessaires pour évaluer les mesures de cybersécurité adoptées par l'entité. Ces informations devraient comprendre des politiques de cybersécurité documentées, des données d'accès, des documents ou toute information nécessaire à l'accomplissement de leurs missions de surveillance, ainsi que des preuves de la mise en œuvre des politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

([7]) Directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE (JO L 158 du 14.6.2019, p. 125).

(15) Afin d'éviter les lacunes ou les doubles emplois en ce qui concerne les obligations en matière de gestion des risques de cybersécurité imposées aux entités à fort impact et à impact critique, les autorités nationales au sens de la directive (UE) 2022/2555 et les autorités compétentes au sens du présent règlement devraient coopérer pour la mise en œuvre des mesures de gestion des risques de cybersécurité et la surveillance du respect de ces mesures au niveau national. La conformité d'une entité avec les exigences en matière de gestion des risques de cybersécurité énoncées dans le présent règlement pourrait être considérée par les autorités compétentes au sens de la directive (UE) 2022/2555 comme garantissant le respect des exigences correspondantes énoncées dans ladite directive, ou vice versa.

(16) Une approche commune de la prévention et de la gestion simultanées des crises électriques nécessite une compréhension commune entre les États membres de ce qui constitue une crise électrique simultanée et d'à quel moment une cyberattaque en est un facteur important. En particulier, la coordination entre les États membres et les entités concernées devrait être facilitée afin de remédier à une situation dans laquelle le risque potentiel de pénurie significative d'électricité ou d'impossibilité de fournir de l'électricité aux clients est présent ou imminent, et ce en raison d'une cyberattaque.

(17) Le considérant 1 du règlement (UE) 2019/881 du Parlement européen et du Conseil ([8]) reconnaît le rôle essentiel des réseaux et des systèmes d'information ainsi que des réseaux et services de communications électroniques pour maintenir le fonctionnement de l'économie dans des secteurs clés tels que l'énergie, tandis que le considérant 44 explique que l'Agence de l'Union européenne pour la cybersécurité (ENISA) devrait se concerter avec l'Agence de l'Union européenne pour la coopération des régulateurs de l'énergie (ci-après l'«ACER»).

(18) Le règlement (UE) 2019/943 attribue des responsabilités spécifiques en matière de cybersécurité aux gestionnaires de réseau de transport (GRT) et aux gestionnaires de réseau de distribution (GRD). Leurs associations européennes, à savoir le réseau européen des GRT pour l'électricité («REGRT pour l'électricité») et l'entité européenne pour les GRD (ci-après l'«entité des GRD de l'Union»), conformément, respectivement, aux articles 30 et 55 dudit règlement, promeuvent la cybersécurité en coopération avec les autorités compétentes et les entités réglementées.

(19) Une approche commune de la prévention et de la gestion des crises électriques simultanées ayant des causes profondes liées à la cybersécurité exige également que toutes les parties prenantes concernées utilisent des méthodes et des définitions harmonisées pour recenser les risques liés à la cybersécurité de l'approvisionnement en électricité. Elles doivent également d'être en mesure de comparer efficacement leurs performances dans ce domaine et celles de leurs voisins. Par conséquent, il est nécessaire d'établir les processus, les rôles et les responsabilités pour élaborer et mettre à jour des méthodes de gestion des risques, des échelles de classification des incidents et des mesures de cybersécurité adaptées aux risques de cybersécurité ayant un impact sur les flux transfrontaliers d'électricité.

(20) Les États membres, par l'intermédiaire de l'autorité compétente désignée aux fins du présent règlement, sont chargés d'identifier les entités qui remplissent les critères pour être considérées comme des entités à fort impact ou à impact critique. Afin d'éliminer les divergences importantes entre les États membres à cet égard et de garantir la sécurité juridique concernant les mesures de gestion des risques de cybersécurité et les obligations d'information pour toutes les entités concernées, il convient d'établir un ensemble de critères déterminant quelles entités relèvent du champ d'application du présent règlement. Cet ensemble de critères devrait être défini et régulièrement mis à jour dans le cadre du processus d'élaboration et d'adoption des modalités, conditions et méthodes définies dans le présent règlement.

(21) Les dispositions du présent règlement devraient être sans préjudice du droit de l'Union prévoyant des règles spécifiques relatives à la certification des produits des technologies de l'information et de la communication (TIC), des services TIC et des processus TIC, et plus particulièrement sans préjudice du règlement (UE) 2019/881 en ce qui concerne le cadre pour l'établissement de schémas européens de certification en matière de cybersécurité. Dans le contexte du présent règlement, les produits TIC devraient également inclure les dispositifs techniques et les logiciels qui permettent une interaction directe avec le réseau électrotechnique, en particulier les systèmes de contrôle industriel pouvant être utilisés pour le transport, la distribution et la production d'énergie, ainsi que pour la collecte et la transmission d'informations connexes. Les dispositions devraient garantir que les objectifs de sécurité pertinents énoncés à l'article 51 du règlement (UE) 2019/881 sont atteints par les produits TIC, services TIC et processus TIC à acquérir.

([8]) 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).

(22) Les récentes cyberattaques montrent que les entités sont de plus en plus la cible d'attaques au niveau de la chaîne d'approvisionnement. Ces attaques sur la chaîne d'approvisionnement ont non seulement un impact sur des entités individuelles relevant du champ d'application, mais peuvent également avoir un effet en cascade sur des attaques de plus grande ampleur contre des entités auxquelles elles sont connectées dans le réseau électrique. Des dispositions et des recommandations visant à contribuer à atténuer les risques de cybersécurité associés aux processus liés à la chaîne d'approvisionnement, notamment les marchés publics, ayant un impact sur les flux transfrontaliers d'électricité ont donc été ajoutées.

(23) Étant donné que l'exploitation des vulnérabilités des réseaux et des systèmes d'information peut causer des perturbations de l'approvisionnement en énergie et des dommages importants pour l'économie et les consommateurs, il convient de les recenser rapidement et d'y remédier afin de réduire les risques. Afin de faciliter la mise en œuvre effective du présent règlement, les entités concernées et les autorités compétentes devraient coopérer pour exercer et tester des activités jugées appropriées à cette fin, y compris l'échange d'informations sur les cybermenaces, les cyberattaques, les vulnérabilités, les outils et méthodes, les tactiques, les techniques et procédures, la préparation à la gestion des crises de cybersécurité et d'autres exercices. Étant donné que la technologie évolue constamment et que la numérisation du secteur de l'électricité progresse rapidement, la mise en œuvre des dispositions adoptées ne devrait pas nuire à l'innovation et ne pas constituer un obstacle à l'accès au marché de l'électricité ni à l'utilisation ultérieure de solutions innovantes qui contribuent à l'efficacité et à la durabilité du système électrique.

(24) Les informations recueillies en vue du suivi de la mise en œuvre du présent règlement devraient être raisonnablement limitées selon le principe du besoin d'en connaître. Les parties prenantes devraient se voir accorder des délais réalisables et effectifs pour la présentation de ces informations. Il convient d'éviter une double notification.

(25) La protection en matière de cybersécurité ne s'arrête pas aux frontières de l'Union. Un système sécurisé nécessite la participation des pays tiers voisins. L'Union et ses États membres devraient s'efforcer d'aider les pays tiers voisins dont les infrastructures électriques sont connectées au réseau européen à appliquer des règles de cybersécurité similaires à celles énoncées dans le présent règlement.

(26) Afin d'améliorer rapidement la coordination en matière de sécurité et de tester les futures modalités, conditions et méthodes contraignantes, le REGRT pour l'électricité, l'entité des GRD de l'Union et les autorités compétentes devraient commencer à élaborer des orientations non contraignantes immédiatement après l'entrée en vigueur du présent règlement. Ces orientations serviront de référence pour l'élaboration des modalités, conditions et méthodes futures. Parallèlement, les autorités compétentes devraient recenser les entités susceptibles d'être classées à fort impact ou à impact critique afin qu'elles commencent, sur une base volontaire, à s'acquitter de leurs obligations.

(27) Le présent règlement a été élaboré en étroite coopération avec l'ACER, l'ENISA, le REGRT pour l'électricité, l'entité des GRD de l'Union et d'autres parties prenantes, afin d'adopter des règles efficaces, équilibrées et proportionnées de manière transparente et participative.

(28) Le présent règlement complète et renforce les mesures de gestion de crise établies dans le cadre de l'Union pour la réaction aux crises de cybersécurité, conformément à la recommandation (UE) 2017/1584 de la Commission ([9]). Une cyberattaque pourrait causer une crise électrique, telle que définie à l'article 2, point 9), du règlement (UE) 2019/941, contribuer à cette crise ou coïncider avec elle, avec un impact sur les flux transfrontaliers d'électricité. Cette crise électrique pourrait entraîner une crise électrique simultanée au sens de l'article 2, point 10), du règlement (UE) 2019/941. Un tel incident pourrait également avoir un impact sur d'autres secteurs dépendant de la sécurité de l'approvisionnement en électricité. Si un tel incident devait déboucher sur un incident de cybersécurité majeur au sens de l'article 16 de la directive (UE) 2022/2555, les dispositions dudit article établissant le réseau européen d'organisations de liaison en cas de crise de cybersécurité («EU-CyCLONe») devraient s'appliquer. Pour la gestion des crises au niveau de l'Union, les parties concernées devraient s'appuyer sur le dispositif intégré de l'Union pour une réaction au niveau politique dans les situations de crise instauré par la décision d'exécution (UE) 2018/1993 du Conseil ([10]) (ci-après dénommé «dispositif IPCR»).

(29) Le présent règlement ne porte pas atteinte à la compétence des États membres pour l'adoption des mesures nécessaires en vue de garantir la protection des intérêts essentiels de sa sécurité, d'assurer l'action publique et la sécurité publique et de permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Conformément à l'article 346 du TFUE, aucun État membre n'est tenu de fournir des renseignements dont il considère la divulgation contraire aux intérêts essentiels de sa sécurité.

([9]) 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).

([10]) Décision d'exécution (UE) 2018/1993 du Conseil du 11 décembre 2018 concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (JO L 320 du 17.12.2018, p. 28).

(30) Bien que le présent règlement s'applique, en principe, aux entités exerçant des activités de production d'électricité à partir de centrales nucléaires, certaines de ces activités peuvent être liées à la sécurité nationale.

(31) Le droit de l'Union en matière de protection des données et en matière de protection de la vie privée devrait s'appliquer à tout traitement de données à caractère personnel au titre du présent règlement. En particulier, le présent règlement est sans préjudice du règlement (UE) 2016/679 du Parlement européen et du Conseil ([11]), de la directive 2002/58/CE du Parlement européen et du Conseil ([12]) et du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([13]). Le présent règlement ne devrait donc pas porter atteinte, entre autres, aux tâches ni aux compétences des autorités compétentes pour contrôler le respect du droit de l'Union applicable en matière de protection des données et de protection de la vie privée.

(32) Compte tenu de l'importance de la coopération internationale en matière de cybersécurité, les autorités compétentes qui sont chargées d'exécuter les tâches que leur assigne le présent règlement et qui sont désignées par les États membres devraient pouvoir participer aux réseaux de coopération internationale. Par conséquent, aux fins de l'accomplissement de leurs tâches, les autorités compétentes devraient pouvoir échanger des informations, y compris des données à caractère personnel, avec les autorités compétentes de pays tiers, pour autant que les conditions prévues par le droit de l'Union en matière de protection des données pour les transferts de données à caractère personnel vers des pays tiers, entre autres celles de l'article 49 du règlement (UE) 2016/679, soient remplies.

(33) Le traitement de données à caractère personnel, dans la mesure nécessaire et proportionnée aux fins de garantir la sécurité des actifs, par des entités à fort impact ou à impact critique, pourrait être considéré comme licite au motif qu'il respecte une obligation légale à laquelle le responsable du traitement est soumis, conformément aux exigences de l'article 6, paragraphe 1, point c), et de l'article 6, paragraphe 3, du règlement (UE) 2016/679. Le traitement des données à caractère personnel peut également être nécessaire à des intérêts légitimes poursuivis par des entités à fort impact ou à impact critique, ainsi que par des fournisseurs de technologies et de services de sécurité agissant pour le compte de ces entités, conformément à l'article 6, paragraphe 1, point f), du règlement (UE) 2016/679, y compris lorsque ce traitement est nécessaire à des accords de partage d'informations en matière de cybersécurité ou à la notification volontaire d'informations pertinentes conformément au présent règlement. Les mesures liées à la prévention, à la détection, à l'identification, à l'endiguement, à l'analyse des cyberattaques et à la réaction à celles-ci, les mesures de sensibilisation à des cybermenaces spécifiques, l'échange d'informations dans le cadre de la correction des vulnérabilités et de la divulgation coordonnée des vulnérabilités, l'échange volontaire d'informations sur ces cyberattaques ainsi que sur les cybermenaces et les vulnérabilités, les indicateurs de compromis, les tactiques, techniques et procédures, les alertes de cybersécurité et les outils de configuration peuvent nécessiter le traitement de certaines catégories de données à caractère personnel, telles que les adresses IP, les localisateurs de ressources uniformes (URL), les noms de domaine, les adresses électroniques et, lorsqu'ils révèlent des données à caractère personnel, les horodatages. Le traitement des données à caractère personnel par les autorités compétentes, les points de contact uniques et les CSIRT peut constituer une obligation légale ou être considéré comme nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement en vertu de l'article 6, paragraphe 1, point c) ou e), et de l'article 6, paragraphe 3, du règlement (UE) 2016/679, ou à la poursuite d'un intérêt légitime des entités à fort impact ou à impact critique comme visé à l'article 6, paragraphe 1, point f), dudit règlement. En outre, le droit national peut établir des règles permettant aux autorités compétentes, aux points de contact uniques et aux CSIRT, dans la mesure nécessaire et proportionnée aux fins d'assurer la sécurité des réseaux et des systèmes d'information des entités à fort impact ou à impact critique, de traiter des catégories particulières de données à caractère personnel conformément à l'article 9 du règlement (UE) 2016/679, notamment en prévoyant des mesures appropriées et spécifiques pour protéger les droits fondamentaux et les intérêts des personnes physiques, y compris des limitations techniques à la réutilisation de ces données et le recours aux mesures de sécurité et de protection de la vie privée les plus récentes, telles que la pseudonymisation, ou le chiffrement lorsque l'anonymisation peut avoir un effet important sur la finalité poursuivie.

([11]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([12]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

([13]) 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) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

(34) Dans de nombreux cas, des données à caractère personnel sont compromises à la suite de cyberattaques. Dans de telles circonstances, les autorités compétentes devraient coopérer et échanger des informations sur tous les aspects pertinents avec les autorités visées dans le règlement (UE) 2016/679 et la directive 2002/58/CE.

(35) 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 novembre 2023,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

Le présent règlement établit un code de réseau qui fixe des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité, y compris des règles sur les exigences minimales communes, la planification, la surveillance, les rapports et la gestion de crise.

Article 2

Champ d'application

1. Le présent règlement s'applique aux aspects liés à la cybersécurité des flux transfrontaliers d'électricité dans le cadre des activités des entités suivantes, si elles sont identifiées comme des entités à fort impact ou à impact critique conformément à l'article 24:

a) les entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944;

b) les opérateurs désignés du marché de l'électricité (NEMO) au sens de l'article 2, point 8), du règlement (UE) 2019/943;

c) les places de marché organisées ou les «marchés organisés», tels que définis à l'article 2, point 4), du règlement d'exécution (UE) nº 1348/2014 de la Commission ([14]), qui organisent des transactions sur des produits pertinents pour les flux transfrontaliers d'électricité;

d) les prestataires critiques de services TIC définis à l'article 3, point 9), du présent règlement;

e) le REGRT pour l'électricité établi conformément à l'article 28 du règlement (UE) 2019/943;

f) l'entité des GRD de l'Union établie conformément à l'article 52 du règlement (UE) 2019/943;

g) les responsables d'équilibre au sens de l'article 2, point 14), du règlement (UE) 2019/943;

h) les exploitants de points de recharge au sens de l'annexe I de la directive (UE) 2022/2555;

i) les centres de coordination régionaux établis en application de l'article 35 du règlement (UE) 2019/943;

j) les fournisseurs de services de sécurité gérés au sens de l'article 6, point 40), de la directive (UE) 2022/2555;

k) toute autre entité ou tout tiers auquel des responsabilités ont été déléguées ou attribuées en application du présent règlement.

2. Dans le cadre de leurs mandats actuels, les autorités suivantes sont chargées d'exécuter les tâches assignées par le présent règlement:

a) l'Agence de coopération des régulateurs de l'énergie («ACER»), instituée par le règlement (UE) nº 2019/942 du Parlement européen et du Conseil ([15]);

b) les autorités nationales compétentes qui sont chargées d'exécuter les tâches que leur assigne le présent règlement et qui sont désignées par les États membres en application de l'article 4, ou «autorités compétentes»;

c) les autorités réglementaires nationales («ARN») désignées par chaque État membre conformément à l'article 57, paragraphe 1, de la directive (UE) 2019/944;

([14]) Règlement d'exécution (UE) nº 1348/2014 de la Commission du 17 décembre 2014 concernant la déclaration des données en application de l'article 8, paragraphes 2 et 6, du règlement (UE) nº 1227/2011 du Parlement européen et du Conseil concernant l'intégrité et la transparence du marché de gros de l'énergie (JO L 363 du 18.12.2014, p. 121).

([15]) Règlement (UE) 2019/942 du Parlement européen et du Conseil du 5 juin 2019 instituant une agence de l'Union européenne pour la coopération des régulateurs de l'énergie (JO L 158 du 14.6.2019, p. 22).

d) les autorités compétentes pour la préparation aux risques («ANC-PR») établies conformément à l'article 3 du règlement (UE) 2019/941;

e) les centres de réponse aux incidents de sécurité informatique (CSIRT) désignés ou créés conformément à l'article 10 de la directive (UE) 2022/2555;

f) les autorités compétentes en matière de cybersécurité («ANC-CS») désignées ou établies par application de l'article 8 de la directive (UE) 2022/2555;

g) l'Agence de l'Union européenne pour la cybersécurité instituée par le règlement (UE) 2019/881;

h) toute autre entité ou tout tiers auquel des responsabilités ont été déléguées ou attribuées en application de l'article 4, paragraphe 3.

3. Le présent règlement s'applique également à toutes les entités qui ne sont pas établies dans l'Union mais qui fournissent des services à des entités dans l'Union, pour autant qu'elles aient été identifiées comme des entités à fort impact ou à impact critique par les autorités compétentes conformément à l'article 24, paragraphe 2.

4. Le présent règlement est sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de leur pouvoir de sauvegarder d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public.

5. Le présent règlement est sans préjudice de la responsabilité des États membres de préserver la sécurité nationale en ce qui concerne les activités de production d'électricité à partir de centrales nucléaires, y compris les activités au sein de la chaîne de valeur nucléaire, conformément aux traités.

6. Les entités, les autorités compétentes, les points de contact uniques au niveau des entités et les CSIRT traitent les données à caractère personnel dans la mesure nécessaire aux fins du présent règlement et conformément au règlement (UE) 2016/679; ce traitement est fondé en particulier sur l'article 6 dudit règlement.

Article 3

Définitions

On entend par:

1) «actif», toute information, tout logiciel ou matériel dans le réseau et les systèmes d'information, corporels ou incorporels, ayant une valeur pour une personne physique, une organisation ou une administration publique;

2) «autorité compétente pour la préparation aux risques», l'autorité compétente désignée en application de l'article 3 du règlement (UE) 2019/941;

3) «centre de réponse aux incidents de sécurité informatique», un centre chargé de la gestion des risques et des incidents conformément à l'article 10 de la directive (UE) 2022/2555;

4) «actif à impact critique», un actif qui est nécessaire pour mener à bien un processus à impact critique;

5) «entité à impact critique», une entité qui met en œuvre un processus à impact critique et qui est identifiée par les autorités compétentes conformément à l'article 24;

6) «périmètre à impact critique», un périmètre défini par une entité visée à l'article 2, paragraphe 1, qui contient tous les actifs à impact critique, dans lequel l'accès à ces actifs peut être contrôlé et qui définit le champ d'application des contrôles de cybersécurité avancés;

7) «processus à impact critique», un processus opérationnel mis en œuvre par une entité pour laquelle les indices d'impact sur la cybersécurité de l'électricité sont supérieurs au seuil d'impact critique;

8) «seuil d'impact critique», les valeurs des indices d'impact sur la cybersécurité de l'électricité visés à l'article 19, paragraphe 3, point b), au-dessus desquelles une cyberattaque contre un processus opérationnel entraînera une perturbation critique des flux transfrontaliers d'électricité;

9) «prestataire critique de services TIC», une entité qui fournit un service TIC, ou un processus TIC qui est nécessaire à un processus à impact critique ou à fort impact affectant les aspects des flux transfrontaliers d'électricité liés à la cybersécurité et qui, s'il est compromis, peut causer une cyberattaque dont l'impact dépasse le seuil d'impact critique ou de fort impact;

10) «flux transfrontalier d'électricité», le flux transfrontalier tel que défini à l'article 2, point 3), du règlement (UE) 2019/943;

11) «cyberattaque», un incident tel que défini à l'article 3, point 14), du règlement (UE) 2022/2554;

12) «cybersécurité», la cybersécurité telle que définie à l'article 2, point 1), du règlement (UE) 2019/881;

13) «contrôle de cybersécurité», les actions ou procédures menées dans le but d'éviter, de détecter, de contrer ou de réduire au minimum les risques de cybersécurité;

14) «incident de cybersécurité», un incident au sens de l'article 6, point 6), de la directive (UE) 2022/2555;

15) «système de gestion de la cybersécurité», les politiques, procédures, lignes directrices, ainsi que les ressources et activités associées, gérées collectivement par une entité, visant à protéger ses ressources d'information contre les cybermenaces de manière systématique en établissant, en mettant en œuvre, en exploitant, en surveillant, en examinant, en maintenant et en améliorant la sécurité des réseaux et des systèmes d'information d'une organisation;

16) «centre d'opérations de cybersécurité», un centre spécialisé dans lequel une équipe technique composée d'un ou de plusieurs experts, soutenus par des systèmes informatiques de cybersécurité, exécute des tâches liées à la sécurité [services du centre opérationnel de cybersécurité (CSOC)], telles que le traitement des cyberattaques et des erreurs de configuration de sécurité, la surveillance de la sécurité, l'analyse des journaux d'événements et la détection des cyberattaques;

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

18) «gestion des vulnérabilités en matière de cybersécurité», la pratique consistant à recenser les vulnérabilités et à y remédier;

19) «entité», une entité au sens de l'article 6, point 38), de la directive (UE) 2022/2555;

20) «alerte précoce», les informations nécessaires pour indiquer si l'incident important est suspecté d'être causé par des actes illicites ou malveillants ou pourrait avoir un impact transfrontalier;

21) «indice d'impact sur la cybersécurité de l'électricité» (ECII), un indice ou une échelle de classification qui classe les conséquences possibles des cyberattaques sur les processus opérationnels associés aux flux transfrontaliers d'électricité;

22) «schéma européen de certification de cybersécurité», un schéma tel que défini à l'article 2, point 9), du règlement (UE) 2019/881;

23) «entité à fort impact», une entité qui met en œuvre un processus à fort impact et qui est identifiée par les autorités compétentes conformément à l'article 24;

24) «processus à fort impact», un processus opérationnel mis en œuvre par une entité pour lequel les indices d'impact sur la cybersécurité de l'électricité sont supérieurs au seuil de fort impact;

25) «actif à fort impact», un actif qui est nécessaire pour mener à bien un processus à fort impact;

26) «seuil de fort impact», les valeurs des indices d'impact sur la cybersécurité de l'électricité visés à l'article 19, paragraphe 3, point b), au-dessus desquelles une cyberattaque contre un processus opérationnel entraînera une forte perturbation des flux transfrontaliers d'électricité;

27) «périmètre à fort impact», un périmètre défini par une entité visée à l'article 2, paragraphe 1, qui contient tous les actifs à fort impact, dans lequel l'accès à ces actifs peut être contrôlé et qui définit le champ d'application des contrôles minimaux de cybersécurité;

28) «produit TIC», un produit TIC au sens de l'article 2, point 12), du règlement (UE) 2019/881;

29) «service TIC», un service TIC au sens de l'article 2, point 13), du règlement (UE) 2019/881;

30) «processus TIC», un processus TIC au sens de l'article 2, point 14), du règlement (UE) 2019/881;

31) «système hérité», un système de TIC au sens de l'article 3, point 3), du règlement (UE) 2022/2554;

32) «point de contact unique national», le point de contact unique désigné ou établi par chaque État membre conformément à l'article 8, paragraphe 3, de la directive (UE) 2022/2555;

33) «autorités de gestion des crises de cybersécurité», les autorités désignées ou établies conformément à l'article 9, point 1), de la directive (UE) 2022/2555;

34) «initiateur», une entité qui initie un événement d'échange, de partage ou de stockage d'informations;

35) «cahier des charges», les spécifications que les entités définissent pour l'acquisition de produits TIC, processus TIC ou services TIC nouveaux ou mis à jour;

36) «représentant», une personne physique ou morale établie dans l'Union qui est explicitement désignée pour agir au nom d'une entité à fort impact ou à impact critique qui n'est pas établie dans l'Union mais qui fournit des services à des entités dans l'Union et qui peut être contactée par une autorité compétente ou un CSIRT en lieu et place de l'entité à fort impact ou à impact critique elle-même en ce qui concerne les obligations incombant à cette entité en vertu du présent règlement;

37) «risque», un risque au sens de l'article 6, point 9), de la directive (UE) 2022/2555;

38) «matrice d'impact des risques», une matrice utilisée lors de l'évaluation des risques pour déterminer le niveau d'impact du risque pour chaque risque évalué;

39) «crise électrique simultanée», une crise électrique telle que définie à l'article 2, point 10), du règlement (UE) 2019/941;

40) «point de contact unique au niveau de l'entité», un point de contact unique au niveau de l'entité désigné à l'article 38, paragraphe 1, point c);

41) «partie prenante», toute partie ayant un intérêt au succès et au fonctionnement continu d'une organisation ou d'un processus, telle que les salariés, les administrateurs, les actionnaires, les régulateurs, les associations, les fournisseurs et les clients;

42) «norme», une norme au sens de l'article 2, point 1), du règlement (UE) nº 1025/2012 du Parlement européen et du Conseil ([16]);

43) «région d'exploitation du réseau», les régions d'exploitation du réseau telles que définies à l'annexe I de la décision 05-2022 de l'ACER relative à la définition des régions d'exploitation du réseau, établies conformément à l'article 36 du règlement (UE) 2019/943;

44) «gestionnaires de réseau», le «gestionnaire de réseau de distribution» (GRD) et le «gestionnaire de réseau de transport» (GRT) au sens de l'article 2, points 29) et 35), de la directive (UE) 2019/944;

45) «processus à impact critique à l'échelle de l'Union», tout processus du secteur de l'électricité, impliquant éventuellement plusieurs entités, pour lequel l'impact éventuel d'une cyberattaque peut être considéré comme critique au cours de l'évaluation des risques de cybersécurité à l'échelle de l'Union;

46) «processus à fort impact à l'échelle de l'Union», tout processus du secteur de l'électricité, impliquant éventuellement plusieurs entités, pour lequel l'impact éventuel d'une cyberattaque peut être considéré comme fort au cours de l'évaluation des risques de cybersécurité à l'échelle de l'Union;

47) «vulnérabilité non corrigée activement exploitée», une vulnérabilité qui n'a pas encore été publiquement divulguée ni corrigée et pour laquelle il existe des preuves fiables que l'exécution d'un code malveillant a été effectuée par un acteur sur un système sans l'autorisation du propriétaire du système;

48) «vulnérabilité», une vulnérabilité au sens de l'article 6, point 15), de la directive (UE) 2022/2555.

Article 4

Autorité compétente

1. Dès que possible et, en tout état de cause, au plus tard le 13 décembre 2024, chaque État membre désigne une autorité gouvernementale ou réglementaire nationale chargée d'exécuter les tâches qui lui sont assignées par le présent règlement (ci-après dénommée «autorité compétente»). Jusqu'à ce que l'autorité compétente se soit vu assigner les tâches prévues par le présent règlement, l'autorité de régulation désignée par chaque État membre conformément à l'article 57, paragraphe 1, de la directive (UE) 2019/944 exécute les tâches de l'autorité compétente conformément au présent règlement.

2. Les États membres notifient sans tarder à la Commission, à l'ACER, à l'ENISA, au groupe de coopération SRI établi conformément à l'article 14 de la directive (UE) 2022/2555 et au groupe de coordination pour l'électricité institué conformément à l'article 1er de la décision de la Commission du 15 novembre 2012 ([17]) et leur communiquent le nom et les coordonnées de leur autorité compétente désignée en application du paragraphe 1 du présent article, ainsi que toute modification ultérieure y afférente.

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

([17]) Décision de la Commission du 15 novembre 2012 portant création du groupe de coordination pour l'électricité (2012/C/353/02) (JO C 353 du 17.11.2012, p. 2).

3. Les États membres peuvent autoriser leur autorité compétente à déléguer les tâches qui lui sont assignées par le présent règlement à d'autres autorités nationales, à l'exception des tâches énumérées à l'article 5. Chaque autorité compétente contrôle l'application du présent règlement par les autorités auxquelles elle a délégué des tâches. L'autorité compétente communique le nom, les coordonnées, les tâches assignées et toute modification ultérieure des autorités auxquelles une tâche a été déléguée à la Commission, à l'ACER, au groupe de coordination pour l'électricité, à l'ENISA et au groupe de coopération SRI.

Article 5

Coopération entre les autorités et organismes compétents au niveau national

Les autorités compétentes coordonnent et assurent une coopération appropriée entre les autorités compétentes en matière de cybersécurité, les autorités chargées de la gestion des crises de cybersécurité, les ARN, les autorités compétentes pour la préparation aux risques et les CSIRT aux fins du respect des obligations pertinentes énoncées dans le présent règlement. Les autorités compétentes se coordonnent également avec tout autre organisme ou autorité déterminé par chaque État membre, afin de garantir l'efficacité des procédures et d'éviter les doubles emplois dans les tâches et les obligations. Les autorités compétentes peuvent donner instruction aux ARN respectives de demander l'avis de l'ACER conformément à l'article 8, paragraphe 3.

Article 6

Modalités et conditions ou méthodes des GRT

1. Les GRT élaborent, en coopération avec l'entité des GRD de l'Union, des propositions de modalités et conditions ou de méthodes conformément au paragraphe 2, ou de plans conformément au paragraphe 3.

2. Les propositions concernant les modalités et conditions ou méthodes et chacune de leurs modifications sont soumises à l'approbation de l'Agence:

a) les méthodes d'évaluation des risques de cybersécurité conformément à l'article 18, paragraphe 1;

b) le rapport d'évaluation complète des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité conformément à l'article 23;

c) les contrôles minimaux et avancés de cybersécurité conformément à l'article 29, la cartographie des contrôles de cybersécurité de l'électricité par rapport aux normes, conformément à l'article 34, y compris les contrôles minimaux et avancés de cybersécurité dans la chaîne d'approvisionnement conformément à l'article 33;

d) une recommandation relative à la passation de marchés dans le domaine de la cybersécurité conformément à l'article 35;

e) la méthode/échelle de classification des cyberattaques conformément à l'article 37, paragraphe 8.

3. Les propositions de plans régionaux d'atténuation des risques de cybersécurité en application de l'article 22 sont soumises à l'approbation de toutes les autorités compétentes de la région d'exploitation du réseau concernée.

4. Les propositions de modalités et conditions ainsi que de méthodes énumérées au paragraphe 2 ou de plans énumérés au paragraphe 3 comprennent une proposition de calendrier pour leur mise en œuvre et une description de leur incidence attendue sur les objectifs du présent règlement.

5. L'entité des GRD de l'Union peut adresser un avis motivé aux GRT concernés jusqu'à 3 semaines avant la date limite de soumission de la proposition de modalités et conditions, de méthodes ou de plans aux autorités compétentes. Les GRT responsables de la proposition de modalités et conditions ou de méthodes ou de plans tiennent compte de l'avis motivé de l'entité des GRD de l'Union avant de le soumettre à l'approbation des autorités compétentes. Les GRT fournissent une motivation lorsque l'avis de l'entité des GRD de l'Union n'est pas pris en compte.

6. Lorsqu'ils élaborent conjointement les modalités, conditions et méthodes et plans, les GRT participants coopèrent étroitement. Les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, informent régulièrement les autorités compétentes et l'ACER des progrès accomplis dans l'élaboration des modalités et conditions, des méthodes ou des plans.

Article 7

Règles de vote au sein des GRT

1. Lorsque les GRT statuant sur des propositions de modalités et conditions ou de méthodes ne sont pas en mesure de parvenir à un accord, ils statuent à la majorité qualifiée. La majorité qualifiée pour ces propositions est calculée comme suit:

a) un ensemble de GRT représentant au moins 55 % des États membres; et

b) un ensemble de GRT représentant des États membres comprenant au moins 65 % de la population de l'Union.

2. La minorité de blocage pour les décisions relatives aux propositions de modalités et conditions ou de méthodologies visées à l'article 6, paragraphe 2, doit inclure des GRT représentant au moins quatre États membres, faute de quoi la majorité qualifiée est réputée acquise.

3. Lorsque les GRT d'une région d'exploitation du réseau qui décident des propositions de plans énumérés à l'article 6, paragraphe 2, ne sont pas en mesure de parvenir à un accord, et lorsque la région d'exploitation du réseau concernée est composée de plus de cinq États membres, les GRT statuent à la majorité qualifiée. La majorité qualifiée pour les propositions visées à l'article 6, paragraphe 2, correspond à la majorité suivante:

a) un ensemble de GRT représentant au moins 72 % des États membres concernés; et

b) un ensemble de GRT représentant des États membres comprenant au moins 65 % de la population de la région concernée.

4. Une minorité de blocage pour les décisions sur les propositions de plans doit inclure au moins le nombre minimum de GRT représentant plus de 35 % de la population des États membres participants, plus un ensemble de GRT représentant au moins un État membre supplémentaire concerné, faute de quoi la majorité qualifiée est réputée acquise.

5. Pour les décisions des GRT relatives aux propositions de modalités et conditions ou de méthodes visées à l'article 6, paragraphe 2, une seule voix est attribuée par État membre. S'il existe plusieurs GRT sur le territoire d'un État membre, cet État membre répartit les droits de vote entre les GRT.

6. Si, en coopération avec l'entité des GRD de l'Union, les GRT ne soumettent pas de proposition initiale ou modifiée de modalités et conditions ou de méthodes, ou de plans, aux autorités compétentes concernées dans les délais fixés dans le présent règlement, ils fournissent aux autorités compétentes concernées et à l'ACER les projets pertinents de modalités et conditions, de méthodes ou de plans. Ils expliquent ce qui a empêché un accord. Les autorités compétentes prennent conjointement les mesures appropriées en vue de l'adoption des modalités et conditions ou des méthodes requises, ou des plans requis. Cela peut se faire, par exemple, en demandant des modifications aux projets conformément au présent paragraphe, en révisant et en complétant ces projets ou, lorsque aucun projet n'a été fourni, en définissant et en approuvant les modalités et conditions, les méthodes ou les plans requis.

Article 8

Transmission de propositions aux autorités compétentes

1. Les GRT soumettent les propositions de modalités et conditions ou de méthodes, ou de plans, pour approbation, aux autorités compétentes concernées dans les délais respectifs fixés aux articles 18, 23, 29, 33, 34, 35 et 37. Les autorités compétentes peuvent prolonger conjointement ces délais dans des circonstances exceptionnelles, notamment dans les cas où un délai ne peut être respecté en raison de circonstances extérieures à la sphère des GRT ou de l'entité des GRD de l'Union.

2. Les propositions de modalités et conditions, de méthodes ou de plans en application du paragraphe 1 sont soumises pour information à l'ACER au moment où elles sont soumises aux autorités compétentes.

3. À la demande conjointe des ARN, l'ACER émet un avis sur la proposition de modalités et conditions ou de méthodes, ou de plans, dans un délai de six mois à compter de la réception des propositions de modalités et conditions ou de méthodes, ou de plans, et notifie cet avis aux ARN et aux autorités compétentes. Les ARN, les ANC-CS et toute autre autorité désignée comme autorité compétente se coordonnent avant que les ARN ne demandent un avis à l'ACER. L'ACER peut inclure des recommandations dans cet avis. L'ACER consulte l'ENISA avant d'émettre un avis sur les propositions énumérées à l'article 6, paragraphe 2.

4. Les autorités compétentes se consultent, coopèrent et se coordonnent étroitement afin de parvenir à un accord sur les modalités et conditions, méthodes ou plans proposés. Avant d'approuver les modalités et conditions ou les méthodes, ou les plans, elles révisent et complètent les propositions si nécessaire, après consultation du REGRT pour l'électricité et de l'entité des GRD de l'Union, afin de veiller à ce que les propositions soient conformes au présent règlement et contribuent à un niveau élevé commun de cybersécurité dans l'ensemble de l'Union.

5. Les autorités compétentes se prononcent sur les modalités et conditions, sur les méthodes ou sur les plans dans un délai de six mois à compter de la réception des modalités et conditions, des méthodes ou des plans par l'autorité compétente concernée ou, le cas échéant, par la dernière autorité compétente concernée.

6. Lorsque l'ACER émet un avis, les autorités compétentes concernées tiennent compte de cet avis et prennent leurs décisions dans un délai de six mois à compter de la réception de l'avis de l'ACER.

7. Lorsque les autorités compétentes exigent conjointement une modification des modalités et conditions ou des méthodes proposées, ou des plans, afin de les approuver, les GRT élaborent, en coopération avec l'entité des GRD de l'Union, une proposition de modification des modalités et conditions ou des méthodes, ou des plans. Les GRT soumettent la proposition modifiée pour approbation dans un délai de deux mois à compter de la demande des autorités compétentes. Les autorités compétentes statuent sur les modalités et conditions, les méthodes ou les plans modifiés dans un délai de deux mois à compter de sa soumission.

8. Lorsque les autorités compétentes n'ont pas été en mesure de parvenir à un accord dans le délai prévu au paragraphe 5 ou 7, elles en informent la Commission. La Commission peut prendre les mesures appropriées pour permettre l'adoption des modalités et conditions, des méthodes ou des plans requis.

9. Les GRT, avec l'aide du REGRT pour l'électricité, et de l'entité des GRD de l'Union, publient les modalités et conditions, les méthodes ou les plans sur leurs sites internet après approbation par les autorités compétentes concernées, sauf lorsque ces informations sont considérées comme confidentielles conformément à l'article 47.

10. Les autorités compétentes peuvent demander conjointement aux GRT et à l'entité des GRD de l'Union des propositions de modification des modalités et conditions ou des méthodes approuvées, ou des plans approuvés, et fixer un délai pour la soumission de ces propositions. Les GRT, en coopération avec l'entité des GRD de l'Union, peuvent également proposer des modifications aux autorités compétentes de leur propre initiative. Les propositions de modification des modalités et conditions, des méthodes ou des plans sont élaborées et approuvées conformément à la procédure prévue au présent article.

11. Au moins tous les trois ans après la première adoption des modalités et conditions, des méthodes ou des plans, les GRT, en coopération avec l'entité des GRD de l'Union, examinent l'efficacité des modalités et conditions, des méthodes ou des plans adoptés, et communiquent les conclusions de cet examen aux autorités compétentes et à l'ACER dans les meilleurs délais.

Article 9

Consultation

1. Les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, consultent les parties prenantes, y compris l'ACER, l'ENISA et l'autorité compétente de chaque État membre, sur les projets de propositions de modalités et conditions ou de méthodes énumérés à l'article 6, paragraphe 2, et de plans visés à l'article 6, paragraphe 3. La durée de la consultation n'est pas inférieure à un mois.

2. Les propositions de modalités et conditions ou de méthodes énumérées à l'article 6, paragraphe 2 soumises par les GRT, en coopération avec l'entité des GRD de l'Union, sont publiées et soumises à consultation au niveau de l'Union. Les propositions de plans énumérées à l'article 6, paragraphe 3, soumises par les GRT compétents, en coopération avec l'entité des GRD de l'Union, au niveau régional sont soumises à consultation au moins au niveau régional.

3. Les GRT, avec l'aide du REGRT pour l'électricité, et de l'entité des GRD de l'Union responsable de la proposition de modalités et conditions ou de méthodes ou de plans tiennent dûment compte des avis des parties prenantes résultant des consultations menées conformément au paragraphe 1, avant de le soumettre pour approbation par les autorités de régulation. En tout état de cause, les raisons précises pour lesquelles les avis exprimés lors de la consultation ont été ou non pris en considération sont jointes à la soumission, et publiées en temps utile, avant ou en même temps que la proposition de modalités et conditions ou de méthodes.

Article 10

Participation des parties prenantes

L'ACER, en étroite coopération avec le REGRT pour l'électricité et l'entité des GRD de l'Union, organise la participation des parties prenantes, y compris des réunions régulières avec les parties prenantes afin de recenser les problèmes et de proposer des améliorations liées à la mise en œuvre du présent règlement.

Article 11

Recouvrement des frais

1. Les coûts supportés par les GRT et les GRD soumis à la réglementation tarifaire du réseau et découlant des obligations prévues par le présent règlement, y compris les coûts supportés par le REGRT pour l'électricité et l'entité des GRD de l'Union, sont évalués par l'ARN compétente de chaque État membre.

2. Les coûts jugés raisonnables, efficaces et proportionnés sont récupérés au moyen de tarifs de réseau ou d'autres mécanismes appropriés, tels que déterminés par l'ARN compétente.

3. À la demande des ARN compétentes, les GRT et les GRD visés au paragraphe 1 fournissent, dans un délai raisonnable déterminé par l'ARN, les informations nécessaires pour faciliter l'évaluation des coûts encourus.

Article 12

Surveillance

1. L'ACER surveille la mise en œuvre du présent règlement conformément à l'article 32, paragraphe 1, du règlement (UE) 2019/943 et à l'article 4, paragraphe 2, du règlement (CE) n° 2019/942. Dans le cadre de cette surveillance, l'ACER peut coopérer avec l'ENISA et demander le soutien de l'ENTSO pour l'électricité et de l'entité des GRD de l'Union. L'ACER informe régulièrement le groupe de coordination pour l'électricité et le groupe de coopération SRI sur la mise en œuvre du présent règlement.

2. L'ACER publie un rapport au moins tous les trois ans après l'entrée en vigueur du présent règlement afin:

a) d'examiner l'état d'avancement de la mise en œuvre des mesures de gestion des risques de cybersécurité applicables en ce qui concerne les entités à fort impact et à impact critique;

b) de déterminer si des règles supplémentaires relatives aux exigences communes, à la planification, à la surveillance, à l'établissement de rapports et à la gestion des crises peuvent être nécessaires pour prévenir les risques pour le secteur de l'électricité; et

c) de recenser les domaines à améliorer en vue de la révision du présent règlement, ou de déterminer les domaines non couverts et les nouvelles priorités qui pourraient apparaître en raison des évolutions technologiques.

3. Au plus tard le 13 juin 2025, l'ACER, en coopération avec l'ENISA et après consultation du REGRT pour l'électricité et de l'entité des GRD de l'Union, peut publier des orientations sur les informations pertinentes devant être communiquées à l'ACER aux fins de la surveillance ainsi que sur le processus et la fréquence de la collecte, sur la base des indicateurs de performance définis conformément au paragraphe 5.

4. Les autorités compétentes peuvent avoir accès aux informations pertinentes détenues par l'ACER qu'elle a collectées conformément au présent article.

5. L'ACER, en coopération avec l'ENISA et avec le soutien du REGRT pour l'électricité et de l'entité des GRD de l'Union, publie des indicateurs de performance non contraignants pour l'évaluation de la fiabilité opérationnelle qui sont liés aux aspects de cybersécurité des flux transfrontaliers d'électricité.

6. Les entités énumérées à l'article 2, paragraphe 1, du présent règlement communiquent à l'ACER les informations dont elle a besoin pour accomplir les tâches énumérées au paragraphe 2.

Article 13

Évaluation comparative

1. Au plus tard le 13 juin 2025, l'ACER, en coopération avec l'ENISA, établit un guide non contraignant d'évaluation comparative en matière de cybersécurité. Le guide explique aux ARN les principes de l'évaluation comparative des contrôles de cybersécurité mis en œuvre conformément au paragraphe 2 du présent article, en tenant compte des coûts de mise en œuvre des contrôles et de l'efficacité de la fonction assurée par les processus, produits, services, systèmes et solutions utilisés pour mettre en œuvre ces contrôles. L'ACER tient compte des rapports d'évaluation comparative existants lors de l'élaboration du guide d'évaluation comparative non contraignant en matière de cybersécurité. L'ACER soumet le guide non contraignant d'évaluation comparative en matière de cybersécurité aux ARN pour information.

2. Dans les 12 mois à compter de la mise en place du guide d'évaluation comparative conformément au paragraphe 1, les ARN effectuent une évaluation comparative afin de déterminer si les investissements actuels dans la cybersécurité:

a) atténuent les risques ayant un impact sur les flux transfrontaliers d'électricité;

b) donnent les résultats souhaités et génèrent des gains d'efficacité pour le développement des systèmes électriques;

c) sont efficaces et intégrés dans l'ensemble des marchés publics d'actifs et de services.

3. Aux fins de l'évaluation comparative, les ARN peuvent tenir compte du guide non contraignant d'évaluation comparative en matière de cybersécurité établi par l'ACER et évaluent en particulier:

a) les dépenses moyennes liées à la cybersécurité pour atténuer les risques ayant un impact sur les flux transfrontaliers d'électricité, en particulier en ce qui concerne les entités à fort impact et à impact critique;

b) en coopération avec le REGRT pour l'électricité et l'entité des GRD de l'Union, les prix moyens des services, systèmes et produits de cybersécurité qui contribuent dans une large mesure à l'amélioration et à la maintenance des mesures de gestion des risques de cybersécurité dans les différentes régions d'exploitation du réseau;

c) l'existence et le niveau de comparabilité des coûts et des fonctions des services, systèmes et solutions de cybersécurité adaptés à la mise en œuvre du présent règlement, en identifiant les mesures envisageables en faveur de l'efficacité des dépenses, en particulier lorsque des investissements technologiques dans le domaine de la cybersécurité peuvent s'avérer nécessaires.

4. Toute information liée à l'évaluation comparative est traitée conformément aux exigences en matière de classification des données du présent règlement, des contrôles minimaux de cybersécurité et du rapport d'évaluation transfrontalière des risques de cybersécurité dans le secteur de l'électricité. L'évaluation comparative visée aux paragraphes 2 et 3 n'est pas rendue publique.

5. Sans préjudice des exigences de confidentialité à l'article 47 et de la nécessité de protéger la sécurité des entités soumises aux dispositions du présent règlement, l'évaluation comparative visée aux paragraphes 2 et 3 du présent article est communiquée à toutes les ARN, toutes les autorités compétentes, l'ACER, l'ENISA et la Commission.

Article 14

Accords avec des GRT extérieurs à l'Union

1. Dans un délai de 18 mois à compter de l'entrée en vigueur du présent règlement, les GRT d'une région d'exploitation du réseau voisine d'un pays tiers s'efforcent de conclure avec les GRT du pays tiers voisin des accords qui sont conformes au droit de l'Union applicable et qui définissent la base de la coopération en matière de protection de la cybersécurité et des accords de coopération en matière de cybersécurité avec ces GRT.

2. Les GRT informent l'autorité compétente des accords conclus en application du paragraphe 1.

Article 15

Représentants légaux

1. Les entités qui n'ont pas d'établissement dans l'Union, mais qui fournissent des services à des entités de l'Union et qui ont été notifiées comme étant des entités à fort impact ou à impact critique conformément à l'article 24, paragraphe 6, désignent, par écrit, dans un délai de trois mois à compter de la notification, un représentant dans l'Union et en informent l'autorité compétente notifiante.

2. Ce représentant est mandaté pour être considéré par toute autorité compétente ou un CSIRT dans l'Union comme en complément ou en lieu et place de l'entité à fort impact ou à impact critique en ce qui concerne les obligations de l'entité au titre du présent règlement. L'entité à fort impact ou à impact critique dote son représentant légal des pouvoirs nécessaires et des ressources suffisantes pour garantir sa coopération efficace et en temps utile avec les autorités compétentes ou les CSIRT concernés.

3. Ce représentant est établi dans l'un des États membres dans lesquels les services sont fournis. L'entité est considérée comme relevant de la compétence de l'État membre dans lequel le représentant est établi. Les entités à fort impact ou à impact critique communiquent le nom, l'adresse postale, l'adresse de courrier électronique et le numéro de téléphone de leur représentant légal au coordinateur pour les services numériques de l'État membre dans lequel le représentant légal réside ou est établi.

4. Le représentant légal désigné peut être tenu pour responsable du non-respect des obligations prévues dans le présent règlement, sans préjudice de la responsabilité de l'entité à fort impact ou à impact critique elle-même et des actions en justice qui pourraient être intentées contre elle.

5. S'il n'est pas procédé à la désignation, selon le présent article, d'un représentant au sein de l'Union, tout État membre dans lequel l'entité fournit des services peut intenter une action en justice contre l'entité pour non-respect des obligations découlant du présent règlement.

6. La désignation d'un représentant légal dans l'Union en application du paragraphe 1 ne constitue pas un établissement dans l'Union.

Article 16

Coopération entre le REGRT pour l'électricité et l'entité des GRD de l'Union

1. Le REGRT pour l'électricité et l'entité des GRD de l'Union coopèrent à la réalisation des évaluations des risques de cybersécurité conformément à l'article 19 et à l'article 21, et plus particulièrement des tâches suivantes:

a) élaboration des méthodes d'évaluation des risques de cybersécurité conformément à l'article 18, paragraphe 1;

b) établissement du rapport d'évaluation complète des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité, conformément à l'article 23;

c) définition du cadre commun en matière de cybersécurité dans le secteur de l'électricité conformément au chapitre III;

d) formulation d'une recommandation relative à la passation de marchés dans le domaine de la cybersécurité conformément à l'article 35;

e) définition de la méthode/échelle de classification des cyberattaques conformément à l'article 37, paragraphe 8;

f) fixation de l'indice provisoire d'impact sur la cybersécurité de l'électricité (ECII) conformément à l'article 48, paragraphe 1, point a);

g) établissement de la liste provisoire consolidée des entités à fort impact et à impact critique conformément à l'article 48, paragraphe 3;

h) établissement de la liste provisoire des processus à fort impact et à impact critique à l'échelle de l'Union conformément à l'article 48, paragraphe 4;

i) établissement de la liste provisoire des normes et contrôles européens et internationaux conformément à l'article 48, paragraphe 6;

j) réalisation de l'évaluation des risques de cybersécurité à l'échelle de l'Union conformément à l'article 19;

k) réalisation des évaluations régionales des risques de cybersécurité conformément à l'article 21;

l) définition des plans régionaux d'atténuation des risques de cybersécurité conformément à l'article 22;

m) élaboration d'orientations sur les schémas européens de certification de cybersécurité pour les produits TIC, services TIC et processus TIC conformément l'article 36;

n) élaboration de lignes directrices pour la mise en œuvre du présent règlement en concertation avec l'ACER et l'ENISA.

2. La coopération entre le REGRT pour l'électricité et le GRD de l'Union peut prendre la forme d'un groupe de travail sur les risques de cybersécurité.

3. Le REGRT pour l'électricité et l'entité des GRD de l'Union informent régulièrement l'ACER, l'ENISA, le groupe de coopération SRI et le groupe de coordination pour l'électricité des progrès accomplis dans la mise en œuvre des évaluations des risques de cybersécurité à l'échelle de l'Union et au niveau régional conformément à l'article 19 et à l'article 21.

Article 17

Coopération entre l'ACER et les autorités compétentes

L'ACER, en coopération avec chaque autorité compétente:

1) surveille la mise en œuvre des mesures de gestion des risques de cybersécurité conformément à l'article 12, paragraphe 2, point a), et des obligations en matière de rapport conformément à l'article 27 et à l'article 39; et

2) surveille le processus d'adoption et la mise en œuvre des modalités et conditions, des méthodes ou plans conformément à l'article 6, paragraphes 2 et 3. La coopération entre l'ACER, l'ENISA et chaque autorité compétente peut prendre la forme d'un organisme de surveillance des risques de cybersécurité.

CHAPITRE II

ÉVALUATION DES RISQUES ET IDENTIFICATION DES RISQUES DE CYBERSÉCURITÉ PERTINENTS

Article 18

Méthode d'évaluation des risques de cybersécurité

1. Au plus tard le 13 mars 2025, les GRT, avec l'aide du REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union et après consultation du groupe de coopération SRI, soumettent une proposition de méthodes d'évaluation des risques de cybersécurité au niveau de l'Union, au niveau régional et au niveau des États membres.

2. Les méthodes d'évaluation des risques de cybersécurité au niveau de l'Union, au niveau régional et au niveau des États membres comprennent:

a) une liste des cybermenaces à prendre en considération, comprenant au moins les menaces suivantes sur la chaîne d'approvisionnement:

   i) une dégradation grave et inattendue de la chaîne d'approvisionnement;

   ii) l'indisponibilité de produits TIC, services TIC ou processus TIC de la chaîne d'approvisionnement;

iii) des cyberattaques lancées par des acteurs de la chaîne d'approvisionnement;

iv) des fuites d'informations sensibles tout au long de la chaîne d'approvisionnement, y compris le suivi de la chaîne d'approvisionnement;

v) l'introduction de faiblesses ou de portes dérobées dans les produits TIC, les services TIC ou les processus TIC par l'intermédiaire d'acteurs de la chaîne d'approvisionnement.

b) les critères permettant d'évaluer l'impact des risques de cybersécurité, qu'ils soient élevés ou critiques, en utilisant des seuils définis en matière de conséquences et de probabilité;

c) une approche visant à analyser les risques de cybersécurité découlant de systèmes historiques, les effets en cascade des cyberattaques et le caractère «en temps réel» des systèmes assurant le fonctionnement du réseau électrique.

d) une approche visant à analyser les risques de cybersécurité découlant de la dépendance à l'égard d'un fournisseur unique de produits TIC, de services TIC ou de processus TIC.

3. Les méthodes d'évaluation des risques de cybersécurité au niveau de l'Union, au niveau régional et au niveau des États membres reposent sur la même matrice d'impact des risques. La matrice d'impact des risques permet de:

a) mesurer les conséquences des cyberattaques sur la base des critères suivants:

i) perte de charge;

ii) réduction de la production d'électricité;

iii) perte de capacité dans la réserve primaire de stabilisation de la fréquence;

iv) perte de capacité de reconstitution d'un réseau électrique sans recourir au réseau de transport externe pour le rétablissement après un arrêt total ou partiel (également appelée «démarrage autonome»);

v) durée prévue d'une panne d'électricité affectant les clients, combinée à l'ampleur de l'indisponibilité en nombre de clients;

vi) tout autre critère quantitatif ou qualitatif qui pourrait raisonnablement servir d'indicateur de l'effet d'une cyberattaque sur les flux transfrontaliers d'électricité.

b) mesurer la probabilité d'un incident sous forme de la fréquence annuelle des cyberattaques.

4. Les méthodes d'évaluation des risques de cybersécurité au niveau de l'Union décrivent la manière dont les valeurs ECII pour les seuils de fort impact et d'impact critique seront définies. L'ECII permet aux entités d'estimer, à l'aide des critères visés au paragraphe 2, point b), l'incidence des risques sur leur processus opérationnel, lors des analyses d'impact sur les activités qu'elles effectuent conformément à l'article 26, paragraphe 4, point c) i).

5. Le REGRT pour l'électricité, en coordination avec l'entité des GRD de l'Union, informe le groupe de coordination pour l'électricité des propositions de méthodes d'évaluation des risques de cybersécurité qui sont élaborées conformément au paragraphe 1.

Article 19

Évaluation des risques de cybersécurité à l'échelle de l'Union

1. Dans un délai de 9 mois à compter de l'approbation des méthodes d'évaluation des risques de cybersécurité conformément à l'article 8, et par la suite tous les trois ans, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union et en concertation avec le groupe de coopération SRI, procède, sans préjudice de l'article 22 de la directive (UE) 2022/2555, à une évaluation des risques de cybersécurité à l'échelle de l'Union et élabore un projet de rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union. À cette fin seront utilisées les méthodes élaborées conformément à l'article 18 et approuvées conformément à l'article 8 pour identifier, analyser et évaluer les conséquences possibles des cyberattaques qui nuisent à la sécurité d'exploitation du système électrique et perturbent les flux transfrontaliers d'électricité. L'évaluation des risques de cybersécurité à l'échelle de l'Union ne tient pas compte des atteintes juridiques, financières ou à la réputation liées aux cyberattaques.

2. Le rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union comprend les éléments suivants:

a) les processus à fort impact à l'échelle de l'Union et les processus à impact critique à l'échelle de l'Union;

b) une matrice d'impact des risques que les entités et les autorités compétentes utilisent pour évaluer les risques de cybersécurité recensés dans l'évaluation des risques de cybersécurité au niveau des États membres effectuée conformément à l'article 20 et dans l'évaluation des risques de cybersécurité au niveau de l'entité conformément à l'article 26, paragraphe 2, point b).

3. En ce qui concerne les processus à fort impact à l'échelle de l'Union et les processus à impact critique à l'échelle de l'Union, le rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union comprend:

a) une évaluation des conséquences possibles d'une cyberattaque à l'aide des paramètres définis dans la méthode d'évaluation des risques de cybersécurité élaborée conformément à l'article 18, paragraphes 2, 3 et 4, et approuvée conformément à l'article 8;

b) les seuils ECII et les seuils de fort impact et d'impact critique que les autorités compétentes utiliseront conformément à l'article 24, paragraphes 1 et 2, pour recenser les entités à fort impact et à impact critique participant aux processus à fort impact à l'échelle de l'Union ou aux processus à impact critique à l'échelle de l'Union.

4. Le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, soumet à l'ACER, pour avis, le projet de rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union, accompagné des résultats de l'évaluation des risques de cybersécurité à l'échelle de l'Union. L'ACER émet un avis sur le projet de rapport dans un délai de trois mois à compter de sa réception. Le REGRT pour l'électricité et l'entité des GRD de l'Union tiennent le plus grand compte de l'avis de l'ACER lors de la finalisation de ce rapport.

5. Dans un délai de trois mois à compter de la réception de l'avis de l'ACER, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, notifie le rapport final d'évaluation des risques de cybersécurité à l'ACER, à la Commission, à l'ENISA et aux autorités compétentes.

Article 20

Évaluation des risques de cybersécurité au niveau des États membres

1. Chaque autorité compétente procède à une évaluation des risques de cybersécurité d'un État membre pour toutes les entités à fort impact ou à impact critique dans son État membre en utilisant les méthodes élaborées conformément à l'article 18 et approuvées conformément à l'article 8. L'évaluation des risques de cybersécurité au niveau des États membres recense et analyse les risques de cyberattaques portant atteinte à la sécurité d'exploitation du système électrique et perturbant les flux transfrontaliers d'électricité. L'évaluation des risques de cybersécurité à l'échelle de l'Union ne tient pas compte des atteintes juridiques, financières ou à la réputation liées aux cyberattaques.

2. Dans un délai de 21 mois à compter de la notification des entités à fort impact ou à impact critique conformément à l'article 24, paragraphe 6, et tous les trois ans après cette date, après consultation de l'AC CS-ANC responsable de l'électricité, chaque autorité compétente, soutenue par le CSIRT, transmet au REGRT pour l'électricité et à l'entité des GRD de l'Union un rapport d'évaluation des risques de cybersécurité des États membres, contenant les informations suivantes pour chaque processus opérationnel à fort impact ou à impact critique:

a) l'état d'avancement de la mise en œuvre des contrôles minimaux et avancés de cybersécurité conformément à l'article 29;

b) une liste de toutes les cyberattaques signalées au cours des trois dernières années conformément à l'article 38, paragraphe 3;

c) un résumé des informations sur les cybermenaces communiquées au cours des trois années précédentes conformément à l'article 38, paragraphe 6;

d) pour chaque processus à fort impact ou à impact critique à l'échelle de l'Union, une estimation des risques de compromission de la confidentialité, de l'intégrité et de la disponibilité des informations et des actifs pertinents;

e) s'il y a lieu, une liste des entités supplémentaires identifiées comme ayant un fort impact ou un impact critique conformément à l'article 24, paragraphes 1, 2, 3 et 5.

3. Le rapport d'évaluation des risques de cybersécurité au niveau d'un État membre tient compte du plan de préparation aux risques de l'État membre établi conformément à l'article 10 du règlement (UE) 2019/941.

4. Les informations contenues dans le rapport d'évaluation des risques de cybersécurité au niveau d'un État membre conformément au paragraphe 2, points a) à d), ne sont pas liées à des entités ou actifs spécifiques. Le rapport sur l'évaluation des risques de cybersécurité au niveau d'un État membre comprend également une évaluation des risques liés aux dérogations temporaires accordées par les autorités compétentes des États membres sur la base de l'article 30.

5. Le REGRT pour l'électricité et l'entité des GRD de l'Union peuvent demander des informations complémentaires aux autorités compétentes en ce qui concerne les tâches visées au paragraphe 2, points a) et c).

6. Les autorités compétentes veillent à ce que les informations qu'elles fournissent soient exactes et correctes.

Article 21

Évaluations des risques de cybersécurité au niveau régional

1. Le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union et en concertation avec le centre de coordination régional compétent, procède à une évaluation régionale des risques de cybersécurité pour chaque région d'exploitation du réseau en utilisant les méthodes définies conformément à l'article 19 et approuvées conformément à l'article 8, pour identifier, analyser et évaluer les risques de cyberattaques affectant la sécurité d'exploitation du système électrique et perturbant les flux transfrontaliers d'électricité. L'évaluation des risques de cybersécurité au niveau régional ne tient pas compte des atteintes juridiques, financières ou à la réputation liées aux cyberattaques.

2. Dans un délai de 30 mois à compter de la notification des entités à fort impact ou à impact critique conformément à l'article 24, paragraphe 6, et par la suite tous les trois ans, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union et en concertation avec le groupe de coopération SRI, élabore un rapport d'évaluation des risques de cybersécurité au niveau régional pour chaque région d'exploitation du réseau.

3. Le rapport d'évaluation des risques de cybersécurité au niveau régional tient compte des informations pertinentes contenues dans les rapports d'évaluation des risques de cybersécurité à l'échelle de l'Union et dans les rapports d'évaluation des risques de cybersécurité au niveau des États membres.

4. L'évaluation des risques de cybersécurité au niveau régional tient compte des scénarios régionaux de crise électrique liés à la cybersécurité identifiés conformément à l'article 6 du règlement (UE) 2019/941.

Article 22

Plans régionaux d'atténuation des risques de cybersécurité

1. Dans un délai de 36 mois à compter de la notification des entités à fort impact ou à impact critique conformément à l'article 24, paragraphe 6, et au plus tard le 13 juin 2031, et par la suite tous les trois ans, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union et en concertation avec le groupe de coopération SRI, élabore un rapport d'évaluation des risques de cybersécurité au niveau régional pour chaque région d'exploitation du réseau.

2. Les plans régionaux d'atténuation des risques de cybersécurité comprennent:

a) les contrôles minimaux et avancés de cybersécurité que les entités à fort impact et les entités à impact critique appliquent dans la région d'exploitation du réseau;

b) les risques résiduels en matière de cybersécurité dans les régions d'exploitation du réseau après application des contrôles visés au point a).

3. Le REGRT pour l'électricité soumet les plans régionaux d'atténuation des risques aux gestionnaires de réseau de transport concernés, aux autorités compétentes et au groupe de coordination pour l'électricité. Le groupe de coordination pour l'électricité peut recommander des modifications.

4. Les GRT, avec l'aide du REGRT pour l'électricité en coopération avec l'entité des GRD de l'Union et en concertation avec le groupe de coopération SRI, mettent à jour les plans régionaux d'atténuation des risques tous les trois ans, sauf si les circonstances justifient des mises à jour plus fréquentes.

Article 23

Rapport d'évaluation complète des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité

1. Dans un délai de 40 mois à compter de la notification des entités à fort impact critique conformément à l'article 24, paragraphe 6, et par la suite tous les trois ans, les GRT, avec l'aide du REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union et en concertation avec le groupe de coopération SRI, transmettent au groupe de coordination pour l'électricité un rapport sur les résultats de l'évaluation des risques de cybersécurité en ce qui concerne les flux transfrontaliers d'électricité (ci-après le «rapport d'évaluation complète des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité»).

2. Le rapport d'évaluation complète des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité est fondé sur le rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union, sur les rapports d'évaluation des risques de cybersécurité des États membres et sur les rapports régionaux d'évaluation des risques de cybersécurité et comprend les informations suivantes:

a) la liste des processus à fort impact et à impact critique à l'échelle de l'Union recensés dans le rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union conformément à l'article 19, paragraphe 2, point a), y compris l'estimation de la probabilité et de l'impact des risques de cybersécurité évalués lors des rapports régionaux d'évaluation des risques de cybersécurité conformément à l'article 21, paragraphe 2, et à l'article 19, paragraphe 3, point a);

b) les cybermenaces actuelles, en mettant particulièrement l'accent sur les menaces et les risques émergents pour le système électrique;

c) les cyberattaques de la période précédente au niveau de l'Union, en fournissant une vue d'ensemble critique de la manière dont ces cyberattaques ont pu avoir un impact sur les flux transfrontaliers d'électricité;

d) l'état d'avancement général de la mise en œuvre des mesures de cybersécurité;

e) l'état d'avancement de la mise en œuvre des flux d'informations conformément aux articles 37 et 38;

f) la liste des informations ou les critères spécifiques de classification des informations conformément à l'article 46;

g) les risques recensés et soulignés qui peuvent découler d'une gestion non sécurisée de la chaîne d'approvisionnement;

h) les résultats et l'expérience accumulée issus des exercices de cybersécurité régionaux et transrégionaux organisés conformément à l'article 44;

i) une analyse de l'évolution des risques transfrontaliers globaux de cybersécurité dans le secteur de l'électricité depuis les dernières évaluations régionales des risques de cybersécurité;

j) toute autre information susceptible d'être utile pour identifier d'éventuelles améliorations du présent règlement ou la nécessité d'une révision du présent règlement ou de l'un de ses outils;

k) des informations agrégées et anonymisées sur les dérogations accordées en application de l'article 30, paragraphe 3.

3. Les entités énumérées à l'article 2, paragraphe 1, peuvent contribuer à l'élaboration du rapport d'évaluation complète des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité, dans le respect de la confidentialité des informations conformément à l'article 47. Les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, consultent ces entités à un stade précoce.

4. Le rapport d'évaluation complète des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité est soumis aux règles relatives à la protection de l'échange d'informations en application de l'article 46. Sans préjudice de l'article 10, paragraphe 4, et de l'article 47, paragraphe 4, le REGRT pour l'électricité et l'entité des GRD de l'Union publient une version publique de ce rapport qui ne contient pas d'informations susceptibles de causer des dommages aux entités énumérées à l'article 2, paragraphe 1. La version publique de ce rapport n'est publiée qu'avec l'accord du groupe de coopération SRI et du groupe de coordination pour l'électricité. Le REGRT pour l'électricité, en coordination avec l'entité des GRD de l'Union, est responsable de la compilation et de la publication de la version publique du rapport.

Article 24

Identification des entités à fort impact ou à impact critique

1. Chaque autorité compétente identifie, en utilisant l'ECII et les seuils de fort impact et d'impact critique inclus dans le rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union conformément à l'article 19, paragraphe 3, point b), les entités à fort impact ou à impact critique de son État membre qui participent aux processus à fort impact ou à impact critique à l'échelle de l'Union. Les autorités compétentes peuvent demander des informations à une entité de leur État membre pour déterminer les valeurs ECII de cette entité. Si l'ECII déterminé d'une entité est supérieur au seuil de fort impact ou d'impact critique, l'entité identifiée est inscrite sur la liste du rapport d'évaluation des risques de cybersécurité de l'État membre prévu à l'article 20, paragraphe 2.

2. Chaque autorité compétente identifie, en utilisant l'ECII et les seuils de fort impact et d'impact critique inclus dans le rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union conformément à l'article 19, paragraphe 3, point b), les entités à fort impact ou à impact critique établies hors de l'Union, dans la mesure où elles sont actives dans l'Union. Les autorités compétentes peuvent demander des informations à une entité établie hors de l'Union afin de déterminer les valeurs ECII pour cette entité.

3. Chaque autorité compétente peut désigner d'autres entités dans son État membre en tant qu'entités à fort impact ou à impact critique si les critères suivants sont remplis:

a) l'entité fait partie d'un groupe d'entités pour lesquelles il existe un risque important qu'elles soient touchées simultanément par une cyberattaque;

b) l'ECII agrégé pour le groupe d'entités est supérieur au seuil de fort impact ou d'impact critique.

4. Si une autorité compétente identifie des entités supplémentaires conformément au paragraphe 3, tous les processus de ces entités pour lesquels l'ECII agrégé au sein du groupe est supérieur au seuil de fort impact sont considérés comme des processus à fort impact, et tous les processus de ces entités pour lesquels l'ECII agrégé sur l'ensemble du groupe est supérieur aux seuils d'impact critique sont considérés comme des processus à impact critique.

5. Si une autorité compétente identifie des entités visées au paragraphe 3, point a), dans plus d'un État membre, elle en informe les autres autorités compétentes, le REGRT pour l'électricité et l'entité des GRD de l'Union. Le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, sur la base des informations reçues de toutes les autorités compétentes, fournit aux autorités compétentes une analyse de l'agrégation des entités de plus d'un État membre susceptibles de créer une perturbation distribuée des flux transfrontaliers d'électricité et d'entraîner une cyberattaque. Lorsqu'un groupe d'entités dans plusieurs États membres est identifié comme une agrégation dont l'ECII est supérieur au seuil de fort impact ou d'impact critique, toutes les autorités compétentes concernées identifient les entités de ce groupe comme étant des entités à fort impact ou à impact critique pour leur État membre respectif, sur la base de l'ECII agrégé pour le groupe des entités, et les entités identifiées sont énumérées dans le rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union.

6. Dans un délai de neuf mois à compter de la notification par le REGRT pour l'électricité et l'entité des GRD de l'Union du rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union conformément à l'article 19, paragraphe 5 et, en tout état de cause, au plus tard le 13 juin 2028, chaque autorité compétente notifie à chaque entité figurant sur la liste qu'elle a été recensée comme entité à fort impact ou à impact critique dans son État membre.

7. Lorsqu'un prestataire de services est déclaré à une autorité compétente comme étant un prestataire de services TIC critiques conformément à l'article 27, point c), cette autorité compétente le notifie aux autorités compétentes des États membres sur le territoire desquels se trouve le siège ou le représentant. Cette dernière autorité compétente informe le prestataire de services qu'il a été identifié comme étant un prestataire de services critique.

Article 25

Systèmes nationaux de vérification

1. Les autorités compétentes peuvent mettre en place un système national de vérification pour vérifier que les entités à impact critique recensées conformément à l'article 24, paragraphe 1, ont mis en œuvre le cadre législatif national qui est inclus dans la matrice de cartographie visée à l'article 34. Le système national de vérification peut être fondé sur une inspection effectuée par l'autorité compétente, sur des audits de sécurité indépendants ou sur des examens mutuels par les pairs réalisés par des entités à impact critique dans le même État membre et supervisés par l'autorité compétente.

2. Si une autorité compétente décide d'établir un programme national de vérification, elle veille à ce que la vérification soit effectuée conformément aux exigences suivantes:

a) toute partie qui procède à l'examen par les pairs, à l'audit ou à l'inspection est indépendante de l'entité à impact critique en cours de vérification et ne se trouve pas en situation de conflit d'intérêts;

b) le personnel chargé de l'examen par les pairs, de l'audit ou de l'inspection doit avoir une connaissance démontrable:

   i) de la cybersécurité dans le secteur de l'électricité;

   ii) des systèmes de gestion de la cybersécurité;

   iii) des principes de l'audit;

   iv) des évaluations des risques de cybersécurité:

   v) du cadre commun de cybersécurité dans le secteur de l'électricité;

   vi) du cadre législatif et réglementaire national et des normes européennes et internationales relevant du champ d'application de la vérification;

   vii) des processus d'impact critique dans le cadre de la vérification;

c) la partie qui effectue l'examen par les pairs, l'audit ou l'inspection dispose d'un délai suffisant pour mener à bien ces activités;

d) la partie qui procède à l'examen par les pairs, à l'audit ou à l'inspection prend les mesures appropriées pour protéger les informations qu'elle recueille au cours de la vérification, dans le respect de leur niveau de confidentialité;

e) les examens par les pairs, les audits ou les inspections sont effectués au moins une fois par an et couvrent au moins tous les trois ans tout le champ d'application de la vérification.

3. Si une autorité compétente décide d'établir un système national de vérification, elle indique chaque année à l'ACER la fréquence à laquelle elle a effectué des inspections dans le cadre de ce système.

Article 26

Gestion des risques de cybersécurité au niveau de l'entité

1. Chaque entité à fort impact ou à impact critique identifiée par les autorités compétentes conformément à l'article 24, paragraphe 1, assure la gestion des risques de cybersécurité pour tous ses actifs dans ses périmètres à fort impact ou à impact critique. Chaque entité à fort impact ou à impact critique effectue tous les trois ans une gestion des risques comportant les phases visées au paragraphe 2.

2. Chaque entité à fort impact ou à impact critique fonde sa gestion des risques de cybersécurité sur une approche qui vise à protéger ses réseaux et systèmes d'information et qui comprend les phases suivantes:

a) établissement du contexte;

b) gestion des risques de cybersécurité au niveau de l'entité;

c) traitement des risques de cybersécurité;

d) acceptation des risques de cybersécurité.

3. Au cours de la phase de mise en place du contexte, chaque entité à fort impact ou à impact critique:

a) définit le champ d'application de l'évaluation des risques de cybersécurité, y compris les processus à fort impact ou à impact critique recensés par le REGRT pour l'électricité et l'entité des GRD de l'Union, ainsi que d'autres processus susceptibles de cibler des cyberattaques à fort impact ou à impact critique sur les flux transfrontaliers d'électricité;

b) définit les critères d'évaluation des risques et d'acceptation des risques conformément à la matrice d'impact des risques que les entités et les autorités compétentes utilisent pour évaluer les risques de cybersécurité dans les méthodes d'évaluation des risques de cybersécurité au niveau de l'Union, au niveau régional et au niveau des États membres élaborées par le REGRT pour l'électricité et l'entité des GRD de l'Union conformément à l'article 19, paragraphe 2.

4. Au cours de la phase d'évaluation des risques de cybersécurité, chaque entité à fort impact ou à impact critique:

a) identifie les risques de cybersécurité en tenant compte:

i) de tous les actifs à l'appui des processus à fort impact ou à impact critique à l'échelle de l'Union, avec une évaluation de l'impact possible sur les flux transfrontaliers d'électricité si l'actif est compromis;

ii) les cybermenaces éventuelles, compte tenu des cybermenaces recensées dans le dernier rapport d'évaluation complète transfrontalière des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité prévu à l'article 23 et des menaces sur la chaîne d'approvisionnement;

iii) des vulnérabilités, y compris les vulnérabilités dans les systèmes hérités;

iv) des scénarios possibles de cyberattaque, y compris les cyberattaques portant atteinte à la sécurité opérationnelle du système électrique et perturbant les flux transfrontaliers d'électricité;

v) des évaluations et analyses des risques pertinentes effectuées au niveau de l'Union, y compris des évaluations coordonnées des risques liés aux chaînes d'approvisionnement critiques conformément à l'article 22 de la directive (UE) 2022/2555; et

vi) des contrôles existants mis en œuvre;

b) analyse la probabilité et les conséquences des risques de cybersécurité recensés au point a) et détermine le niveau de risque de cybersécurité sur la base de la matrice d'impact des risques utilisée pour évaluer les risques de cybersécurité dans les méthodes d'évaluation des risques de cybersécurité au niveau de l'Union, au niveau régional et au niveau des États membres, élaborées par le REGRT pour l'électricité et l'entité des GRD de l'Union conformément à l'article 19, paragraphe 2;

c) classe les actifs en fonction des conséquences possibles lorsque la cybersécurité est compromise et détermine le périmètre à fort impact ou à impact critique selon les étapes suivantes:

i) réalisation, pour tous les processus couverts par l'évaluation des risques de cybersécurité, d'une analyse d'impact sur les activités à l'aide de l'ECII;

ii) classification d'un processus comme «à fort impact» ou «à impact critique» si son ECII est supérieur au seuil de fort impact ou d'impact critique respectivement;

iii) détermination de tous les actifs à fort impact ou à impact critique comme étant les actifs nécessaires aux processus à fort impact ou à impact critique respectivement;

iv) définition des périmètres à fort impact ou à impact critique contenant respectivement tous les actifs à fort impact ou à impact critique, de manière que l'accès aux périmètres puisse être contrôlé;

d) évalue les risques de cybersécurité en les hiérarchisant au moyen de critères d'évaluation des risques et des critères d'acceptation des risques visés au paragraphe 3, point b).

5. Au cours de la phase de traitement des risques de cybersécurité, chaque entité à fort impact ou à impact critique établit un plan d'atténuation des risques au niveau de l'entité en sélectionnant des options de traitement des risques appropriées pour gérer les risques et identifier les risques résiduels.

6. Au cours de la phase d'acceptation des risques de cybersécurité, chaque entité à fort impact ou à impact critique décide d'accepter ou non le risque résiduel sur la base des critères d'acceptation des risques énoncés au paragraphe 3, point b).

7. Chaque entité à fort impact ou à impact critique doit enregistrer les actifs identifiés au paragraphe 1 dans un inventaire des actifs. Cet inventaire des actifs ne fait pas partie du rapport d'évaluation des risques.

8. L'autorité compétente peut inspecter les actifs de l'inventaire lors des inspections.

Article 27

Gestion des risques de cybersécurité au niveau de l'entité

Chaque entité à fort impact ou à impact critique communique à l'autorité compétente, dans un délai de 12 mois à compter de la notification de ces entités conformément à l'article 24, paragraphe 6, et par la suite tous les trois ans, un rapport contenant les informations suivantes:

1) une liste des contrôles sélectionnés pour le plan d'atténuation des risques au niveau de l'entité conformément à l'article 26, paragraphe 5, avec l'état d'avancement de la mise en œuvre de chaque contrôle;

2) pour chaque processus à fort impact ou à impact critique à l'échelle de l'Union, une estimation des risques de compromission de la confidentialité, de l'intégrité et de la disponibilité des informations et des actifs pertinents. L'estimation de ce risque est donnée conformément à la matrice d'impact des risques visée à l'article 19, paragraphe 2;

3) une liste des prestataires de services TIC critiques pour leurs processus d'impact critique.

CHAPITRE III

CADRE COMMUN DE CYBERSÉCURITÉ DANS LE SECTEUR DE L'ÉLECTRICITÉ

Article 28

Composition, fonctionnement et réexamen du cadre commun de cybersécurité dans le secteur de l'électricité

1. Le cadre commun de cybersécurité de l'électricité se compose des contrôles et du système de gestion de la cybersécurité suivants:

a) les contrôles minimaux de cybersécurité, élaborés conformément à l'article 29;

b) les contrôles avancés en matière de cybersécurité, développés conformément à l'article 29;

c) la matrice de cartographie, élaborée conformément à l'article 34, qui permet de cartographier les contrôles visés aux points a) et b) par rapport à une sélection de normes européennes et internationales et de cadres législatifs ou réglementaires nationaux;

d) le système de gestion de la cybersécurité mis en place conformément à l'article 32.

2. Toutes les entités à fort impact appliquent les contrôles minimaux de cybersécurité conformément au paragraphe 1, point a), dans leur périmètre à fort impact.

3. Toutes les entités à impact critique appliquent les contrôles avancés de cybersécurité conformément au paragraphe 1, point b), dans leur périmètre d'impact critique.

4. Dans un délai de 7 mois à compter de la présentation du premier projet de rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union conformément à l'article 19, paragraphe 4, le cadre commun de cybersécurité de l'électricité prévu au paragraphe 1 est complété par les contrôles de cybersécurité minimaux et avancés dans la chaîne d'approvisionnement définis conformément à l'article 33.

Article 29

Contrôles de cybersécurité minimaux et avancés

1. Dans un délai de 7 mois à compter de la soumission du premier projet de rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union conformément à l'article 19, paragraphe 4, les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, élaborent une proposition de contrôles de cybersécurité minimaux et avancés.

2. Dans un délai de 6 mois à compter de l'établissement de chaque rapport régional d'évaluation des risques de cybersécurité conformément à l'article 21, paragraphe 2, les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, proposent à l'autorité compétente une modification des contrôles de cybersécurité minimaux et avancés. La proposition sera faite conformément à l'article 8, paragraphe 10, et tiendra compte des risques recensés dans l'évaluation régionale des risques.

3. Les contrôles minimaux et avancés de cybersécurité sont vérifiables au moyen d'une participation à un schéma national de vérification conformément à la procédure définie à l'article 31 ou dans le cadre d'audits de sécurité réalisés par un tiers indépendant conformément aux exigences énumérées à l'article 25, paragraphe 2.

4. Les contrôles de cybersécurité initiaux minimaux et avancés définis conformément au paragraphe 1 sont fondés sur les risques recensés dans le rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union visé à l'article 19, paragraphe 5. Les contrôles de cybersécurité minimaux et avancés modifiés conformément au paragraphe 2 sont fondés sur le rapport régional d'évaluation des risques de cybersécurité prévu à l'article 21, paragraphe 2.

5. Les contrôles minimaux de cybersécurité comprennent des contrôles visant à protéger les informations échangées en application de l'article 46.

6. Dans un délai de 12 mois à compter de l'approbation des contrôles de cybersécurité minimaux et avancés conformément à l'article 8, paragraphe 5, ou après chaque mise à jour conformément à l'article 8, paragraphe 10, les entités énumérées à l'article 2, paragraphe 1, et identifiées en tant qu'entités à impact critique ou à fort impact conformément à l'article 24 appliquent, lors de la mise en place du plan d'atténuation des risques au niveau de l'entité conformément à l'article 26, paragraphe 5, les contrôles minimaux de cybersécurité dans le périmètre à fort impact et les contrôles de cybersécurité avancés dans le périmètre à impact critique.

Article 30

Dérogations aux contrôles minimaux et avancés de cybersécurité

1. Les entités énumérées à l'article 2, paragraphe 1, peuvent demander à l'autorité compétente concernée d'accorder une dérogation à leur obligation d'appliquer les contrôles de cybersécurité minimaux et avancés visés à l'article 29, paragraphe 6. L'autorité compétente peut accorder une telle dérogation pour l'un des motifs suivants:

a) dans des circonstances exceptionnelles, lorsque l'entité peut démontrer que les coûts liés à la mise en œuvre des contrôles de cybersécurité appropriés dépassent considérablement les avantages. L'ACER et le REGRT pour l'électricité, en coopération avec l'entité des GRD, peuvent élaborer conjointement des orientations pour estimer les coûts des contrôles de cybersécurité afin d'aider les entités;

b) lorsque l'entité fournit un plan de traitement des risques au niveau de l'entité qui atténue les risques de cybersécurité au moyen d'autres contrôles jusqu'à un niveau acceptable conformément aux critères d'acceptation des risques visés à l'article 26, paragraphe 3, point b).

2. Dans un délai de trois mois à compter de la réception de la demande visée au paragraphe 1, chaque autorité compétente décide s'il y a lieu d'accorder une dérogation aux contrôles de cybersécurité minimaux et avancés. Les dérogations aux contrôles de cybersécurité minimaux ou avancés sont accordées pour une durée maximale de trois ans, avec possibilité de renouvellement.

3. Les informations agrégées et anonymisées relatives aux dérogations accordées sont incluses en annexe du rapport d'évaluation complète des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité prévu à l'article 23. Le REGRT pour l'électricité et l'entité des GRD de l'Union mettent à jour conjointement la liste, si nécessaire.

Article 31

Vérification du cadre commun de cybersécurité dans le secteur de l'électricité

1. Au plus tard 24 mois après l'adoption des contrôles visés à l'article 28, paragraphe 1, points a), b), c) et la mise en place du système de gestion de la cybersécurité visée au même article, paragraphe 1, point d), chaque entité à impact critique identifiée conformément à l'article 24, paragraphe 1, est en mesure de démontrer, à la demande de l'autorité compétente, qu'elle respecte le système de gestion de la cybersécurité et les contrôles de cybersécurité minimaux ou avancés.

2. Chaque entité à impact critique s'acquitte de l'obligation visée au paragraphe 1 en se soumettant à des audits de sécurité effectués par des tiers indépendants conformément aux exigences énumérées à l'article 25, paragraphe 2, ou en participant à un système national de vérification conformément à l'article 25, paragraphe 1.

3. La vérification qu'une entité à impact critique respecte le système de gestion de la cybersécurité et les contrôles de cybersécurité minimaux ou avancés couvre tous les actifs se trouvant dans le périmètre d'impact critique de l'entité à impact critique.

4. La vérification qu'une entité à impact critique respecte le système de gestion de la cybersécurité et les contrôles de cybersécurité minimaux ou avancés est répétée au plus tard 36 mois après la fin de la première vérification, et par la suite tous les 3 ans.

5. Chaque entité à impact critique définie conformément à l'article 24 démontre qu'elle respecte les contrôles visés à l'article 28, paragraphe 1, points a), b), c) et la mise en place du système de gestion de la cybersécurité visée au même article, paragraphe 1, point d), en rendant compte des résultats de la vérification de la conformité à l'autorité compétente.

Article 32

Systèmes de gestion de la cybersécurité

1. Dans un délai de 24 mois à compter de la notification par l'autorité compétente qu'elle a été identifiée comme entité à fort impact ou à impact critique conformément à l'article 24, paragraphe 6, chaque entité à fort impact ou à impact critique met en place un système de gestion de la cybersécurité et le réexamine par la suite tous les trois ans afin:

a) de déterminer le champ d'application du système de gestion de la cybersécurité en tenant compte des interfaces et des dépendances avec d'autres entités;

b) de veiller à ce que tous ses cadres dirigeants soient informés des obligations légales pertinentes et contribuent activement à la mise en œuvre du système de gestion de la cybersécurité par des décisions en temps utile et des réactions rapides;

c) de veiller à ce que les ressources requises pour le système de management environnemental soient disponibles;

d) d'établir une politique de cybersécurité qui doit être documentée et communiquée au sein de l'entité et aux parties concernées par les risques pour la sécurité;

e) d'assigner et de communiquer les responsabilités associées aux rôles liés à la cybersécurité;

f) d'assurer la gestion des risques de cybersécurité au niveau de l'entité comme définie à l'article 26;

g) de déterminer et de fournir les ressources nécessaires à la mise en œuvre, à la maintenance et à l'amélioration continue du système de gestion de la cybersécurité, en tenant compte des compétences et des connaissances nécessaires concernant les ressources de cybersécurité;

h) de déterminer la communication interne et externe pertinente en matière de cybersécurité;

i) de créer, mettre à jour et contrôler les informations documentées relatives au système de gestion de la cybersécurité;

j) d'évaluer les performances et l'efficacité du système de gestion de la cybersécurité;

k) d'effectuer des audits internes à intervalles programmés pour s'assurer que le système de gestion de la cybersécurité est effectivement mis en œuvre et maintenu;

l) de contrôler la mise en œuvre du système de gestion de la cybersécurité à intervalles programmés; et de contrôler, en apportant les éventuelles corrections nécessaires, la conformité des ressources et des activités avec les politiques, procédures et lignes directrices du système de gestion de la cybersécurité.

2. Le champ d'application du système de gestion de la cybersécurité inclut tous les actifs appartenant au périmètre à fort impact ou à impact critique de l'entité à fort impact ou à impact critique.

3. Les autorités compétentes encouragent, sans imposer ni s'inscrire en faveur de l'utilisation d'un type particulier de technologie, l'utilisation de normes et spécifications européennes ou internationales relatives aux systèmes de gestion et pertinentes pour la sécurité des réseaux et des systèmes d'information.

Article 33

Contrôles minimaux et avancés de cybersécurité dans la chaîne d'approvisionnement

1. Dans un délai de 7 mois à compter de la soumission du premier projet de rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union conformément à l'article 19, paragraphe 4, les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, élaborent une proposition concernant les contrôles de cybersécurité minimaux et avancés dans la chaîne d'approvisionnement qui atténuent les risques de la chaîne d'approvisionnement recensés dans les évaluations des risques de cybersécurité à l'échelle de l'Union, en complétant les contrôles de cybersécurité minimaux et avancés élaborés conformément à l'article 29. Les contrôles minimaux et avancés de cybersécurité dans la chaîne d'approvisionnement sont élaborés en même temps que les contrôles minimaux et avancés de cybersécurité conformément à l'article 29. Les contrôles minimaux et avancés de cybersécurité dans la chaîne d'approvisionnement couvrent l'ensemble du cycle de vie de tous les produits TIC, services TIC et processus TIC à l'intérieur des périmètres à fort impact ou à impact critique d'une entité à fort impact ou à impact critique. Le groupe de coopération SRI est consulté lors de l'élaboration de la proposition concernant les contrôles minimaux et avancés de cybersécurité dans la chaîne d'approvisionnement.

2. Les contrôles minimaux de cybersécurité dans la chaîne d'approvisionnement consistent en des contrôles pour les entités à fort impact ou à impact critique qui:

a) incluent des recommandations pour l'acquisition de produits TIC, de services TIC et de processus TIC faisant référence au cahier des charges de cybersécurité, couvrant au moins:

   i) les vérifications des antécédents du personnel du fournisseur intervenant dans la chaîne d'approvisionnement et traitant des informations sensibles ou ayant accès aux actifs à fort impact ou à impact critique de l'entité. La vérification des antécédents peut comprendre une vérification de l'identité et des antécédents du personnel ou des contractants d'une entité conformément au droit national et aux procédures nationales ainsi qu'au droit pertinent et applicable de l'Union, notamment le règlement (UE) 2016/679 et la directive (UE) 2016/680 du Parlement européen et du Conseil ([18]). Les vérifications des antécédents sont proportionnées et strictement limitées à ce qui est nécessaire. Elles sont effectuées dans le seul but d'évaluer un risque potentiel pour la sécurité de l'entité concernée. Elles doivent être proportionnelles aux exigences commerciales, à la classification des informations auxquelles il s'agit d'accéder et aux risques perçus, et peuvent être effectuées par l'entité elle-même, par une entreprise externe effectuant un filtrage ou par l'intermédiaire d'une agence d'État;

   ii) les processus de conception, de développement et de production sécurisés et contrôlés de produits TIC, services TIC et processus TIC, en promouvant la conception et le développement de produits TIC, services TIC et processus TIC, qui comprennent des mesures techniques appropriées pour garantir la cybersécurité;

   iii) la conception de réseaux et de systèmes d'information dans lesquels les dispositifs ne sont pas jugés fiables, même lorsqu'ils se trouvent dans un périmètre sécurisé, nécessitent la vérification de toutes les demandes qu'ils reçoivent et appliquent le principe du moindre privilège;

   iv) l'accès du fournisseur aux actifs de l'entité;

([18]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

v) les obligations contractuelles incombant au fournisseur de protéger et de restreindre l'accès aux informations sensibles de l'entité;

vi) le cahier des charges de cybersécurité sous-jacent destiné aux sous-traitants du fournisseur;

vii) la traçabilité de l'application du cahier des charges de cybersécurité, depuis le développement jusqu'à la fourniture de produits TIC, de services TIC ou de processus TIC;

viii) l'assistance pour les mises à jour de sécurité tout au long de la durée de vie des produits TIC, services TIC ou processus TIC;

ix) le droit de vérifier la cybersécurité dans les processus de conception, de développement et de production du fournisseur; et

x) l'évaluation du profil de risque du fournisseur;

b) exigent de ces entités qu'elles tiennent compte des recommandations en matière de passation de marchés visées au point a) lorsqu'elles concluent des contrats avec des fournisseurs, des partenaires de collaboration et d'autres parties de la chaîne d'approvisionnement, couvrant les livraisons ordinaires de produits TIC, services TIC et processus TIC, ainsi que les événements et circonstances non sollicités tels que la résiliation et la transition de contrats en cas de négligence du partenaire contractuel;

c) exigent de ces entités qu'elles tiennent compte des résultats des évaluations coordonnées pertinentes des risques pour la sécurité des chaînes d'approvisionnement critiques effectuées conformément à l'article 22, paragraphe 1, de la directive (UE) 2022/2555;

d) incluent des critères de sélection de fournisseurs et de passation de marchés avec des fournisseurs qui peuvent satisfaire au cahier des charges de cybersécurité visées au point a) et qui possèdent un niveau de cybersécurité adapté aux risques de cybersécurité du produit TIC, service TIC ou processus TIC que le fournisseur livre;

e) incluent des critères visant à diversifier les sources d'approvisionnement pour les produits TIC, les services TIC et les processus TIC et réduire le risque d'enfermement propriétaire;

f) incluent des critères permettant de suivre, de réviser ou d'auditer régulièrement le cahier des charges de cybersécurité en ce qui concerne les processus opérationnels internes des fournisseurs tout au long du cycle de vie de chaque produit TIC, service TIC et processus TIC.

3. Pour le cahier des charges de cybersécurité figurant dans la recommandation relative aux marchés de cybersécurité visée au paragraphe 2, point a), les entités à fort impact ou à impact critique utilisent les principes de passation de marchés énoncés dans la directive 2014/24/UE du Parlement européen et du Conseil ([19]), conformément à l'article 35, paragraphe 4, ou définissent leur propre cahier des charges sur la base des résultats de l'évaluation des risques de cybersécurité au niveau de l'entité.

4. Les contrôles avancés de cybersécurité dans la chaîne d'approvisionnement comprennent des contrôles pour les entités à impact critique afin de vérifier, lors de la passation de marchés, que les produits TIC, services TIC et processus TIC qui seront utilisés comme actifs à impact critique satisfont au cahier des charges de cybersécurité. Le produit TIC, service TIC ou processus TIC est vérifié soit au moyen d'un schéma européen de certification de cybersécurité tel que visé à l'article 31, soit au moyen d'activités de vérification sélectionnées et organisées par l'entité. L'ampleur et la portée des activités de vérification sont suffisantes pour garantir que le produit TIC, service TIC ou processus TIC peut être utilisé pour atténuer les risques recensés dans l'évaluation des risques au niveau de l'entité. L'entité à impact critique documente les mesures prises pour réduire les risques identifiés.

5. Les contrôles minimaux et avancés de cybersécurité dans la chaîne d'approvisionnement s'appliquent à l'acquisition de produits TIC, services TIC et processus TIC pertinents. Les contrôles minimaux et avancés de cybersécurité de la chaîne d'approvisionnement s'appliquent aux procédures de passation de marchés dans les entités identifiées en tant qu'entités à impact critique ou à fort impact conformément à l'article 24 commençant six mois après l'adoption ou la mise à jour des contrôles de cybersécurité minimaux et avancés visés à l'article 29.

([19]) Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

6. Dans un délai de 6 mois à compter de l'établissement de chaque rapport régional d'évaluation des risques de cybersécurité conformément à l'article 21, paragraphe 2, les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, proposent à l'autorité compétente une modification des contrôles de cybersécurité minimaux et avancés. La proposition est faite conformément à l'article 8, paragraphe 10, et tient compte des risques recensés dans l'évaluation régionale des risques.

Article 34

Matrice de cartographie des contrôles de cybersécurité dans le secteur de l'électricité par rapport aux normes

1. Dans un délai de 7 mois à compter de la soumission du premier projet de rapport d'évaluation des risques de cybersécurité à l'échelle de l'Union conformément à l'article 19, paragraphe 4, les GRT, avec l'aide du REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union et en concertation avec l'ENISA, élaborent une proposition de matrice pour cartographier les contrôles visés à l'article 28, paragraphe 1, points a) et b), par rapport à une sélection de normes européennes et internationales ainsi qu'aux spécifications techniques pertinentes (ci-après la «matrice cartographique»). Le REGRT pour l'électricité et l'entité des GRD de l'Union documentent l'équivalence des différents contrôles avec les contrôles visés à l'article 28, paragraphe 1, points a) et b).

2. Les autorités compétentes peuvent fournir au REGRT pour l'électricité et à l'entité des GRD de l'Union une cartographie des contrôles visés à l'article 28, paragraphe 1, points a) et b), avec une référence aux cadres législatifs ou réglementaires nationaux correspondants, y compris les normes nationales pertinentes des États membres conformément à l'article 25 de la directive (UE) 2022/2555. Si l'autorité compétente d'un État membre fournit une telle cartographie, le REGRT pour l'électricité et l'entité des GRD de l'Union intègrent cette cartographie nationale dans la matrice cartographique.

3. Dans un délai de 6 mois à compter de l'établissement de chaque rapport régional d'évaluation des risques de cybersécurité conformément à l'article 21, paragraphe 2, les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union et en concertation avec l'ENISA, proposent à l'autorité compétente une modification de la matrice cartographique. La proposition est faite conformément à l'article 8, paragraphe 10, et tient compte des risques recensés dans l'évaluation régionale des risques.

CHAPITRE IV

RECOMMANDATIONS EN MATIÈRE DE PASSATION DE MARCHÉS DANS LE DOMAINE DE LA CYBERSÉCURITÉ

Article 35

Recommandations en matière de passation de marchés dans le domaine de la cybersécurité

1. Les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, élaborent, dans un programme de travail à établir et à mettre à jour chaque fois qu'un rapport régional d'évaluation des risques de cybersécurité est adopté, des séries de recommandations non contraignantes relatives aux marchés de cybersécurité que les entités à fort impact ou à impact critique peuvent utiliser comme base pour l'acquisition de produits TIC, de services TIC et de processus TIC dans les périmètres à fort impact ou à impact critique. Le programme de travail comporte les éléments suivants:

a) une description et une classification des types de produits TIC, services TIC et processus TIC utilisés par les entités à fort impact ou à impact critique dans le périmètre à fort impact ou à impact critique;

b) une liste des types de produits TIC, services TIC et processus TIC pour lesquels un ensemble de recommandations non contraignantes en matière de cybersécurité est élaboré sur la base des rapports régionaux pertinents d'évaluation des risques de cybersécurité et des priorités des entités à fort impact ou à impact critique.

2. Le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, fournit à l'ACER, dans un délai de 6 mois à compter de l'adoption ou de la mise à jour du rapport régional d'évaluation des risques de cybersécurité, un résumé de ce programme de travail.

3. Les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, s'efforcent de veiller à ce que les recommandations non contraignantes en matière de passation de marchés de cybersécurité élaborées sur la base de l'évaluation régionale pertinente des risques de cybersécurité soient similaires ou comparables entre les régions d'exploitation du réseau. Les séries de recommandations relatives aux marchés de cybersécurité couvrent au moins le cahier des charges visé à l'article 33, paragraphe 2, point a). Dans la mesure du possible, le cahier des charges est établi à partir de normes européennes ou internationales.

4. Les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, veillent à ce que les séries de recommandations relatives aux marchés de cybersécurité:

a) respectent les principes de passation des marchés énoncés dans la directive 2014/24/UE; et

b) soient compatibles avec les schémas européens de certification de cybersécurité les plus récents disponibles et tiennent compte de ces derniers, en rapport avec le produit TIC, le service TIC ou le processus TIC pertinent.

Article 36

Orientations sur l'utilisation des systèmes européens de certification de cybersécurité pour l'acquisition de produits TIC, services TIC et processus TIC

1. Les recommandations non contraignantes en matière de passation de marchés de cybersécurité élaborées en application de l'article 35 peuvent inclure des orientations sectorielles sur l'utilisation de schémas européens de certification de cybersécurité, chaque fois qu'un schéma approprié est disponible pour un type de produit TIC, service TIC ou processus TIC utilisé par des entités à impact critique, sans préjudice du cadre pour l'établissement de schémas européens de certification de cybersécurité conformément à l'article 46 du règlement (UE) 2019/881.

2. Les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, coopèrent étroitement avec l'ENISA pour fournir les orientations sectorielles incluses dans les recommandations non contraignantes en matière de passation de marchés de cybersécurité conformément au paragraphe 1.

CHAPITRE V

FLUX D'INFORMATIONS, CYBERATTAQUES ET GESTION DES CRISES

Article 37

Règles relatives au partage d'informations

1. Si une autorité compétente reçoit des informations relatives à une cyberattaque devant faire l'objet d'une déclaration, elle:

a) évalue le niveau de confidentialité de ces informations et informe l'entité du résultat de son évaluation dans les meilleurs délais et, au plus tard, dans les 24 heures suivant la réception des informations;

b) s'efforce de trouver toute autre cyberattaque similaire dans l'Union signalée à d'autres autorités compétentes, afin de corréler les informations reçues dans le cadre de la cyberattaque devant faire l'objet d'une déclaration avec les informations fournies dans le cadre d'autres cyberattaques et d'enrichir les informations existantes, de renforcer et de coordonner les réponses en matière de cybersécurité;

c) est responsable de la suppression des secrets d'affaires et de l'anonymisation des informations conformément aux règles nationales et de l'Union applicables;

d) communique les informations aux points de contact uniques nationaux, aux CSIRT et à toutes les autorités compétentes désignées conformément à l'article 4 dans d'autres États membres, dans les meilleurs délais et, au plus tard, 24 heures après la réception d'une cyberattaque devant faire l'objet d'une déclaration, et il fournit régulièrement des informations actualisées à ces autorités ou organismes;

e) diffuse les informations relatives à la cyberattaque, après anonymisation et suppression des secrets d'affaires conformément au paragraphe 1, point c), auprès des entités à impact critique ou à fort impact, dans les meilleurs délais et, au plus tard, 24 heures après avoir reçu les informations visées au paragraphe 1, point a), et il fournit régulièrement des informations actualisées permettant aux entités d'organiser efficacement leur défense;

f) peut demander à l'entité déclarante à fort impact ou à impact critique de diffuser davantage les informations relatives à la cyberattaque devant faire l'objet d'une déclaration de manière sécurisée auprès d'autres entités susceptibles d'être touchées, afin que le secteur de l'électricité ait connaissance de la situation et afin de prévenir la réalisation d'un risque pouvant conduire à un incident transfrontalier de cybersécurité dans le secteur de l'électricité;

g) communique à l'ENISA un rapport de synthèse, après anonymisation et suppression des secrets d'affaires, contenant les informations relatives à la cyberattaque.

2. Si un CSIRT a connaissance d'une vulnérabilité non corrigée activement exploitée, il:

a) en informe sans tarder l'ENISA par l'intermédiaire d'un canal d'échange d'informations sécurisé approprié, sauf disposition contraire prévue par d'autres actes de l'Union;

b) aide l'entité concernée afin qu'elle bénéficie, de la part du fabricant ou du fournisseur, d'une gestion efficace, coordonnée et rapide de la vulnérabilité activement exploitée, ou de mesures d'atténuation efficaces et efficientes;

c) communique les informations disponibles au vendeur et demande au fabricant ou au fournisseur, dans la mesure du possible, d'identifier une liste des CSIRT dans les États membres concernés par la vulnérabilité activement exploitée et qui en sont informés;

d) communique les informations disponibles aux CSIRT identifiés au point précédent, sur la base du principe du besoin d'en connaître;

e) partage, lorsqu'elles existent, des stratégies et mesures d'atténuation applicables à la vulnérabilité non corrigée activement exploitée.

3. Si une autorité compétente a connaissance d'une vulnérabilité non corrigée activement exploitée, elle:

a) partage, lorsqu'elles existent, des stratégies et mesures d'atténuation de la vulnérabilité non corrigée activement exploitée, en coordination avec les CSIRT;

b) communique les informations à un CSIRT de l'État membre dans lequel la vulnérabilité non corrigée activement exploitée a été signalée.

4. Si l'autorité compétente a connaissance d'une vulnérabilité non corrigée, sans qu'il soit prouvé qu'elle est déjà activement exploitée, elle se concerte sans tarder avec le CSIRT aux fins de la divulgation coordonnée de cette vulnérabilité conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555.

5. Si un CSIRT reçoit des informations relatives aux cybermenaces de la part d'une ou de plusieurs entités à fort impact ou à impact critique en application de l'article 38, paragraphe 6, il diffuse ces informations ou toute autre information importante pour prévenir, détecter ou atténuer le risque y afférent auprès des entités à impact critique ou à fort impact dans son État membre et, s'il y a lieu, auprès de tous les CSIRT concernés et de son point de contact unique national, dans les meilleurs délais et, au plus tard, quatre heures après avoir reçu les informations.

6. Si une autorité compétente a connaissance d'informations relatives à des cybermenaces émanant d'une ou de plusieurs entités à fort impact ou à impact critique, elle transmet ces informations au CSIRT aux fins du paragraphe 5.

7. Les autorités compétentes peuvent déléguer en tout ou en partie les responsabilités visées aux paragraphes 3 et 4 concernant une ou plusieurs entités à fort impact ou à impact critique actives dans plus d'un État membre à une autre autorité compétente de l'un de ces États membres, à la suite d'un accord entre les autorités compétentes concernées.

8. Les GRT, avec l'aide du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'Union, élaborent une méthode/échelle de classification des cyberattaques pour le 13 juin 2025. Les GRT, avec l'aide du REGRT pour l'électricité et de l'entité des GRD de l'Union, peuvent demander aux autorités compétentes de consulter l'ENISA et leurs autorités compétentes en matière de cybersécurité afin d'aider à l'élaboration d'une telle échelle de classification. La méthode prévoit la classification de la gravité d'une cyberattaque selon 5 niveaux, les deux niveaux les plus hauts étant «élevée» et «critique». La classification est fondée sur l'évaluation des paramètres suivants:

a) l'impact potentiel compte tenu des actifs et des périmètres exposés, déterminé conformément à l'article 26, paragraphe 4, point c); et

b) la gravité de la cyberattaque.

9. Au plus tard le 13 juin 2026, le REGRT pour l'électricité, en collaboration avec l'entité des GRD de l'Union, réalise une étude de faisabilité afin d'évaluer la possibilité de mettre au point un outil commun permettant à toutes les entités de partager des informations avec les autorités nationales compétentes, et les coûts financiers nécessaires à cette mise au point.

10. L'étude de faisabilité examinera la possibilité, pour un tel outil commun:

a) de soutenir les entités à impact critique ou à fort impact en leur communiquant des informations en matière de sécurité pertinentes pour les opérations de flux transfrontaliers d'électricité, telles que le signalement en temps quasi réel des cyberattaques, les alertes précoces liées à des questions de cybersécurité et les vulnérabilités non divulguées d'équipements utilisés dans le système électrique;

b) d'être entretenu dans un environnement approprié et hautement fiable;

c) de permettre la collecte de données auprès d'entités à impact critique ou à fort impact et de faciliter le retrait des informations confidentielles et l'anonymisation des données ainsi que leur diffusion rapide auprès des entités à impact critique et à fort impact.

11. Le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union:

a) consulte l'ENISA et le groupe de coopération SRI, les points de contact uniques nationaux et les représentants des principales parties prenantes lors de l'évaluation de la faisabilité;

b) présente les résultats de l'étude de faisabilité à l'ACER et au groupe de coopération SRI.

12. Le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, peut analyser et faciliter les initiatives proposées par les entités à impact critique ou à fort impact afin d'évaluer et de tester ces outils de partage d'informations.

Article 38

Rôle des entités à fort impact ou à impact critique en ce qui concerne le partage d'informations

1. Chaque entité à fort impact ou à impact critique:

a) établit, pour tous les actifs relevant de son périmètre de cybersécurité déterminé conformément à l'article 26, paragraphe 4, point c), au moins les capacités CSOC permettant:

   i) de veiller à ce que les réseaux et les systèmes et applications d'information pertinents fournissent des journaux de sécurité aux fins de la surveillance de la sécurité afin de permettre la détection des anomalies et de recueillir des informations sur les cyberattaques;

   ii) d'assurer la surveillance de la sécurité, y compris en détectant les intrusions et en évaluant les vulnérabilités des réseaux et des systèmes d'information;

   iii) d'analyser et, si nécessaire, de prendre toutes les mesures requises sous sa responsabilité et sa capacité de protection de l'entité;

   iv) de participer à la collecte et au partage d'informations décrits dans le présent article;

b) a le droit d'acquérir tout ou partie de ces capacités visées au point a) par l'intermédiaire des fournisseurs de services de sécurité gérés. Les entités à impact critique ou à fort impact restent responsables des fournisseurs de services de sécurité gérés et supervisent leurs efforts;

c) désigne un point de contact unique au niveau de l'entité aux fins du partage d'informations.

2. L'ENISA peut publier des orientations non contraignantes sur la mise en place de ces capacités ou la sous-traitance du service aux fournisseurs de services de sécurité gérés, dans le cadre de la tâche définie à l'article 6, paragraphe 2, du règlement (UE) 2019/881.

3. Chaque entité à impact critique et à fort impact communique les informations pertinentes relatives à une cyberattaque devant faire l'objet d'une déclaration à ses CSIRT et à son autorité compétente dans les meilleurs délais et, au plus tard, quatre heures après avoir appris que l'incident doit faire l'objet d'une déclaration.

4. Les informations liées à une cyberattaque sont considérées comme devant faire l'objet d'une déclaration lorsque l'évaluation de la cyberattaque par l'entité concernée conclut à une gravité allant de «élevée» à «critique» selon la méthode/échelle de classification des cyberattaques établie conformément à l'article 37, paragraphe 8. Le point de contact unique au niveau de l'entité désigné conformément au paragraphe 1, point c), transmet la classification des incidents.

5. Lorsque des entités à impact critique ou à fort impact notifient à un CSIRT des informations pertinentes relatives à des vulnérabilités non corrigées activement exploitées, ce dernier peut relayer ces informations à son autorité compétente. Compte tenu du niveau de sensibilité des informations notifiées, le CSIRT peut ne pas les communiquer ou en retarder la transmission pour des raisons motivées liées à la cybersécurité.

6. Chaque entité à impact critique ou à fort impact fournit sans tarder à ses CSIRT toute information relative à une cybermenace devant faire l'objet d'une déclaration susceptible d'avoir un effet transfrontalier. Les informations relatives à une cybermenace sont considérées comme devant faire l'objet d'une déclaration lorsqu'au moins l'une des conditions suivantes est remplie:

a) elles constituent pour d'autres entités à impact critique ou à fort impact des éléments pertinents pour la prévention, la détection, la gestion ou l'atténuation de l'impact du risque;

b) les techniques, tactiques et procédures identifiées utilisées dans le contexte d'une attaque donnent lieu à des informations telles que des adresses URL ou IP compromises, des hachages ou tout autre attribut utile pour contextualiser et corréler l'attaque;

c) une cybermenace peut être évaluée plus avant et contextualisée avec des informations supplémentaires communiquées par des fournisseurs de services ou des tiers ne relevant pas du présent règlement.

7. Chaque entité à impact critique et entité à fort impact précise, lors du partage d'informations en application du présent article, les éléments suivants:

a) que les informations sont soumises en application du présent règlement;

b) si les informations concernent:

   i) une cyberattaque devant faire l'objet d'une déclaration visée au paragraphe 3;

   ii) des vulnérabilités non corrigées activement exploitées et non connues du public visées au paragraphe 4;

   iii) une cyberattaque devant faire l'objet d'une déclaration visée au paragraphe 5;

c) dans le cas d'une cyberattaque devant faire l'objet d'une déclaration, le niveau de la cyberattaque conformément à la méthode/échelle de classification des cyberattaques prévue à l'article 37, paragraphe 8, et les informations conduisant à cette classification, y compris au moins la gravité de la cyberattaque.

8. Lorsqu'une entité à impact critique ou à fort impact notifie un incident important conformément à l'article 23 de la directive (UE) 2022/2555 et que le signalement d'incident au titre dudit article contient des informations pertinentes requises par le paragraphe 3 du présent article, le signalement de l'entité en application de l'article 23, paragraphe 1, de ladite directive constitue un signalement d'informations au titre du paragraphe 3 du présent article.

9. Chaque entité à impact critique ou à fort impact fait rapport à son autorité compétente ou au CSIRT en identifiant clairement les informations spécifiques qui ne doivent être communiquées qu'à l'autorité compétente ou au CSIRT dans les cas où le partage d'informations pourrait être à l'origine d'une cyberattaque. Chaque entité à impact critique ou à fort impact a le droit de fournir une version non confidentielle des informations au CSIRT compétent.

Article 39

Détection des cyberattaques et traitement des informations connexes

1. Les entités à impact critique ou à fort impact développent les capacités nécessaires pour gérer les cyberattaques détectées avec le soutien nécessaire de l'autorité compétente concernée, du REGRT pour l'électricité et de l'entité des GRD de l'Union. Les entités à impact critique ou à fort impact peuvent être soutenues par le CSIRT désigné dans leur État membre respectif dans le cadre de la mission confiée aux CSIRT par l'article 11, paragraphe 5, point a), de la directive (UE) 2022/2555. Les entités à impact critique ou à fort impact mettent en œuvre des processus efficaces de détection et de classification des cyberattaques qui affecteront ou sont susceptibles d'affecter les flux transfrontaliers d'électricité, afin de réduire au minimum leurs effets.

2. Si une cyberattaque a un impact sur les flux transfrontaliers d'électricité, les points de contact uniques au niveau de l'entité des entités à impact critique ou à fort impact coopèrent pour partager des informations entre elles, sous la coordination de l'autorité compétente de l'État membre dans lequel la cyberattaque a été signalée pour la première fois.

3. Les entités à impact critique ou à fort impact:

a) veillent à ce que leur propre point de contact unique au niveau de l'entité ait accès, sur la base du besoin d'en connaître, aux informations qu'il a reçues du point de contact unique national par l'intermédiaire de son autorité compétente;

b) sauf si cela a déjà été fait en application de l'article 3, paragraphe 4, de la directive (UE) 2022/2555, notifient à l'autorité compétente de l'État membre dans lequel elles sont établies et au point de contact unique national une liste de leurs points de contact uniques en matière de cybersécurité au niveau de l'entité:

   i) dont l'autorité compétente et le point de contact unique national peuvent s'attendre à recevoir des informations sur des cyberattaques devant faire l'objet d'une déclaration;

   ii) auxquels les autorités compétentes et les points de contact uniques nationaux peuvent être amenés à fournir des informations;

c) établissent des procédures de gestion des cyberattaques, y compris les rôles et responsabilités, les tâches et les réactions, sur la base de l'évolution observable de la cyberattaque dans les périmètres à impact critique ou à fort impact;

d) testent les procédures globales de gestion des cyberattaques au moins une fois par an sur au moins un scénario affectant directement ou indirectement les flux transfrontaliers d'électricité. Ce test annuel peut être effectué par des entités à impact critique ou à fort impact au cours des exercices réguliers prévus à l'article 43. Toute activité de réaction aux cyberattaques en direct ayant une conséquence classée au moins à l'échelle 2, conformément à la méthode/échelle de classification des cyberattaques prévue à l'article 37, paragraphe 8 et ayant une cause profonde liée à la cybersécurité, peut servir de test annuel du plan de réaction aux cyberattaques.

4. Les tâches visées au paragraphe 1 peuvent également être déléguées par les États membres aux centres de coordination régionaux conformément à l'article 37, paragraphe 2, du règlement (UE) 2019/943.

Article 40

Gestion de crises

1. Lorsque l'autorité compétente établit qu'une crise électrique est liée à une cyberattaque ayant un impact sur plusieurs États membres, les autorités compétentes des États membres touchés, les ANC-CS, les ANC-PR et les autorités de gestion des crises de cybersécurité (SRI) des États membres touchés créent conjointement un groupe ad hoc de coordination de crise transfrontalière.

2. Le groupe ad hoc de coordination de crise transfrontalière:

a) coordonne la recherche et la diffusion efficaces de toutes les informations pertinentes en matière de cybersécurité auprès des entités participant au processus de gestion de crise;

b) organise la communication entre toutes les entités touchées par la crise et les autorités compétentes, afin de réduire les chevauchements et d'accroître l'efficacité des analyses et des réponses techniques pour remédier aux crises électriques simultanées ayant une cause profonde en matière de cybersécurité;

c) fournit aux entités touchées par l'incident, en coopération avec les CSIRT compétents, l'expertise requise, y compris des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation;

d) notifie et fournit régulièrement à la Commission et au groupe de coordination pour l'électricité des informations actualisées sur l'état de l'incident, conformément aux principes de protection énoncés à l'article 46;

e) demande conseil aux autorités, agences ou entités concernées qui pourraient contribuer à atténuer la crise électrique.

3. Lorsque la cyberattaque remplit, ou que l'on s'attend à ce qu'elle remplisse, les critères d'un incident de cybersécurité majeur, le groupe ad hoc de coordination de crise transfrontalière informe immédiatement les autorités nationales de gestion des crises de cybersécurité conformément à l'article 9, paragraphe 1, de la directive (UE) 2022/2555 dans les États membres touchés par l'incident, ainsi que la Commission et EU CyCLONe. Dans une telle situation, le groupe ad hoc de coordination transfrontalière en cas de crise assiste EU CyCLONe en ce qui concerne les spécificités sectorielles.

4. Les entités à impact critique ou à fort impact développent et ont à leur disposition des capacités, des lignes directrices internes, des plans de préparation et du personnel pour participer à la détection et à l'atténuation des crises transfrontalières. L'entité à impact critique ou à fort impact touchée par une crise électrique simultanée enquête sur la cause profonde de cette crise, en coopération avec son autorité compétente, afin de déterminer dans quelle mesure la crise est liée à une cyberattaque.

5. Les tâches visées au paragraphe 4 peuvent également être déléguées par les États membres aux centres de coordination régionaux conformément à l'article 37, paragraphe 2, du règlement (UE) 2019/943.

Article 41

Plans de gestion des crises de cybersécurité et de réaction à ces crises

1. Dans un délai de 24 mois à compter de la notification à l'ACER du rapport d'évaluation des risques à l'échelle de l'Union, l'ACER élabore, en étroite coopération avec l'ENISA, le REGRT pour l'électricité, l'entité des GRD de l'Union, les ANC-CS, les autorités compétentes, les ANC-PR, les ARN et les autorités nationales de gestion des crises de cybersécurité (SRI), un plan de gestion des crises de cybersécurité et de réaction à ces crises au niveau de l'Union pour le secteur de l'électricité.

2. Dans les 12 mois suivant l'élaboration par l'ACER du plan de gestion des crises de cybersécurité et de réaction à ces crises au niveau de l'Union pour le secteur de l'électricité conformément au paragraphe 1, chaque autorité compétente élabore un plan national de gestion des crises de cybersécurité et de réaction à ces crises pour les flux transfrontaliers d'électricité en tenant compte du plan de gestion des crises de cybersécurité au niveau de l'Union et du plan national de préparation aux risques établi conformément à l'article 10 du règlement (UE) 2019/941. Ce plan est en cohérence avec le plan de réaction aux incidents de cybersécurité majeurs et aux crises conformément à l'article 9, paragraphe 4, de la directive (UE) 2022/2555. L'autorité compétente se coordonne avec les entités à impact critique et à fort impact et avec l'ANC-PR dans son État membre.

3. Le plan national de réaction aux incidents et crises de cybersécurité majeurs requis conformément à l'article 9, paragraphe 4, de la directive (UE) 2022/2555 est considéré comme un plan national de gestion des crises de cybersécurité au sens du présent article s'il comprend des dispositions relatives à la gestion des crises et à la réaction à celles-ci pour les flux transfrontaliers d'électricité.

4. Les tâches énumérées aux paragraphes 1 et 2 peuvent également être déléguées par les États membres aux centres de coordination régionaux conformément à l'article 37, paragraphe 2, du règlement (UE) 2019/943.

5. Les entités à impact critique ou à fort impact veillent à ce que leurs processus de gestion des crises de cybersécurité:

a) comprennent des procédures compatibles de traitement des incidents de cybersécurité transfrontaliers, tel que défini à l'article 6, point 8), de la directive (UE) 2022/2555, formellement intégrées dans leurs plans de gestion des crises;

b) fassent partie des activités générales de gestion des crises.

6. Dans un délai de 12 mois à compter de la notification des entités à fort impact ou à impact critique conformément à l'article 24, paragraphe 6, et par la suite tous les trois ans, les entités à impact critique ou à fort impact élaborent un plan de gestion de crise au niveau de l'entité pour une crise liée à la cybersécurité, qui est inclus dans leurs plans généraux de gestion des crises. Il comprend au moins les éléments suivants:

a) les règles de déclaration de la crise visées à l'article 14, paragraphes 2 et 3, du règlement (UE) 2019/941;

b) des rôles et responsabilités clairs en matière de gestion des crises, y compris le rôle d'autres entités à impact critique ou à fort impact;

c) des coordonnées actualisées ainsi que des règles de communication et de partage d'informations en situation de crise, y compris la connexion aux CSIRT.

7. Les mesures de gestion des crises prévues à l'article 21, paragraphe 2, point c), de la directive (UE) 2022/2555 sont considérées comme un plan de gestion des crises au niveau de l'entité pour le secteur de l'électricité au titre du présent article si elles incluent toutes les exigences énumérées au paragraphe 6.

8. Les plans de gestion des crises sont testés au cours des exercices de cybersécurité visés aux articles 43, 44 et 45.

9. Les entités à impact critique ou à fort impact incluent leurs plans de gestion des crises au niveau de l'entité dans leurs plans de continuité des activités pour les processus à impact critique ou à fort impact. Les plans de gestion des crises au niveau de l'entité comprennent:

a) des processus en fonction de la disponibilité, de l'intégrité et de la fiabilité des services informatiques;

b) tous les sites de continuité des activités, y compris les emplacements du matériel et des logiciels;

c) tous les rôles et responsabilités internes liés aux processus de continuité des activités.

10. Les entités à impact critique ou à fort impact mettent à jour leurs plans de gestion de crise au niveau de l'entité au moins tous les trois ans et chaque fois que cela est nécessaire.

11. L'ACER met à jour le plan de gestion des crises de cybersécurité et de réaction à ces crises au niveau de l'Union pour le secteur de l'électricité élaboré conformément au paragraphe 1 au moins tous les trois ans et chaque fois que cela est nécessaire.

12. Chaque autorité compétente met à jour le plan national de gestion des crises de cybersécurité et de réaction à ces crises pour les flux transfrontaliers d'électricité élaboré conformément au paragraphe 2 au moins tous les trois ans et chaque fois que cela est nécessaire.

13. Les entités à impact critique ou à fort impact testent leurs plans de continuité des activités au moins une fois tous les trois ans ou après des changements majeurs dans un processus à impact critique. Les résultats des essais du plan de continuité des activités sont documentés. Les entités à impact critique ou à fort impact peuvent inclure le test de leur plan de continuité des activités dans les exercices de cybersécurité.

14. Les entités à impact critique ou à fort impact mettent à jour leur plan de continuité des activités chaque fois que cela est nécessaire et au moins une fois tous les trois ans en tenant compte des résultats du test.

15. Si un test révèle des lacunes dans le plan de continuité des activités, l'entité à impact critique ou à fort impact corrige ces défaillances dans les 180 jours civils suivant le test et procède à un nouveau test afin de prouver que les mesures correctives sont efficaces.

16. Lorsqu'une entité à impact critique ou à fort impact ne peut corriger les défaillances dans un délai de 180 jours civils, elle en indique les raisons dans le rapport à fournir à son autorité compétente conformément à l'article 27.

Article 42

Capacités d'alerte précoce en matière de cybersécurité pour le secteur de l'électricité

1. Les autorités compétentes coopèrent avec l'ENISA pour développer les capacités d'alerte précoce en matière de cybersécurité dans le domaine de l'électricité (ECEAC) dans le cadre de l'assistance aux États membres conformément à l'article 6, paragraphe 2, et à l'article 7 du règlement (UE) 2019/881.

2. L'ECEAC permet à l'ENISA, lorsqu'elle exécute les tâches énumérées à l'article 7, paragraphe 7, du règlement (UE) 2019/881:

a) de recueillir des informations partagées sur une base volontaire auprès:

   i) des CSIRT et des autorités compétentes;

   ii) des entités visées à l'article 2 du présent règlement;

   iii) de toute autre entité désireuse de partager des informations pertinentes sur une base volontaire;

b) d'évaluer et de classer les informations recueillies;

c) d'évaluer les informations auxquelles l'ENISA a accès pour déterminer les conditions de risque de cybersécurité et les indicateurs pertinents pour certains aspects des flux transfrontaliers d'électricité;

d) de recenser les conditions et les indicateurs fréquemment corrélés avec les cyberattaques dans le secteur de l'électricité;

e) de définir si des analyses complémentaires et des mesures préventives doivent être prises, au moyen d'une évaluation et d'un recensement des facteurs de risque;

f) d'informer les autorités compétentes des risques recensés et des mesures préventives spécifiques recommandées aux entités concernées;

g) d'informer toutes les entités concernées énumérées à l'article 2 des résultats de l'évaluation des informations effectuée conformément aux points b), c) et d) du présent paragraphe;

h) d'inclure périodiquement les informations pertinentes dans le rapport de situation technique publié conformément à l'article 7, paragraphe 6, du règlement (UE) 2019/881;

i) de tirer des informations recueillies, dans la mesure du possible, des données utiles indiquant une atteinte à la sécurité ou une cyberattaque potentielle («indicateurs de compromission»).

3. Les CSIRT diffusent sans tarder les informations reçues de l'ENISA auprès des entités concernées, dans le cadre de leurs tâches définies à l'article 11, paragraphe 3, point b), de la directive (UE) 2022/2555.

4. L'ACER contrôle l'efficacité de l'ECEAC. L'ENISA assiste l'ACER en fournissant toutes les informations nécessaires, conformément à l'article 6, paragraphe 2, et à l'article 7, paragraphe 1, du règlement (UE) 2019/881. L'analyse de cette activité de surveillance fait partie de la surveillance prévue à l'article 12 du présent règlement.

CHAPITRE VI

CADRE D'EXERCICES DE CYBERSÉCURITÉ DANS LE SECTEUR DE L'ÉLECTRICITÉ

Article 43

Exercices de cybersécurité au niveau des entités et des États membres

1. Au plus tard le 31 décembre de l'année suivant la notification des entités à impact critique, et par la suite tous les trois ans, chaque entité à impact critique réalise un exercice de cybersécurité comprenant un ou plusieurs scénarios de cyberattaques affectant directement ou indirectement les flux transfrontaliers d'électricité et liés aux risques recensés lors des évaluations des risques de cybersécurité au niveau des États membres et des entités conformément à l'article 20 et à l'article 27.

2. Par dérogation au paragraphe 1, l'ANC-PR, après consultation de l'autorité compétente et de l'autorité de gestion des crises de cybersécurité concernée, désignée ou établie dans la directive (UE) 2022/2555, conformément à l'article 9, peut décider d'organiser un exercice de cybersécurité au niveau de l'État membre, comme décrit au paragraphe 1, au lieu de procéder à l'exercice de cybersécurité au niveau de l'entité. À cet égard, l'autorité compétente informe:

a) toutes les entités à impact critique de son État membre, l'ARN, les CSIRT et l'autorité nationale compétente en matière de cybersécurité au plus tard le 30 juin de l'année précédant l'exercice de cybersécurité au niveau de l'entité;

b) chaque entité qui participe à l'exercice de cybersécurité au niveau des États membres, au plus tard 6 mois avant la date à laquelle l'exercice doit avoir lieu.

3. L'autorité nationale compétente en matière de préparation aux risques, avec le soutien technique de ses CSIRT, organise l'exercice de cybersécurité décrit au paragraphe 2 au niveau de l'État membre, de manière indépendante ou dans le cadre d'un autre exercice de cybersécurité dans cet État membre. Afin de pouvoir regrouper ces exercices, l'autorité nationale compétente en matière de préparation aux risques peut reporter d'un an l'exercice de cybersécurité au niveau des États membres prévu au paragraphe 1.

4. Les exercices de cybersécurité au niveau de l'entité et des États membres sont compatibles avec les cadres nationaux de gestion des crises de cybersécurité conformément à l'article 9, paragraphe 4, point d), de la directive (UE) 2022/2555.

5. Au plus tard le 31 décembre 2026, et par la suite tous les trois ans, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, met à disposition un modèle de scénario d'exercice pour effectuer les exercices de cybersécurité au niveau de l'entité et de l'État membre prévus au paragraphe 1. Ce modèle tient compte des résultats de l'évaluation des risques de cybersécurité la plus récente au niveau de l'entité et des États membres et comprend des critères de réussite clés. Le REGRT pour l'électricité et l'entité des GRD de l'Union associent l'ACER et l'ENISA à l'élaboration de ce modèle.

Article 44

Exercices régionaux ou transrégionaux de cybersécurité

1. Au plus tard le 31 décembre 2029 et par la suite tous les trois ans, dans chaque région d'exploitation du réseau, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, organise un exercice régional de cybersécurité. Les entités à impact critique dans la région d'exploitation du réseau participent à l'exercice régional de cybersécurité. Le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, peut organiser dans le même délai, au lieu d'un exercice régional de cybersécurité, un exercice de cybersécurité transrégional dans plus d'une région exploitant un réseau. L'exercice devrait tenir compte d'autres évaluations des risques de cybersécurité et des scénarios existants élaborés au niveau de l'Union.

2. L'ENISA soutient le REGRT pour l'électricité et l'entité des GRD de l'Union dans la préparation et l'organisation de l'exercice de cybersécurité au niveau régional ou transrégional.

3. Le REGRT pour l'électricité, en coordination avec l'entité des GRD de l'Union, informe les entités à impact critique qui participent à l'exercice régional ou transrégional de cybersécurité six mois avant la réalisation de l'exercice.

4. L'organisateur d'un exercice régulier de cybersécurité au niveau de l'Union conformément à l'article 7, paragraphe 5, du règlement (UE) 2019/881, ou de tout exercice obligatoire de cybersécurité lié au secteur de l'électricité dans le même périmètre géographique, peut inviter le REGRT pour l'électricité et l'entité des GRD de l'Union à participer. Dans de tels cas, l'obligation prévue au paragraphe 1 ne s'applique pas, à condition que toutes les entités à impact critique dans la région d'exploitation du réseau participent au même exercice.

5. Si le REGRT pour l'électricité et l'entité des GRD de l'Union participent à un exercice de cybersécurité visé au paragraphe 4, ils peuvent reporter d'un an l'exercice régional ou transrégional de cybersécurité prévu au paragraphe 1.

6. Au plus tard le 31 décembre 2027, et par la suite tous les trois ans, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, met à disposition un modèle de scénario d'exercice pour effectuer les exercices régionaux ou transrégionaux de cybersécurité. Ce modèle tient compte des résultats de l'évaluation des risques de cybersécurité la plus récente au niveau régional et comprend des critères de réussite clés. Le REGRT pour l'électricité consulte la Commission et peut demander conseil à l'ACER, à l'ENISA et au Centre commun de recherche sur l'organisation et l'exécution des exercices de cybersécurité régionaux et transrégionaux.

Article 45

Résultats des exercices de cybersécurité aux niveaux de l'entité, des États membres, régionaux ou transrégionaux

1. À la demande d'une entité à impact critique, les fournisseurs de services critiques participent aux exercices de cybersécurité visés à l'article 43, paragraphes 1 et 2, et à l'article 44, paragraphe 1, lorsqu'ils fournissent des services à l'entité à impact critique dans le domaine correspondant au champ d'application de l'exercice de cybersécurité concerné.

2. Les organisateurs des exercices de cybersécurité visés à l'article 43, paragraphes 1 et 2, et à l'article 44, paragraphe 1, avec l'avis de l'ENISA s'ils en font la demande et conformément à l'article 7, paragraphe 5, du règlement (UE) 2019/881, analysent et finalisent l'exercice de cybersécurité concerné au moyen d'un rapport résumant les enseignements, adressé à tous les participants. Le rapport contient:

a) les scénarios d'exercice, les rapports de réunion, les principales positions, les réussites et les enseignements tirés à tous les niveaux de la chaîne de valeur de l'électricité;

b) l'indication, le cas échéant, que les principaux critères de réussite ont été remplis.

c) une liste de recommandations à l'intention des entités participant à l'exercice de cybersécurité concerné afin que celles-ci corrigent, adaptent ou modifient les processus, procédures, modèles de gouvernance associés en matière de cybersécurité et tout engagement contractuel existant avec des fournisseurs de services critiques.

3. À la demande du réseau des CSIRT, du groupe de coopération SRI ou d'EU CyCLONe, les organisateurs des exercices de cybersécurité mentionnés à l'article 43, paragraphes 1 et 2, et à l'article 44, paragraphe 1, partagent les résultats de l'exercice de cybersécurité concerné. Les organisateurs communiquent à chaque entité participant aux exercices les informations visées au paragraphe 2, points a) et b), du présent article. Les organisateurs communiquent la liste des recommandations visées audit paragraphe, point c), exclusivement aux entités visées dans les recommandations.

4. Les organisateurs des exercices de cybersécurité visés à l'article 43, paragraphes 1 et 2, et à l'article 44, paragraphe 1, assurent, avec les entités participant aux exercices, un suivi régulier de la mise en œuvre des recommandations conformément au paragraphe 2, point c), du présent article.

CHAPITRE VII

PROTECTION DE L'INFORMATION

Article 46

Principes de protection des informations échangées

1. Les entités énumérées à l'article 2, paragraphe 1, veillent à ce que les informations fournies, reçues, échangées ou transmises au titre du présent règlement ne soient accessibles que sur la base du besoin d'en connaître et conformément aux règles nationales et de l'Union applicables en matière de sécurité des informations.

2. Les entités énumérées à l'article 2, paragraphe 1, veillent à ce que les informations fournies, reçues, échangées ou transmises au titre du présent règlement soient traitées et suivies tout au long de leur cycle de vie et à ce qu'elles ne puissent être divulguées à la fin de leur cycle de vie qu'après avoir été anonymisées.

3. Les entités énumérées à l'article 2, paragraphe 1, veillent à ce que toutes les mesures de protection de nature organisationnelle et technique nécessaires soient en place pour préserver et protéger la confidentialité, l'intégrité, la disponibilité et la non-répudiation des informations fournies, reçues, échangées ou transmises au titre du présent règlement, indépendamment des moyens utilisés. Les mesures de protection:

a) sont proportionnées;

b) tiennent compte des risques de cybersécurité liés aux menaces passées et émergentes connues auxquelles ces informations peuvent être soumises dans le cadre du présent règlement;

c) se fondent, dans la mesure du possible, sur les normes et bonnes pratiques nationales, européennes ou internationales;

d) sont documentées.

4. Les entités énumérées à l'article 2, paragraphe 1, veillent à ce que toute personne qui se voit accorder l'accès aux informations fournies, reçues, échangées ou transmises au titre du présent règlement soit informée des règles de sécurité applicables au niveau de l'entité et des mesures et procédures applicables à la protection des informations. Ces entités veillent à ce que la personne concernée soit consciente de la responsabilité qui lui incombe de protéger les informations conformément aux instructions données lors de la séance d'information.

5. Les entités énumérées à l'article 2, paragraphe 1, veillent à ce que l'accès aux informations fournies, reçues, échangées ou transmises au titre du présent règlement soit limité aux personnes physiques:

a) qui sont autorisés à accéder à ces informations sur la base de leurs fonctions et dans les limites de l'exécution des tâches qui leur sont assignées;

b) pour lesquelles l'entité a été en mesure d'évaluer le respect des principes éthiques et d'intégrité, ainsi que pour lesquelles il n'existe aucune preuve de résultat négatif d'une vérification des antécédents visant à évaluer la fiabilité de la personne conformément aux meilleures pratiques et aux exigences standard en matière de sécurité de l'entité et, si nécessaire, aux dispositions législatives et réglementaires nationales.

6. Les entités énumérées à l'article 2, paragraphe 1, ont l'accord écrit de la personne physique ou morale qui a créé ou fourni les informations à l'origine, avant de communiquer ces informations à un tiers qui ne relève pas du champ d'application du présent règlement.

7. Une entité énumérée à l'article 2, paragraphe 1, peut considérer que ces informations sont partagées sans se conformer aux paragraphes 1 et 4 du présent article afin de prévenir une crise électrique simultanée ayant une cause profonde en matière de cybersécurité ou toute crise transfrontalière au sein de l'Union dans un autre secteur. Dans ce cas, elle:

a) consulte l'autorité compétente et est autorisée par celle-ci à partager ces informations;

b) anonymise ces informations sans perdre les éléments nécessaires pour informer le public d'un risque imminent et grave pour les flux transfrontaliers d'électricité et des éventuelles mesures d'atténuation;

c) préserve l'identité de l'auteur des informations et des entités qui les ont traitées au titre du présent règlement.

8. Par dérogation au paragraphe 6 du présent article, les autorités compétentes peuvent communiquer des informations fournies, reçues, échangées ou transmises au titre du présent règlement à un tiers qui ne figure pas sur la liste de l'article 2, paragraphe 1, sans le consentement préalable écrit de l'auteur des informations, mais en informant ce dernier le plus tôt possible. Avant de divulguer toute information fournie, reçue, échangée ou transmise au titre du présent règlement à un tiers ne figurant pas sur la liste de l'article 2, paragraphe 1, l'autorité compétente concernée veille raisonnablement à ce que le tiers concerné ait connaissance des règles de sécurité en vigueur, et reçoit l'assurance raisonnable que le tiers concerné peut protéger les informations reçues conformément aux paragraphes 1 à 5 du présent article. L'autorité compétente anonymise ces informations sans perdre les éléments nécessaires pour informer le public d'un risque imminent et grave concernant les flux transfrontaliers d'électricité et d'éventuelles mesures d'atténuation, afin de préserver l'identité de l'auteur des informations. Dans ce cas, le tiers qui ne figure pas sur la liste de l'article 2, paragraphe 1, protège les informations reçues conformément aux dispositions déjà en vigueur au niveau de l'entité ou, lorsque cela n'est pas possible, aux dispositions et instructions fournies par l'autorité compétente concernée.

9. Le présent article ne s'applique pas aux entités non énumérées à l'article 2, paragraphe 1, qui reçoivent des informations en application du paragraphe 6 du présent article. Dans ce cas, le paragraphe 7 du présent article s'applique, ou l'autorité compétente peut fournir à cette entité des dispositions écrites à appliquer dans les cas où des informations sont reçues au titre du présent règlement.

Article 47

Confidentialité des informations

1. Toute information fournie, reçue, échangée ou transmise au titre du présent règlement est soumise aux conditions de secret professionnel prévues aux paragraphes 2 à 5 du présent article et aux exigences énoncées à l'article 65 du règlement (UE) 2019/943. Toute information fournie, reçue, échangée ou transmise entre les entités énumérées à l'article 2 du présent règlement, aux fins de la mise en œuvre du présent règlement, est protégée, compte tenu du niveau de confidentialité des informations appliqué par l'auteur.

2. L'obligation de secret professionnel s'applique aux entités énumérées à l'article 2.

3. Les autorités nationales compétentes en matière de cybersécurité, les ARN, les ANC-PR et les CSIRT échangent toutes les informations nécessaires à l'accomplissement de leurs tâches.

4. Toutes les informations reçues, échangées ou transmises entre les entités énumérées à l'article 2, paragraphe 1, aux fins de la mise en œuvre de l'article 23, sont anonymisées et agrégées.

5. Les informations reçues par toute entité ou autorité assujettie au présent règlement dans l'exercice de ses fonctions ne peuvent être divulguées à aucune autre personne ou autorité, sans préjudice des cas couverts par le droit national, les autres dispositions du présent règlement ou les autres actes applicables de la législation de l'Union.

6. Sans préjudice de la législation nationale ou de l'Union, une autorité, une entité ou une personne physique qui reçoit des informations au titre du présent règlement ne peut les utiliser à d'autres fins que l'accomplissement de ses missions au titre du présent règlement.

7. L'ACER, après avoir consulté l'ENISA, toutes les autorités compétentes, le REGRT pour l'électricité et l'entité des GRD de l'Union, publie, au plus tard le 13 juin 2025, des lignes directrices concernant les mécanismes permettant à toutes les entités énumérées à l'article 2, paragraphe 1, d'échanger des informations, et en particulier les flux de communication envisagés, ainsi que les méthodes d'anonymisation et d'agrégation des informations aux fins de la mise en œuvre du présent article.

8. Les informations confidentielles au titre de règles de l'Union ou nationales ne sont échangées avec la Commission et les autres autorités concernées que si cet échange est nécessaire à l'application du présent règlement. Les informations échangées se limitent à ce qui est nécessaire et proportionné à l'objectif de cet échange. L'échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités à impact critique ou à fort impact.

CHAPITRE VIII

DISPOSITIONS FINALES

Article 48

Dispositions temporaires

1. Jusqu'à l'approbation des modalités et conditions ou des méthodes visées à l'article 6, paragraphe 2, ou des plans visés à l'article 6, paragraphe 3, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, élabore des orientations non contraignantes sur les questions suivantes:

a) un indice d'impact provisoire sur la cybersécurité de l'électricité (ECII) conformément au paragraphe 2 du présent article;

b) une liste provisoire des processus à fort impact et à impact critique à l'échelle de l'Union conformément au paragraphe 4 du présent article;

c) une liste provisoire des normes et contrôles européens et internationaux requis par la législation nationale en rapport avec les aspects liés à la cybersécurité des flux transfrontaliers d'électricité conformément au paragraphe 6 du présent article.

2. Au plus tard le 13 octobre 2024, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, élabore une recommandation concernant un ECII provisoire. Le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, notifie l'ECII provisoire recommandé aux autorités compétentes.

3. Quatre mois à compter de la réception de l'ECII provisoire recommandé, ou au plus tard le 13 février 2025, les autorités compétentes identifient les entités susceptibles d'être classées à fort impact ou à impact critique dans leur État membre sur la base de l'ECII recommandé et établissent une liste provisoire d'entités à fort impact et à impact critique. Les entités à fort impact ou à impact critique figurant sur la liste provisoire peuvent, sur la base d'un principe de précaution, volontairement remplir les obligations qui leur incombent en application du présent règlement. Au plus tard le 13 mars 2025, les autorités compétentes notifient aux entités figurant sur la liste provisoire qu'elles ont été identifiées comme entités à fort impact ou à impact critique.

4. Au plus tard le 13 décembre 2024, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, établit une liste provisoire des processus à fort impact et à impact critique à l'échelle de l'Union. Les entités ayant reçu notification conformément au paragraphe 3 qui décident volontairement de remplir les obligations qui leur incombent en application du présent règlement sur la base d'un principe de précaution utilisent la liste provisoire des processus à fort impact et à impact critique pour déterminer les périmètres provisoires à fort impact ou à impact critique et pour déterminer quels actifs doivent être inclus dans la première évaluation des risques de cybersécurité au niveau de l'entité.

5. Au plus tard le 13 septembre 2024, chaque autorité compétente conformément à l'article 4, paragraphe 1, fournit au REGRT pour l'électricité et à l'entité des GRD de l'Union une liste de sa législation nationale pertinente pour les aspects liés à la cybersécurité des flux transfrontaliers d'électricité.

6. Au plus tard le 13 juin 2025, le REGRT pour l'électricité, en coopération avec l'entité des GRD de l'Union, établit une liste provisoire des normes et contrôles européens et internationaux requis par la législation nationale qui présentent un intérêt pour les aspects liés à la cybersécurité des flux transfrontaliers d'électricité, en tenant compte des informations fournies par les autorités compétentes.

7. La liste provisoire des normes et contrôles européens et internationaux comprend:

a) les normes européennes et internationales et la législation nationale qui fournissent des orientations sur les méthodes de gestion des risques de cybersécurité au niveau de l'entité;

b) des contrôles de cybersécurité équivalents aux contrôles qui devraient faire partie des contrôles minimaux et avancés en matière de cybersécurité.

8. Le REGRT pour l'électricité et l'entité des GRD de l'Union tiennent compte des avis exprimés par l'ENISA et l'ACER lors de la finalisation de la liste provisoire des normes. Le REGRT pour l'électricité et l'entité des GRD de l'Union publient la liste transitoire des normes et contrôles européens et internationaux sur leurs sites web.

9. Le REGRT pour l'électricité et l'entité des GRD de l'Union consultent l'ENISA et l'ACER sur les propositions d'orientations non contraignantes élaborées conformément au paragraphe 1.

10. Jusqu'à ce que les contrôles minimaux et avancés en matière de cybersécurité soient définis conformément à l'article 29 et adoptés conformément l'article 8, toutes les entités énumérées à l'article 2, paragraphe 1, s'efforcent d'appliquer progressivement les orientations non contraignantes élaborées conformément au paragraphe 1.

Article 49

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 11 mars 2024.

Par la Commission
La présidente
Ursula VON DER LEYEN