Journal officiel
de l'Union européenne

FR
Série L

2024/2690

18.10.2024

RÈGLEMENT D'EXÉCUTION (UE) 2024/2690 DE LA COMMISSION

du 17 octobre 2024

établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance

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

LA COMMISSION EUROPÉENNE,

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

vu la 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) ([1]), et notamment son article 21, paragraphe 5, premier alinéa, et son article 23, paragraphe 11, deuxième alinéa,

considérant ce qui suit:

(1) En ce qui concerne les fournisseurs de services DNS, les registres des noms de domaines de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux et les fournisseurs de services de confiance relevant de l'article 3 de la directive (UE) 2022/2555 (ci-après les «entités concernées»), le présent règlement vise à établir les exigences techniques et méthodologiques liées aux mesures visées à l'article 21, paragraphe 2, de la directive (UE) 2022/2555 et à préciser plus en détail les cas dans lesquels un incident devrait être considéré comme important au sens de l'article 23, paragraphe 3, de la directive (UE) 2022/2555.

(2) Compte tenu de la nature transfrontière de leurs activités et afin de garantir un cadre cohérent pour les prestataires de services de confiance, le présent règlement devrait, en ce qui concerne ces prestataires de services, préciser plus en détail les cas dans lesquels un incident est considéré comme important, en plus d'établir les exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité.

(3) Conformément à l'article 21, paragraphe 5, troisième alinéa, de la directive (UE) 2022/2555, les exigences techniques et méthodologiques liées aux mesures de gestion des risques de cybersécurité énoncées à l'annexe du présent règlement sont fondées sur des normes européennes et internationales, telles que ISO/IEC 27001, ISO/IEC 27002 et ETSI EN 319401, et sur des spécifications techniques, telles que CEN/TS 18026: 2024, pertinentes pour la sécurité des réseaux et des systèmes d'information.

(4) En ce qui concerne la mise en œuvre et l'application des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité énoncées à l'annexe du présent règlement, conformément au principe de proportionnalité, il convient de tenir dûment compte des différences d'exposition au risque des entités concernées, telles que la criticité de l'entité, les risques auxquels elle est exposée, la taille et la structure de l'entité, ainsi que la probabilité de survenance d'incidents et leur gravité, y compris leur impact sociétal et économique, lorsque ces entités se conforment aux exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité énoncées à l'annexe du présent règlement.

([1]) JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(5) Conformément au principe de proportionnalité, lorsque les entités concernées ne peuvent pas, en raison de leur taille, mettre en œuvre certaines des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité, ces entités devraient être en mesure de prendre d'autres mesures compensatoires appropriées pour atteindre l'objectif de ces exigences. Par exemple, lors de la définition des rôles, des responsabilités et des pouvoirs en matière de sécurité des réseaux et des systèmes d'information au sein de l'entité concernée, les micro-entités pourraient éprouver des difficultés à séparer les fonctions incompatibles et les domaines de responsabilité contradictoires. Ces entités devraient être en mesure d'envisager des mesures compensatoires telles qu'une surveillance ciblée exercée par la direction de l'entité ou une intensification du suivi et de la journalisation.

(6) Certaines exigences techniques et méthodologiques énoncées à l'annexe du présent règlement devraient être appliquées par les entités concernées s'il est besoin, s'il y a lieu ou dans la mesure du possible. Lorsqu'une entité concernée estime qu'il n'est pas besoin, qu'il n'y a pas lieu, ou qu'il est impossible pour elle d'appliquer certaines de ces exigences techniques et méthodologiques prévues à l'annexe du présent règlement, elle documente de manière compréhensible son argumentation en ce sens. Lorsqu'elles exercent une supervision, les autorités nationales compétentes peuvent tenir compte du temps nécessaire aux entités concernées pour mettre en œuvre les exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité.

(7) L'ENISA ou les autorités nationales compétentes au titre de la directive (UE) 2022/2555 peuvent fournir des orientations pour aider les entités concernées à identifier, analyser et évaluer les risques aux fins de la mise en œuvre des exigences techniques et méthodologiques concernant la mise en place et le maintien d'un cadre approprié de gestion des risques. Ces orientations peuvent comprendre, en particulier, des évaluations des risques nationales et sectorielles ainsi que des évaluations des risques spécifiques à un certain type d'entité. Les orientations peuvent également comprendre des outils ou des modèles pour l'élaboration d'un cadre de gestion des risques au niveau des entités concernées. Les cadres, orientations ou autres mécanismes prévus par le droit national des États membres, ainsi que des normes européennes et internationales pertinentes peuvent également aider les entités concernées à apporter la preuve du respect du présent règlement d'exécution. En outre, l'ENISA ou les autorités nationales compétentes au titre de la directive (UE) 2022/2555 peuvent aider les entités concernées à trouver et à mettre en œuvre des solutions appropriées pour traiter les risques identifiés dans ces évaluations des risques. Ces orientations devraient être sans préjudice de l'obligation des entités concernées d'identifier et de documenter les risques pour la sécurité des réseaux et des systèmes d'information, ainsi que de l'obligation, pour les entités concernées, de mettre en œuvre les exigences techniques et méthodologiques liées aux mesures de gestion des risques de cybersécurité énoncées à l'annexe du présent règlement en fonction de leurs besoins et de leurs ressources.

(8) Les mesures de sécurité des réseaux concernant: i) la transition vers des protocoles de communication de la dernière génération au niveau de la couche réseau, ii) le déploiement de normes modernes de communication par courrier électronique internationalement reconnues et interopérables, et iii) l'application des meilleures pratiques en matière de sécurité DNS, de sécurité du routage sur internet et d'hygiène du routage posent des difficultés particulières eu égard à l'inventaire des meilleures normes et techniques de déploiement disponibles. Afin d'atteindre dès que possible un niveau élevé commun de cybersécurité sur l'ensemble des réseaux, la Commission, avec l'aide de l'Agence de l'Union européenne pour la cybersécurité (ENISA) et en collaboration avec les autorités compétentes, l'industrie — y compris le secteur des télécommunications — et d'autres parties prenantes, devrait soutenir la mise en place d'un forum multipartite chargé d'inventorier ces meilleures normes et techniques de déploiement disponibles. Ces orientations multipartites devraient être sans préjudice de l'obligation, pour les entités concernées, de mettre en œuvre les exigences techniques et méthodologiques liées aux mesures de gestion des risques de cybersécurité énoncées à l'annexe du présent règlement.

(9) Conformément à l'article 21, paragraphe 2, point a), de la directive (UE) 2022/2555, les entités essentielles et importantes devraient être dotées de politiques relatives à l'analyse des risques ainsi que de politiques relatives à la sécurité des systèmes d'information. À cette fin, les entités concernées devraient établir une politique relative à la sécurité des réseaux et des systèmes d'information ainsi que des politiques concernant des domaines spécifiques, telles que des politiques en matière de contrôle d'accès, qui devraient être cohérentes avec la politique relative à la sécurité des réseaux et des systèmes d'information. La politique relative à la sécurité des réseaux et des systèmes d'information devrait occuper le plus haut niveau de la hiérarchie des documents définissant l'approche globale des entités concernées en matière de sécurité de leurs réseaux et systèmes d'information et elle devrait être approuvée par les organes de direction des entités concernées. Les politiques concernant des domaines spécifiques devraient être approuvées à un niveau hiérarchique approprié. La politique devrait définir des indicateurs et des mesures permettant de suivre sa mise en œuvre et l'état actuel du niveau de maturité des entités concernées en matière de sécurité des réseaux et de l'information, en particulier pour faciliter la surveillance de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité par l'intermédiaire des organes de direction.

(10) Aux fins des exigences techniques et méthodologiques énoncées à l'annexe du présent règlement, le terme «utilisateur» devrait englober toutes les personnes physiques et morales qui ont accès au réseau et aux systèmes d'information de l'entité.

(11) Afin d'identifier et de traiter les risques qui pèsent sur la sécurité des réseaux et des systèmes d'information, les entités concernées devraient établir et maintenir un cadre approprié de gestion des risques. Les entités concernées devraient inscrire dans ce cadre l'établissement, la mise en œuvre et le suivi d'un plan de traitement des risques. Les entités concernées peuvent utiliser le plan de traitement des risques pour inventorier et hiérarchiser les options et les mesures relatives au traitement des risques. Parmi les options de traitement des risques figurent notamment la prévention, la réduction ou, dans des cas exceptionnels, l'acceptation des risques. Le choix des options de traitement des risques devrait tenir compte des résultats de l'évaluation des risques effectuée par l'entité concernée et être conforme à la politique de cette dernière en matière de sécurité des réseaux et des systèmes d'information. Afin de donner effet aux options de traitement des risques choisies, les entités concernées devraient prendre les mesures de traitement des risques appropriées.

(12) Pour détecter les événements, les incidents évités et les incidents, les entités concernées devraient surveiller leur réseau et leurs systèmes d'information et prendre des mesures pour évaluer les événements, les incidents évités et les incidents. Ces mesures devraient permettre de détecter en temps utile les attaques réseau en se fondant sur des schémas anormaux de trafic entrant et sortant, ainsi que les attaques par déni de service.

(13) Lorsque les entités concernées procèdent à une analyse de l'impact sur l'activité, elles sont encouragées à réaliser une analyse complète établissant, le cas échéant, les temps d'arrêt maximaux tolérables, les objectifs de délai de rétablissement, les objectifs de points de rétablissement et les objectifs de fourniture de services.

(14) Afin d'atténuer les risques découlant de la chaîne d'approvisionnement d'une entité concernée et des relations de cette dernière avec ses fournisseurs, les entités concernées devraient établir une politique de sécurité de la chaîne d'approvisionnement régissant leurs relations avec leurs fournisseurs et prestataires de services directs. Ces entités devraient faire figurer dans les contrats conclus avec leurs fournisseurs ou prestataires de services directs des clauses de sécurité adéquates, par exemple en exigeant, le cas échéant, des mesures de gestion des risques en matière de cybersécurité conformément à l'article 21, paragraphe 2, de la directive (UE) 2022/2555 ou en imposant d'autres exigences légales similaires.

(15) Les entités concernées devraient effectuer régulièrement des tests de sécurité sur la base d'une politique et de procédures ad hoc afin de vérifier si les mesures de gestion des risques en matière de cybersécurité sont mises en œuvre et fonctionnent correctement. Les tests de sécurité peuvent être effectués sur des réseaux et systèmes d'information spécifiques ou sur l'entité concernée dans son ensemble et peuvent comprendre des tests automatisés ou manuels, des tests d'intrusion, des analyses de vulnérabilité, des tests dynamiques ou statiques de sécurité des applications, des tests de configuration ou des audits de sécurité. Les entités concernées peuvent effectuer des tests de sécurité sur leur réseau et leurs systèmes d'information lors de la mise en place, après des mises à niveau ou des modifications d'infrastructures ou d'applications qu'elles jugent importantes, ou après des opérations de maintenance. Les résultats des tests de sécurité devraient éclairer les politiques et procédures des entités concernées visant à évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité, ainsi que les examens indépendants de leurs politiques de sécurité des réseaux et de l'information.

(16) Afin d'éviter que l'exploitation de vulnérabilités non corrigées dans les réseaux et les systèmes d'information ne cause des perturbations et des préjudices importants, les entités concernées devraient définir et appliquer des procédures appropriées de gestion des correctifs de sécurité qui soient alignées sur leurs procédures pertinentes en matière de gestion des changements, gestion des vulnérabilités, gestion des risques et autres. Les entités concernées devraient prendre des mesures proportionnées à leurs ressources pour veiller à ce que les correctifs de sécurité n'introduisent pas de vulnérabilités ou d'instabilités supplémentaires. Si le service est inaccessible en raison de l'application de correctifs de sécurité, les entités concernées sont encouragées à en informer dûment les clients à l'avance.

(17) Les entités concernées devraient gérer les risques découlant de l'acquisition de produits ou de services TIC auprès de fournisseurs ou de prestataires de services et devraient obtenir l'assurance que les produits ou services TIC à acquérir atteignent certains niveaux de protection en matière de cybersécurité, par exemple au moyen de certificats de cybersécurité européens et de déclarations de conformité de l'UE pour des produits ou services TIC délivrés dans le cadre d'un schéma européen de certification de cybersécurité adopté en vertu de l'article 49 du règlement (UE) 2019/881 du Parlement européen et du Conseil ([2]). Lorsque les entités concernées fixent des exigences de sécurité à imposer aux produits TIC à acquérir, elles devraient tenir compte des exigences essentielles en matière de cybersécurité énoncées dans un règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques.

(18) Afin de se protéger contre les cybermenaces et d'aider à prévenir et à endiguer les violations de données, les entités concernées devraient mettre en œuvre des solutions en matière de sécurité des réseaux. Ces solutions consistent généralement à utiliser des pare-feu pour protéger les réseaux internes des entités concernées, à limiter les connexions et les accès aux services auxquels ces connexions et accès sont absolument nécessaires, à recourir à des réseaux privés virtuels pour l'accès à distance, à soumettre les connexions des fournisseurs de services à une demande d'autorisation et à limiter ces connexions à une durée déterminée telle que la durée d'une opération de maintenance.

(19) Afin de protéger les réseaux des entités concernées et leurs systèmes d'information contre les logiciels malveillants et non autorisés, ces entités devraient mettre en œuvre des contrôles qui préviennent ou détectent l'utilisation de logiciels non autorisés et devraient, le cas échéant, utiliser des logiciels de détection et de réaction. Les entités concernées devraient également envisager de mettre en œuvre des mesures visant à réduire au minimum la surface d'attaque, à réduire les vulnérabilités qui peuvent être exploitées par les auteurs d'attaques, à contrôler l'exécution des applications sur les points terminaux et à déployer des filtres de messagerie électronique et d'applications web afin de réduire l'exposition aux contenus malveillants.

(20) Conformément à l'article 21, paragraphe 2, point g), de la directive (UE) 2022/2555, les États membres doivent veiller à ce que les entités essentielles et importantes appliquent des pratiques élémentaires en matière d'hygiène informatique et de formation à la cybersécurité. Parmi les pratiques élémentaires d'hygiène informatique figurent les principes «confiance zéro», les mises à jour de logiciels, la configuration des dispositifs, la segmentation des réseaux, la gestion des identités et des accès ou la sensibilisation des utilisateurs, l'organisation d'une formation pour le personnel et la sensibilisation aux cybermenaces, à l'hameçonnage ou aux techniques d'ingénierie sociale. Les pratiques d'hygiène informatique font partie des différentes exigences techniques et méthodologiques liées aux mesures de gestion des risques de cybersécurité énoncées à l'annexe du présent règlement. En ce qui concerne les pratiques élémentaires en matière d'hygiène informatique pour les utilisateurs, les entités concernées devraient envisager des pratiques telles que des politiques claires relatives aux bureaux et aux écrans, l'utilisation de moyens d'authentification multifactoriels et autres, l'utilisation sûre du courrier électronique et la navigation sur le web, la protection contre l'hameçonnage et l'ingénierie sociale ou encore les pratiques de travail à distance sécurisées.

(21) Afin d'empêcher l'accès non autorisé à leurs actifs, les entités concernées devraient établir et mettre en œuvre une politique spécifique concernant l'accès par des personnes et par des réseaux et systèmes d'information, tels que les applications.

(22) Afin d'éviter que les employés ne puissent abuser, par exemple, des droits d'accès au sein de l'entité concernée pour causer un préjudice et des dommages, les entités concernées devraient envisager des mesures appropriées de gestion de la sécurité du personnel et sensibiliser le personnel à ces risques. Les entités concernées devraient établir, communiquer et maintenir une procédure disciplinaire de traitement des violations de leurs politiques de sécurité des réseaux et des systèmes d'information, qui peut être intégrée dans d'autres procédures disciplinaires établies par ces entités. Les vérifications des antécédents des employés et, s'il y a lieu, des fournisseurs et des prestataires de services directs des entités concernées devraient contribuer à l'objectif de sécurité des ressources humaines dans les entités concernées et peuvent comprendre des mesures telles que des vérifications du casier judiciaire ou des fonctions professionnelles passées de la personne, selon les fonctions qu'elle occupe au sein de l'entité concernée et conformément à la politique de l'entité concernée en matière de sécurité des réseaux et des systèmes d'information.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) L'authentification multifactorielle peut renforcer la cybersécurité des entités et ces dernières devraient l'envisager, en particulier lorsque les utilisateurs accèdent à des réseaux et à des systèmes d'information à distance, ou lorsqu'ils accèdent à des informations sensibles ou à des comptes privilégiés et à des comptes d'administration de systèmes. L'authentification multifactorielle peut être combinée à d'autres techniques pour exiger des facteurs supplémentaires dans des circonstances particulières, sur la base de règles et de modèles prédéfinis, tels que l'accès depuis un lieu inhabituel, à partir d'un dispositif inhabituel ou à un moment inhabituel.

(24) Les entités concernées devraient assurer la gestion et la protection des actifs ayant de la valeur pour elles en mettant en place une gestion saine des actifs qui devrait également servir de base à l'analyse des risques et à la gestion de la continuité de l'activité. Les entités concernées devraient gérer à la fois les actifs matériels et immatériels et créer un inventaire des actifs, associer à chaque actif un niveau de classification précis, assurer le traitement et la traçabilité des actifs et prendre des mesures pour les protéger tout au long de leur cycle de vie.

(25) La gestion des actifs devrait consister à classer les actifs en fonction de leur type, de leur sensibilité, de leur niveau de risque et des exigences en matière de sécurité, et à appliquer des mesures et des contrôles appropriés pour garantir leur disponibilité, leur intégrité, leur confidentialité et leur authenticité. En classant les actifs par niveau de risque, les entités concernées devraient pouvoir appliquer des mesures et des contrôles de sécurité appropriés pour protéger les actifs, telles que le chiffrement, le contrôle d'accès, y compris le contrôle du périmètre et de l'accès physique et logique, les sauvegardes, la journalisation et le suivi, la conservation et l'élimination. Lorsqu'elles procèdent à une analyse d'impact sur l'activité, les entités concernées peuvent déterminer le niveau de classification en fonction des conséquences qu'aurait une perturbation des actifs pour les entités. Tous les membres du personnel des entités qui sont amenés à traiter des actifs doivent connaître les politiques et les instructions en la matière.

(26) Il convient d'adapter le niveau de détail de l'inventaire des actifs aux besoins des entités concernées. Un inventaire complet des actifs pourrait comprendre, pour chaque actif, au moins un identifiant unique, le propriétaire de l'actif, une description de l'actif, la localisation de l'actif, le type d'actif, le type et la classification des informations traitées dans l'actif, la date de la dernière mise à jour ou du dernier correctif de l'actif, le classement de l'actif dans le cadre de l'évaluation des risques et la fin de vie de l'actif. Lorsqu'elles identifient le propriétaire d'un actif, les entités concernées devraient également identifier la personne responsable de la protection de cet actif.

(27) La répartition et l'organisation des rôles, des responsabilités et des pouvoirs en matière de cybersécurité devraient permettre de mettre en place une structure cohérente pour la gouvernance et la mise en œuvre de la cybersécurité au sein des entités concernées, et d'assurer une communication efficace en cas d'incident. Lors de la définition et de l'attribution des responsabilités à certains rôles, les entités concernées devraient notamment tenir compte du rôle du directeur de la sécurité de l'information, du responsable de la sécurité de l'information, du responsable de la gestion des incidents, de l'auditeur ou d'équivalents comparables. Les entités concernées peuvent attribuer des rôles et des responsabilités à des parties externes, telles que des tiers prestataires de services informatiques.

(28) Conformément à l'article 21, paragraphe 2, de la directive (UE) 2022/2555, les mesures de gestion des risques en matière de cybersécurité doivent se fonder sur une approche «tous risques» qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre des événements tels que le vol, les incendies, les inondations, une défaillance des télécommunications ou une défaillance électrique, ou contre tout accès physique non autorisé et toute atteinte aux informations détenues par l'entité essentielle ou importante et aux installations de traitement de l'information de l'entité, ou toute interférence avec ces informations et installations, susceptibles de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des services offerts par les réseaux et systèmes d'information ou accessibles par ceux-ci. Les exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité devraient donc également porter sur la sécurité physique et la sécurité de l'environnement des réseaux et des systèmes d'information, en incluant des mesures visant à protéger ces systèmes contre les défaillances du système, les erreurs humaines, les actes malveillants ou les phénomènes naturels. On peut citer d'autres exemples de menaces physiques et environnementales telles que les tremblements de terre, les explosions, le sabotage, la menace interne, les troubles civils, les déchets toxiques et les émissions dans l'environnement. La prévention de la perte, de la détérioration ou de la compromission de réseaux et systèmes d'information ou de l'interruption de leur fonctionnement en raison de la défaillance et de la perturbation de services d'utilité publique sous-jacents devrait contribuer à l'objectif de continuité de l'activité dans les entités concernées. En outre, la protection contre les menaces physiques et environnementales devrait contribuer à la sécurité de la maintenance des réseaux et des systèmes d'information dans les entités concernées.

(29) Les entités devraient concevoir et mettre en œuvre des mesures de protection contre les menaces physiques et environnementales, fixer des seuils de contrôle minimaux et maximaux pour les menaces physiques et environnementales et surveiller les paramètres environnementaux. Par exemple, elles devraient envisager d'installer des systèmes permettant de détecter à un stade précoce les inondations dans les zones où se trouvent les réseaux et les systèmes d'information. En ce qui concerne le risque d'incendie, les entités concernées devraient envisager de mettre en place un compartiment coupe-feu séparé pour le centre de données, d'utiliser des matériaux résistant au feu, de recourir à des capteurs pour le contrôle de la température et de l'humidité, de raccorder le bâtiment à un système d'alarme incendie avec notification automatisée aux services locaux de lutte contre les incendies, et de faire appel à des systèmes de détection et d'extinction précoces des incendies. Les entités concernées devraient également procéder régulièrement à des exercices d'incendie et à des inspections de sécurité incendie. En outre, pour assurer l'alimentation électrique, les entités concernées devraient envisager une protection contre les surtensions et une alimentation électrique de secours correspondante, conformément aux normes applicables. Par ailleurs, étant donné que la surchauffe présente un risque pour la disponibilité des réseaux et des systèmes d'information, les entités concernées, en particulier les fournisseurs de services de centres de données, pourraient envisager des systèmes de climatisation adéquats, fonctionnant en continu et redondants.

(30) Le présent règlement doit préciser plus en détail les cas dans lesquels un incident devrait être considéré comme important au sens de l'article 23, paragraphe 3, de la directive (UE) 2022/2555. Les critères devraient être tels que les entités concernées soient en mesure d'évaluer si un incident est important afin de le notifier conformément à la directive (UE) 2022/2555. En outre, les critères énoncés dans le présent règlement devraient être considérés comme exhaustifs, sans préjudice de l'article 5 de la directive (UE) 2022/2555. Le présent règlement précise les cas dans lesquels un incident devrait être considéré comme important en définissant des cas horizontaux ainsi que des cas spécifiques à l'entité.

(31) L'article 23, paragraphe 4, de la directive (UE) 2022/2555 prévoit que les entités concernées notifient les incidents importants dans les délais fixés audit article. Ces délais de notification courent à partir du moment où l'entité a connaissance de tels incidents importants. Par conséquent, l'entité concernée est tenue de notifier les incidents qui, selon son évaluation initiale, pourraient entraîner des perturbations opérationnelles graves des services ou des pertes financières pour ladite entité, ou nuire à d'autres personnes physiques ou morales en causant un dommage matériel, corporel ou moral considérable. Par conséquent, lorsqu'une entité concernée a détecté un événement suspect, ou après qu'un incident potentiel a été porté à son attention par un tiers, tel qu'un particulier, un client, une entité, une autorité, un organisme de médias ou une autre source, l'entité concernée devrait évaluer en temps opportun l'événement suspect afin de déterminer s'il constitue un incident et, dans l'affirmative, en déterminer la nature et la gravité. Il convient donc de considérer que l'entité concernée a «eu connaissance» de l'incident important lorsque, après avoir procédé à cette évaluation initiale, elle est raisonnablement certaine qu'un incident important s'est produit.

(32) Afin d'établir si un incident est important, le cas échéant, les entités concernées devraient compter le nombre d'utilisateurs touchés par l'incident, en tenant compte des clients professionnels et des clients finaux avec lesquels elles entretiennent une relation contractuelle ainsi que des personnes physiques et morales qui sont associées à des clients professionnels. Lorsqu'une entité concernée n'est pas en mesure de calculer le nombre d'utilisateurs touchés, il y a lieu de prendre en considération, aux fins du calcul du nombre total d'utilisateurs touchés par l'incident, l'estimation du nombre maximal possible d'utilisateurs touchés effectuée par cette entité. L'importance d'un incident impliquant un service de confiance devrait être déterminée non seulement par le nombre d'utilisateurs, mais aussi par le nombre de parties utilisatrices, celles-ci pouvant être affectées au même titre par un incident important impliquant un service de confiance en ce qui concerne une perturbation opérationnelle ou un préjudice matériel ou moral. Par conséquent, les prestataires de services de confiance devraient, le cas échéant, également tenir compte du nombre de parties utilisatrices lorsqu'ils établissent si un incident est important. À cette fin, il convient d'entendre par parties utilisatrices des personnes physiques ou morales qui utilisent un service de confiance.

(33) Les opérations de maintenance entraînant une disponibilité limitée ou une indisponibilité des services ne devraient pas être considérées comme des incidents importants si la disponibilité limitée ou l'indisponibilité du service survient à la suite d'une opération de maintenance programmée. En outre, l'indisponibilité d'un service en raison d'interruptions telles que des interruptions programmées ou une indisponibilité sur la base d'un accord contractuel prédéterminé ne devrait pas être considérée comme un incident important.

(34) La durée d'un incident ayant des conséquences sur la disponibilité d'un service devrait être mesurée à partir de l'interruption de la fourniture correcte de ce service jusqu'au moment du rétablissement. Lorsqu'une entité concernée n'est pas en mesure de déterminer le moment à partir duquel l'interruption a commencé, la durée de l'incident devrait être mesurée à partir du moment où l'incident a été détecté, ou de celui où l'incident a été enregistré dans les journaux du réseau, du système ou d'autres sources de données, selon l'éventualité qui intervient en premier.

(35) L'indisponibilité totale d'un service devrait être mesurée à partir du moment où le service est totalement indisponible pour les utilisateurs et le moment où les activités ou opérations régulières ont retrouvé le niveau de service fourni avant l'incident. Lorsqu'une entité concernée n'est pas en mesure de déterminer quand l'indisponibilité totale d'un service a commencé, cette indisponibilité devrait être mesurée à partir du moment où elle a été détectée par cette entité.

(36) Afin de déterminer les pertes financières directes résultant d'un incident, les entités concernées devraient tenir compte de toutes les pertes financières qu'elles ont subies à la suite de l'incident, telles que les coûts du remplacement ou du déplacement de logiciels, de matériel ou d'infrastructures, les frais de personnel, y compris les coûts liés au remplacement ou au déménagement du personnel, au recrutement de personnel supplémentaire, à la rémunération des heures supplémentaires et à la récupération des compétences perdues ou altérées, les frais dus au non-respect d'obligations contractuelles, les coûts de dédommagement et d'indemnisation des clients, les pertes dues aux recettes non perçues, les coûts liés à la communication interne et externe, les frais de conseil, y compris les coûts liés au conseil juridique, aux services d'investigation numérique et aux services de remédiation, et les autres coûts liés à l'incident. Toutefois, les amendes administratives, ainsi que les coûts qui sont nécessaires à la gestion quotidienne de l'activité, ne devraient pas être considérées comme des pertes financières résultant d'un incident, y compris les coûts de maintenance générale des infrastructures, des équipements, du matériel et des logiciels, la mise à jour des compétences du personnel, les coûts internes ou externes pour améliorer l'activité après l'incident, y compris les mises à niveau, les améliorations et les initiatives d'évaluation des risques, ainsi que les primes d'assurance. Les entités concernées devraient calculer le montant des pertes financières sur la base des données disponibles et avoir recours à une estimation lorsqu'il est impossible de déterminer le montant réel de ces pertes.

(37) Les entités concernées devraient également être tenues de signaler les incidents qui ont causé ou sont susceptibles de causer la mort de personnes physiques ou des dommages considérables à la santé de ces dernières, étant donné que ces incidents constituent des cas particulièrement graves de dommages matériels ou moraux considérables. Par exemple, un incident touchant une entité concernée pourrait entraîner l'indisponibilité de services de soins de santé ou d'urgence, ou une perte de confidentialité ou d'intégrité de données ayant une incidence sur la santé des personnes physiques. Pour déterminer si un incident a causé ou est susceptible de causer des dommages considérables à la santé d'une personne physique, les entités concernées devraient examiner si l'incident a causé ou est susceptible de causer des blessures graves et des problèmes de santé. Les entités concernées ne devraient pas être tenues de recueillir, à cette fin, des informations supplémentaires auxquelles elles n'ont pas accès.

(38) Il y a lieu de considérer que la disponibilité est limitée en particulier lorsqu'un service fourni par une entité concernée est considérablement plus lent que la moyenne, ou lorsque toutes les fonctionnalités d'un service ne sont pas disponibles. Dans la mesure du possible, il convient d'utiliser, pour évaluer les retards dans le délai de réponse, des critères objectifs fondés sur les délais moyens de réponse des services fournis par les entités concernées. Une fonctionnalité d'un service peut être, par exemple, une fonctionnalité de discussion en ligne ou une fonctionnalité de recherche d'images.

(39) Un accès non autorisé effectif et suspecté d'être malveillant aux réseaux et systèmes d'information d'une entité concernée devrait être considéré comme un incident important lorsque cet accès est susceptible de causer une perturbation opérationnelle grave. Par exemple, lorsqu'un acteur de cybermenace se pré-positionne dans le réseau et les systèmes d'information d'une entité concernée en vue de perturber les services à l'avenir, l'incident devrait être considéré comme important.

(40) Les incidents récurrents qui sont liés par une cause originelle apparente similaire et qui, pris isolément, ne répondent pas aux critères nécessaires pour être considérés comme importants, devraient être considérés collectivement comme constituant un incident important, à condition qu'ils remplissent collectivement le critère de la perte financière et qu'ils se soient produits au moins deux fois en l'espace de six mois. Ces incidents récurrents peuvent être le signe de défaillances et de faiblesses importantes dans les procédures de gestion des risques de cybersécurité de l'entité concernée et dans leur niveau de maturité en matière de cybersécurité. En outre, de tels incidents récurrents sont susceptibles de causer des pertes financières importantes à l'entité concernée.

(41) La Commission a procédé à un échange de points de vue et a coopéré avec le groupe de coopération et l'ENISA sur le projet d'acte d'exécution conformément à l'article 21, paragraphe 5, et à l'article 23, paragraphe 11, de la directive (UE) 2022/2555.

(42) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([3]) et a rendu son avis le 1er septembre 2024.

(43) Les mesures prévues par le présent règlement sont conformes à l'avis du comité institué par l'article 39 de la directive (UE) 2022/2555,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement établit, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaines de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux et les fournisseurs de services de confiance (ci-après les «entités concernées»), les exigences techniques et méthodologiques liées aux mesures visées à l'article 21, paragraphe 2, de la directive (UE) 2022/2555 et précise plus en détail les cas dans lesquels un incident devrait être considéré comme important au sens de l'article 23, paragraphe 3, de la directive (UE) 2022/2555.

Article 2

Exigences techniques et méthodologiques

1. Pour les entités concernées, les exigences techniques et méthodologiques liées aux mesures de gestion des risques de cybersécurité visées à l'article 21, paragraphe 2, points a) à j), de la directive (UE) 2022/2555 sont énoncées à l'annexe du présent règlement.

2. Lorsqu'elles mettent en œuvre et appliquent les exigences techniques et méthodologiques liées aux mesures de gestion des risques de cybersécurité énoncées à l'annexe du présent règlement, les entités concernées assurent un niveau de sécurité des réseaux et des systèmes d'information adapté aux risques présents. À cette fin, lorsqu'elles se conforment aux exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité énoncées à l'annexe du présent règlement, elles tiennent dûment compte de leur degré d'exposition aux risques, de leur taille et de la probabilité de survenance d'incidents, ainsi que de leur gravité, y compris de leur impact sociétal et économique.

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

Lorsque l'annexe du présent règlement prévoit qu'une exigence technique ou méthodologique liée à une mesure de gestion des risques de cybersécurité est appliquée «s'il est besoin», «s'il y a lieu» ou «dans la mesure du possible», et lorsqu'une entité concernée estime qu'il n'est pas besoin, qu'il n'y a pas lieu, ou qu'il est impossible pour elle d'appliquer certaines de ces exigences techniques et méthodologiques, elle documente de manière compréhensible son argumentation en ce sens.

Article 3

Incidents importants

1. Un incident est considéré comme important au sens de l'article 23, paragraphe 3, de la directive (UE) 2022/2555 eu égard aux entités concernées lorsqu'un ou plusieurs des critères suivants sont remplis:

a) l'incident a causé ou est susceptible de causer à l'entité concernée une perte financière directe supérieure à 500 000 EUR ou à 5 % du chiffre d'affaires annuel total de l'entité concernée au cours de l'exercice complet précédent, le montant le plus faible étant retenu;

b) l'incident a causé ou est susceptible de provoquer l'exfiltration de secrets d'affaires de l'entité concernée, au sens de l'article 2, point 1), de la directive (UE) 2016/943;

c) l'incident a causé ou est susceptible de causer la mort d'une personne physique;

d) l'incident a causé ou est susceptible de causer des dommages considérables à la santé d'une personne physique;

e) il y a eu un accès non autorisé effectif au réseau et aux systèmes d'information d'une entité concernée, qui est suspecté d'être malveillant et est susceptible de causer une perturbation opérationnelle grave;

f) l'incident répond aux critères énoncés à l'article 4;

g) l'incident répond à un ou plusieurs des critères énoncés aux articles 5 à 14.

2. Les interruptions de service programmées et les conséquences prévues des opérations de maintenance programmées effectuées par les entités concernées ou pour leur compte ne sont pas considérées comme des incidents importants.

3. Lorsqu'elles calculent le nombre d'utilisateurs touchés par un incident aux fins de l'article 7 et des articles 9 à 14, les entités concernées tiennent compte de l'ensemble des éléments suivants:

a) le nombre de clients ayant conclu, avec l'entité concernée, un contrat qui leur donne accès au réseau et aux systèmes d'information de l'entité concernée ou aux services proposés par ce réseau et ces systèmes d'information ou accessibles par leur intermédiaire;

b) le nombre de personnes physiques et morales associées à des clients professionnels qui utilisent le réseau et les systèmes d'information de l'entité concernée ou les services proposés par ce réseau et ces systèmes d'information ou accessibles par leur intermédiaire.

Article 4

Incidents récurrents

Les incidents qui, pris isolément, ne sont pas considérés comme des incidents importants au sens de l'article 3 sont considérés collectivement comme un incident important lorsqu'ils remplissent l'ensemble des critères suivants:

a) ils se sont produits au moins deux fois en six mois;

b) ils ont la même cause originelle apparente;

c) ils répondent collectivement aux critères énoncés à l'article 3, paragraphe 1, point a).

Article 5

Incidents importants concernant les fournisseurs de services DNS

En ce qui concerne les fournisseurs de services DNS, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) un service de résolution de noms de domaine récursif ou faisant autorité est totalement indisponible pendant plus de 30 minutes;

b) pendant une période de plus d'une heure, un service de résolution de noms de domaine récursif ou faisant autorité a un temps de réponse moyen aux demandes DNS supérieur à 10 secondes;

c) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture du service de résolution de nom de domaine faisant autorité est compromise, sauf dans les cas où les données de moins de 1 000 noms de domaine gérées par le fournisseur de services DNS, ne représentant pas plus de 1 % des noms de domaine gérés par ce fournisseur, ne sont pas correctes en raison d'une mauvaise configuration.

Article 6

Incidents importants concernant les registres de noms de domaine de premier niveau

En ce qui concerne les registres de noms de domaine de premier niveau, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) un service de résolution de noms de domaine faisant autorité est totalement indisponible;

b) pendant une période de plus d'une heure, un service de résolution de noms de domaine faisant autorité a un temps de réponse moyen aux demandes DNS supérieur à 10 secondes;

c) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées au fonctionnement technique du domaine de premier niveau est compromise.

Article 7

Incidents importants concernant les fournisseurs de services d'informatique en nuage

En ce qui concerne les fournisseurs de services d'informatique en nuage, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) un service d'informatique en nuage est totalement indisponible pendant plus de 30 minutes;

b) la disponibilité d'un service d'informatique en nuage d'un fournisseur est limitée pour plus de 5 % des utilisateurs de ce service dans l'Union, ou pour plus de 1 million d'utilisateurs de ce service dans l'Union, le plus petit nombre étant retenu, pendant plus d'une heure;

c) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un service d'informatique en nuage est compromise par une action suspectée d'être malveillante,

d) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un service d'informatique en nuage est compromise, ce qui a un impact sur plus de 5 % des utilisateurs de ce service dans l'Union, ou sur plus de 1 million d'utilisateurs de ce service dans l'Union, le plus petit nombre étant retenu.

Article 8

Incidents importants concernant les fournisseurs de services de centres de données

En ce qui concerne les fournisseurs de services de centres de données, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) un service d'un centre de données exploité par le fournisseur est totalement indisponible;

b) la disponibilité d'un service d'un centre de données exploité par le fournisseur est limitée pendant plus d'une heure;

c) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un service de centre de données est compromise par une action suspectée d'être malveillante,

d) l'accès physique à un centre de données exploité par le fournisseur est compromis.

Article 9

Incidents importants concernant les fournisseurs de réseaux de diffusion de contenu

En ce qui concerne les fournisseurs de services de réseaux de diffusion de contenu, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) un réseau de diffusion de contenu est totalement indisponible pendant plus de 30 minutes;

b) la disponibilité d'un réseau de diffusion de contenu est limitée pour plus de 5 % des utilisateurs de ce réseau dans l'Union, ou pour plus de 1 million d'utilisateurs de ce réseau dans l'Union, le plus petit nombre étant retenu, pendant plus d'une heure;

c) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un réseau de diffusion de contenu est compromise par une action suspectée d'être malveillante,

d) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un réseau de diffusion de contenu est compromise, ce qui a un impact sur plus de 5 % des utilisateurs de ce réseau dans l'Union, ou sur plus de 1 million d'utilisateurs de ce réseau dans l'Union, le plus petit nombre étant retenu.

Article 10

Incidents importants concernant les fournisseurs de services gérés et les fournisseurs de services de sécurité gérés

En ce qui concerne les fournisseurs de services gérés et les fournisseurs de services de sécurité gérés, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) un service géré ou un service de sécurité géré est totalement indisponible pendant plus de 30 minutes;

b) la disponibilité d'un service géré ou d'un service de sécurité géré est limitée pour plus de 5 % des utilisateurs de ce service dans l'Union, ou pour plus de 1 million d'utilisateurs de ce service dans l'Union, le plus petit nombre étant retenu, pendant plus d'une heure;

c) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un service géré ou d'un service de sécurité géré est compromise par une action suspectée d'être malveillante,

d) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un service géré ou d'un service de sécurité géré est compromise, ce qui a un impact sur plus de 5 % des utilisateurs de ce service géré ou service de sécurité géré dans l'Union, ou sur plus de 1 million d'utilisateurs de ces services dans l'Union, le plus petit nombre étant retenu.

Article 11

Incidents importants concernant les fournisseurs de places de marché en ligne

En ce qui concerne les fournisseurs de places de marché en ligne, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) une place de marché en ligne est totalement indisponible pour plus de 5 % des utilisateurs de cette place de marché en ligne dans l'Union, ou pour plus de 1 million d'utilisateurs de cette place de marché en ligne dans l'Union, le plus petit nombre étant retenu;

b) plus de 5 % des utilisateurs d'une place de marché en ligne dans l'Union, ou plus de 1 million d'utilisateurs d'une place de marché en ligne dans l'Union, le plus petit nombre étant retenu, sont touchés par la disponibilité limitée de cette place de marché en ligne;

c) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'une place de marché en ligne est compromise par une action suspectée d'être malveillante,

d) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'une place de marché en ligne est compromise, ce qui a un impact sur plus de 5 % des utilisateurs de cette place de marché en ligne dans l'Union, ou sur plus de 1 million d'utilisateurs de cette place de marché en ligne dans l'Union, le plus petit nombre étant retenu.

Article 12

Incidents importants concernant les fournisseurs de moteurs de recherche en ligne

En ce qui concerne les fournisseurs de moteurs de recherche en ligne, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) un moteur de recherche en ligne est totalement indisponible pour plus de 5 % des utilisateurs de ce moteur de recherche en ligne dans l'Union, ou pour plus de 1 million d'utilisateurs de ce moteur de recherche en ligne dans l'Union, le plus petit nombre étant retenu;

b) plus de 5 % des utilisateurs d'un moteur de recherche en ligne dans l'Union, ou plus de 1 million d'utilisateurs d'un moteur de recherche en ligne dans l'Union, le plus petit nombre étant retenu, sont touchés par la disponibilité limitée de ce moteur de recherche en ligne;

c) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un moteur de recherche en ligne est compromise par une action suspectée d'être malveillante,

d) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un moteur de recherche en ligne est compromise, ce qui a un impact sur plus de 5 % des utilisateurs de ce moteur de recherche en ligne dans l'Union, ou sur plus de 1 million d'utilisateurs de ce moteur de recherche en ligne dans l'Union, le plus petit nombre étant retenu.

Article 13

Incidents importants concernant les fournisseurs de plateformes de services de réseaux sociaux

En ce qui concerne les fournisseurs de plateformes de services de réseaux sociaux, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) une plateforme de services de réseaux sociaux est totalement indisponible pour plus de 5 % des utilisateurs de cette plateforme dans l'Union, ou pour plus de 1 million d'utilisateurs de cette plateforme dans l'Union, le plus petit nombre étant retenu;

b) plus de 5 % des utilisateurs d'une plateforme de services de réseaux sociaux dans l'Union, ou plus de 1 million d'utilisateurs d'une plateforme de services de réseaux sociaux dans l'Union, le plus petit nombre étant retenu, sont touchés par la disponibilité limitée de cette plateforme;

c) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'une plateforme de services de réseaux sociaux est compromise par une action suspectée d'être malveillante,

d) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'une plateforme de services de réseaux sociaux est compromise, ce qui a un impact sur plus de 5 % des utilisateurs de cette plateforme dans l'Union, ou sur plus de 1 million d'utilisateurs de cette plateforme dans l'Union, le plus petit nombre étant retenu.

Article 14

Incidents importants concernant les fournisseurs de services de confiance

En ce qui concerne les fournisseurs de services de confiance, un incident est considéré comme important au sens de l'article 3, paragraphe 1, point g), lorsqu'il remplit un ou plusieurs des critères suivants:

a) un service de confiance est totalement indisponible pendant plus de 20 minutes;

b) un service de confiance est indisponible pour les utilisateurs ou les parties utilisatrices pendant plus d'une heure, le calcul étant effectué sur la base d'une semaine civile;

c) plus de 1 % des utilisateurs ou des parties utilisatrices dans l'Union, ou plus de 200 000 utilisateurs ou parties utilisatrices dans l'Union, le plus petit nombre étant retenu, sont touchés par la disponibilité limitée de ce service de confiance;

d) l'accès physique à une zone où sont situés des réseaux et des systèmes d'information et dont l'accès est limité au personnel de confiance du fournisseur de services de confiance, ou bien la protection de cet accès physique, est compromis;

e) l'intégrité, la confidentialité ou l'authenticité des données stockées, transmises ou traitées liées à la fourniture d'un service de confiance est compromise, ce qui a un impact sur plus de 0,1 % des utilisateurs ou des parties utilisatrices, ou sur plus de 100 utilisateurs ou parties utilisatrices de ce service de confiance dans l'Union, le plus petit nombre étant retenu.

Article 15

Abrogation

Le règlement d'exécution (UE) 2018/151 ([4]) de la Commission est abrogé.

Article 16

Entrée en vigueur et application

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 17 octobre 2024.

Par la Commission
La présidente
Ursula VON DER LEYEN

([4]) Règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif (JO L 26 du 31.1.2018, p. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

ANNEXE

Exigences techniques et méthodologiques visées à l'article 2 du présent règlement

1. **Politique relative à la sécurité des réseaux et des systèmes d'information [article 21, paragraphe 2, point a), de la directive (UE) 2022/2555]**

1.1. *Politique relative à la sécurité des réseaux et des systèmes d'information*

1.1.1. Aux fins de l'article 21, paragraphe 2, point a), de la directive (UE) 2022/2555, la politique relative à la sécurité des réseaux et des systèmes d'information:

a) définit l'approche que les entités concernées suivent pour gérer la sécurité de leurs réseaux et de leurs systèmes d'information;

b) est adaptée et apporte un complément à la stratégie et aux objectifs économiques des entités concernées;

c) fixe des objectifs en matière de sécurité des réseaux et de l'information;

d) comprend un engagement à améliorer de façon continue la sécurité des réseaux et des systèmes d'information;

e) comprend un engagement à fournir les ressources appropriées pour sa mise en œuvre, y compris le personnel, les moyens financiers, les procédures, les outils et les technologies nécessaires;

f) est communiquée aux membres du personnel concernés et aux tiers concernés, qui en prennent acte;

g) définit les rôles et les responsabilités conformément au point 1.2;

h) dresse la liste des documents à conserver en indiquant leur durée de conservation;

i) énumère les politiques concernant des domaines spécifiques;

j) définit des indicateurs et des mesures pour suivre sa mise en œuvre, ainsi que le stade de maturité atteint par les entités concernées en ce qui concerne la sécurité des réseaux et de l'information;

k) indique la date d'approbation formelle par les organes de direction des entités concernées (ci-après les «organes de direction»).

1.1.2. La politique relative à la sécurité des réseaux et des systèmes d'information est réexaminée et, s'il est besoin, mise à jour par les organes de direction au moins chaque année, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent. Le résultat de ces réexamens est consigné.

1.2. *Rôles, responsabilités et pouvoirs*

1.2.1. Dans le cadre de leur politique relative à la sécurité des réseaux et des systèmes d'information visée au point 1.1, les entités concernées définissent les responsabilités et les pouvoirs en matière de sécurité des réseaux et des systèmes d'information; elles les associent à des rôles, les répartissent en fonction de leurs besoins et en informent leurs organes de direction.

1.2.2. Les entités concernées exigent de l'ensemble du personnel et des tiers qu'ils appliquent les mesures de sécurité des réseaux et des systèmes d'information conformément à leur politique établie en matière de sécurité des réseaux et de l'information, à leurs politiques concernant des domaines spécifiques et à leurs procédures respectives.

1.2.3. Au moins une personne fait directement rapport aux organes de direction sur les questions relatives à la sécurité des réseaux et des systèmes d'information.

1.2.4. Selon la taille des entités concernées, la sécurité des réseaux et des systèmes d'information relève de rôles ou de fonctions spécifiques assumés en sus des rôles existants.

1.2.5. Les fonctions et les domaines de responsabilité incompatibles sont dissociés, s'il y a lieu.

1.2.6. Les rôles, les responsabilités et les pouvoirs sont réexaminés et, s'il est besoin, mis à jour par les organes de direction à intervalles prédéfinis, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

2. **Politique de gestion des risques [article 21, paragraphe 2, point a), de la directive (UE) 2022/2555]**

2.1. *Cadre de gestion des risques*

2.1.1. Aux fins de l'article 21, paragraphe 2, point a), de la directive (UE) 2022/2555, les entités concernées établissent et maintiennent un cadre approprié pour la gestion des risques afin d'identifier les risques pour la sécurité des réseaux et des systèmes d'information et d'y apporter une réponse. Les entités concernées réalisent des évaluations des risques, qu'elles consignent, et, sur la base des résultats obtenus, elles établissent, mettent en œuvre et suivent un plan de traitement des risques. Les résultats de l'évaluation des risques et les risques résiduels sont approuvés par les organes de direction ou, s'il y a lieu, par des personnes qui sont tenues de rendre des comptes et sont habilitées à gérer les risques, à condition que les entités concernées fassent rapport de manière adéquate aux organes de direction.

2.1.2. Aux fins du point 2.1.1, les entités concernées établissent des procédures d'identification, d'analyse, d'évaluation et de traitement des risques (ci-après la «procédure de gestion des risques de cybersécurité»). La procédure de gestion des risques de cybersécurité fait partie intégrante de la procédure globale de gestion des risques des entités concernées, s'il y a lieu. Dans le cadre de la procédure de gestion des risques de cybersécurité, les entités concernées:

a) suivent une méthodologie de gestion des risques;

b) établissent le niveau de tolérance au risque en fonction de leur propension au risque;

c) définissent et maintiennent les critères de risque pertinents;

d) en suivant une approche «tous risques», identifient et consignent les risques pour la sécurité des réseaux et des systèmes d'information, en particulier en ce qui concerne les tiers et les risques susceptibles de perturber la disponibilité, l'intégrité, l'authenticité et la confidentialité des réseaux et des systèmes d'information, y compris l'identification de points uniques de défaillance;

e) analysent les risques qui pèsent sur la sécurité des réseaux et des systèmes d'information, y compris la menace, la probabilité, l'impact et le niveau de risque, en tenant compte des renseignements sur les cybermenaces et des vulnérabilités;

f) évaluent les risques identifiés en se fondant sur les critères de risque;

g) déterminent et hiérarchisent les options et les mesures qu'il convient d'appliquer en matière de traitement des risques;

h) suivent en continu la mise en œuvre des mesures de traitement du risque;

i) déterminent qui est responsable de la mise en œuvre des mesures de traitement des risques et quand celles-ci devraient être mises en œuvre;

j) consignent de manière compréhensible dans un plan de traitement des risques les mesures de traitement des risques choisies et les raisons justifiant l'acceptation des risques résiduels.

2.1.3. Lorsqu'elles identifient et hiérarchisent les options et les mesures de traitement des risques qu'il convient d'appliquer, les entités concernées tiennent compte des résultats de l'évaluation des risques, des résultats de la procédure d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité, du coût de la mise en œuvre par rapport à l'avantage escompté, de la classification des actifs visée au point 12.1 et du bilan d'impact sur l'activité visé au point 4.1.3.

2.1.4. Les entités concernées réexaminent et, s'il est besoin, mettent à jour les résultats de l'évaluation des risques et le plan de traitement des risques à intervalles prédéfinis et au moins chaque année, et lorsque des changements majeurs concernant les opérations ou les risques se produisent, ou lorsque des incidents importants surviennent.

2.2. *Contrôle de la conformité*

2.2.1. Les entités concernées réexaminent régulièrement la conformité avec leurs politiques en matière de sécurité des réseaux et des systèmes d'information, les politiques concernant des domaines spécifiques, les règles et les normes. Les organes de direction sont informés, au moyen de rapports réguliers établis sur la base des examens de conformité, du stade atteint en matière de sécurité des réseaux et de l'information.

2.2.2. Les entités concernées mettent en place un système de rapports de conformité efficace et adapté à leur structure, à l'environnement dans lequel elles opèrent et à leur paysage des menaces. Le système de rapports de conformité est de nature à donner aux organes de direction une vision fiable du stade atteint par les entités concernées en matière de gestion des risques.

2.2.3. Les entités concernées procèdent à un contrôle de conformité à intervalles prédéfinis ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

2.3. *Réexamen indépendant de la sécurité de l'information et des réseaux*

2.3.1. Les entités concernées réexaminent en toute indépendance leur approche de la gestion de la sécurité des réseaux et des systèmes d'information et sa mise en œuvre, y compris en ce qui concerne les effectifs, les procédures et les technologies.

2.3.2. Les entités concernées élaborent et maintiennent les procédures à suivre en vue de réaliser des réexamens indépendants, lesquels seront confiés à des personnes possédant les compétences appropriées en matière d'audit. Lorsque le réexamen indépendant est réalisé par des membres du personnel de l'entité concernée, les personnes qui en sont chargées ne se trouvent pas sous l'autorité hiérarchique du personnel du domaine faisant l'objet du réexamen. Si la taille des entités concernées ne permet pas une telle indépendance vis-à-vis de l'autorité hiérarchique, les entités concernées mettent en place d'autres mesures pour garantir l'impartialité des réexamens.

2.3.3. Les résultats des réexamens indépendants, y compris les résultats du contrôle de la conformité prévu au point 2.2 ainsi que du suivi et du mesurage prévus au point 7, sont communiqués aux organes de direction. Des mesures correctrices sont prises ou le risque résiduel est accepté conformément aux critères d'acceptation des risques des entités concernées.

2.3.4. Les réexamens indépendants ont lieu à intervalles prédéfinis et en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

3. **Gestion des incidents [article 21, paragraphe 2, point b), de la directive (UE) 2022/2555]**

3.1. *Politique de gestion des incidents*

3.1.1. Aux fins de l'article 21, paragraphe 2, point b), de la directive (UE) 2022/2555, les entités concernées établissent et mettent en œuvre, en temps utile, une politique de gestion des incidents qui définit les rôles, les responsabilités et les procédures permettant de détecter, d'analyser, d'endiguer un incident ou d'y réagir, ainsi que de rétablir la situation, de consigner l'incident et de faire rapport.

3.1.2. La politique visée au point 3.1.1 est compatible avec le plan de continuité de l'activité et de rétablissement visé au point 4.1. Cette politique comprend:

a) un système de catégorisation des incidents compatible avec l'évaluation et la classification des événements effectuées conformément au point 3.4.1;

b) des plans de communication efficaces, y compris pour la remontée de l'information et l'établissement des rapports;

c) l'attribution aux membres du personnel compétents de rôles en vue de détecter les incidents et d'y réagir de manière appropriée;

d) les documents à utiliser dans le cadre de la détection et de la réaction aux incidents, tels que des guides d'intervention, des diagrammes de remontée de l'information, des listes de contacts et des modèles.

3.1.3. Les rôles, les responsabilités et les procédures définis dans la politique sont testés, réexaminés et, s'il est besoin, mis à jour à intervalles prédéfinis, ainsi qu'après des incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se sont produits.

3.2. *Surveillance et journalisation*

3.2.1. Les entités concernées établissent des procédures et utilisent des outils pour surveiller et journaliser les activités sur leurs réseaux et dans leurs systèmes d'information afin de détecter les événements qui pourraient être considérés comme des incidents et de réagir en conséquence pour en atténuer l'impact.

3.2.2. Dans la mesure du possible, la surveillance est automatisée et réalisée soit en continu soit à intervalles réguliers, sous réserve de capacités opérationnelles. Les entités concernées mettent en œuvre leurs activités de surveillance de manière à réduire au minimum les faux positifs et les faux négatifs.

3.2.3. Sur la base des procédures visées au point 3.2.1, les entités concernées tiennent des journaux, les documentent et les réexaminent. Les entités concernées établissent une liste des actifs devant faire l'objet d'une journalisation sur la base des résultats de l'évaluation des risques effectuée conformément au point 2.1. Les journaux comprennent, s'il est besoin:

a) le trafic sortant et entrant pertinent sur les réseaux;

b) la création, la modification ou la suppression d'utilisateurs sur les réseaux et dans les systèmes d'information des entités concernées, ainsi que l'extension des autorisations;

c) l'accès aux systèmes et aux applications;

d) les événements liés à l'authentification;

e) tous les accès privilégiés aux systèmes et aux applications, ainsi que les activités exercées par les comptes d'administration;

f) l'accès aux fichiers critiques de configuration et de sauvegarde, ou leur modification;

g) les journaux d'événements et les journaux des outils de sécurité, tels que les antivirus, les systèmes de détection d'intrusion ou les pare-feu;

h) l'utilisation des ressources du système, ainsi que leur performance;

i) l'accès physique aux installations;

j) l'accès à leurs équipements et dispositifs de réseau et leur utilisation;

k) l'activation, l'arrêt et la suspension des divers journaux;

l) les événements liés à l'environnement.

3.2.4. Les journaux sont régulièrement réexaminés pour détecter toute tendance inhabituelle ou indésirable. Les entités concernées fixent, s'il est besoin, les valeurs appropriées correspondant à des seuils d'alarme. Si les valeurs prescrites pour un seuil d'alarme sont dépassées, une alarme est déclenchée, s'il est besoin, de manière automatique. Les entités concernées veillent à ce que, en cas d'alarme, une réponse spécifique et appropriée soit activée en temps utile.

3.2.5. Les entités concernées tiennent les journaux et en font des sauvegardes pendant une période prédéfinie; elles les protègent contre tout accès non autorisé ou toute modification non autorisée.

3.2.6. Dans la mesure du possible, les entités concernées veillent à ce que tous les systèmes disposent d'horloges synchronisées pour être en mesure de corréler les journaux entre les différents systèmes aux fins de l'évaluation des événements. Les entités concernées établissent et tiennent à jour une liste de tous les actifs qui font l'objet d'une journalisation et veillent à ce que les systèmes de surveillance et de journalisation soient redondants. La disponibilité des systèmes de surveillance et de journalisation est contrôlée indépendamment des systèmes soumis à leur surveillance.

3.2.7. Les procédures ainsi que la liste des actifs qui font l'objet d'une journalisation sont réexaminées et, s'il est besoin, mises à jour à intervalles réguliers et à la suite d'incidents importants.

3.3. *Signalement des événements*

3.3.1. Les entités concernées mettent en place un mécanisme simple permettant à leurs membres du personnel, fournisseurs et clients de signaler les événements suspects.

3.3.2. Les entités concernées informent, s'il est besoin, leurs fournisseurs et leurs clients du mécanisme de signalement des événements et dispensent régulièrement à leur personnel une formation à l'utilisation de ce mécanisme.

3.4. *Évaluation et classification des événements*

3.4.1. Les entités concernées évaluent les événements suspects afin de déterminer s'ils constituent des incidents et, dans l'affirmative, en déterminent la nature et la gravité.

3.4.2. Aux fins du point 3.4.1, les entités concernées procèdent de la façon suivante:

a) elles effectuent l'évaluation sur la base de critères prédéfinis établis à l'avance et d'un triage afin d'établir une hiérarchisation des mesures d'endiguement et d'éradication des incidents;

b) elles examinent chaque trimestre si des incidents récurrents tels que décrits à l'article 4 du présent règlement sont survenus;

c) elles passent en revue les journaux appropriés aux fins de l'évaluation et de la classification des événements;

d) elles mettent en place une procédure de corrélation et d'analyse des journaux; et

e) elles réévaluent et reclassent les événements si de nouvelles informations deviennent disponibles ou après analyse d'informations qu'elles possédaient déjà.

3.5. *Réponse aux incidents*

3.5.1. Les entités concernées apportent une réponse aux incidents dans le respect de procédures documentées et en temps utile.

3.5.2. Les procédures de réponse aux incidents comprennent les étapes suivantes:

a) endiguement, afin d'éviter que les conséquences de l'incident ne se propagent;

b) éradication, afin d'éviter que l'incident ne se poursuive ou se reproduise,

c) rétablissement après l'incident, si nécessaire.

3.5.3. Les entités concernées établissent des plans et des procédures de communication:

a) avec les centres de réponse aux incidents de sécurité informatique (CSIRT) ou, s'il y a lieu, avec les autorités compétentes, en rapport avec la notification des incidents;

b) pour la communication entre les membres du personnel de l'entité concernée et pour la communication avec les parties prenantes extérieures à l'entité concernée.

3.5.4. Les entités concernées tiennent un journal des activités de réponse aux incidents conformément aux procédures visées au point 3.2.1 et en conservent des preuves.

3.5.5. Les entités concernées testent leurs procédures de réponse aux incidents à intervalles prédéfinis.

3.6. *Examens postincident*

3.6.1. Les entités concernées procèdent, s'il est besoin, à des examens postincident après le rétablissement. Les examens postincident servent à identifier, dans la mesure du possible, la cause profonde de l'incident et à en tirer des enseignements, documents à l'appui, afin de limiter la survenance et les conséquences d'incidents futurs.

3.6.2. Les entités concernées veillent à ce que les examens postincident contribuent à améliorer leur approche de la sécurité des réseaux et de l'information, du traitement des risques ainsi que des procédures de gestion et de détection des incidents et de réponse aux incidents.

3.6.3. Les entités concernées examinent à intervalles prédéfinis si des incidents ont donné lieu à des examens postincident.

4. **Continuité des activités et gestion des crises [article 21, paragraphe 2, point c), de la directive (UE) 2022/2555]**

4.1. *Plan de continuité de l'activité et de rétablissement*

4.1.1. Aux fins de l'article 21, paragraphe 2, point c), de la directive (UE) 2022/2555, les entités concernées établissent et maintiennent un plan de continuité de l'activité et de rétablissement qui devra être appliqué en cas d'incidents.

4.1.2. Les entités concernées rétablissent leurs opérations conformément au plan de continuité de l'activité et de rétablissement. Le plan est fondé sur les résultats de l'évaluation des risques effectuée conformément au point 2.1 et comprend, s'il est besoin, les informations suivantes:

a) objet, champ d'application et public;

b) rôles et responsabilités;

c) principales personnes de contact et canaux de communication (internes et externes);

d) conditions d'activation et de désactivation du plan;

e) ordre de rétablissement des opérations;

f) plans de rétablissement pour les opérations spécifiques, y compris les objectifs de rétablissement;

g) ressources nécessaires, y compris les sauvegardes et les ressources redondantes;

h) activités restaurées et rétablies à partir de mesures temporaires.

4.1.3. Les entités concernées effectuent un bilan d'impact sur l'activité afin d'évaluer l'impact potentiel de perturbations graves de leurs opérations et définissent, sur la base des résultats du bilan d'impact sur l'activité, des exigences de continuité pour les réseaux et les systèmes d'information.

4.1.4. Le plan de continuité de l'activité et le plan de rétablissement sont testés, réexaminés et, s'il est besoin, mis à jour à intervalles prédéfinis, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent. Les entités concernées veillent à ce que les plans tiennent compte des enseignements tirés de ces tests.

4.2. *Gestion des sauvegardes et des ressources redondantes*

4.2.1. Les entités concernées conservent des copies de sauvegarde des données et prévoient suffisamment de ressources disponibles, y compris des installations, des réseaux et des systèmes d'information, ainsi que du personnel, afin de garantir un niveau approprié de redondance.

4.2.2. Sur la base des résultats de l'évaluation des risques effectuée conformément au point 2.1 et du plan de continuité de l'activité, les entités concernées établissent des plans de sauvegarde qui comprennent les informations suivantes:

a) le délai de rétablissement de l'activité;

b) la preuve que les copies de sauvegarde sont complètes et exactes, y compris les données de configuration et les données stockées dans un environnement de services d'informatique en nuage;

c) le stockage de copies de sauvegarde (en ligne ou hors ligne) dans un ou plusieurs endroits sûrs, qui ne se trouvent pas sur le même réseau que le système et qui sont situés à une distance suffisante pour échapper à tout dommage causé par une catastrophe sur le site principal;

d) des contrôles d'accès physiques et logiques appropriés pour les copies de sauvegarde, conformément au niveau de classification des actifs;

e) les données restaurées à partir de copies de sauvegarde;

f) les périodes de conservation compte tenu des exigences commerciales et réglementaires.

4.2.3. Les entités concernées procèdent régulièrement à des contrôles d'intégrité des copies de sauvegarde.

4.2.4. Sur la base des résultats de l'évaluation des risques effectuée conformément au point 2.1 et du plan de continuité de l'activité, les entités concernées veillent à ce que la disponibilité des ressources soit suffisante moyennant une redondance au moins partielle des éléments suivants:

a) réseaux et systèmes d'information;

b) actifs, y compris les installations, les équipements et les fournitures;

c) personnel doté des responsabilités, des pouvoirs et des compétences nécessaires;

d) canaux de communication appropriés.

4.2.5. S'il est besoin, les entités concernées veillent à ce que la surveillance et l'adaptation des ressources, y compris les installations, les systèmes et le personnel, soient dûment guidées par le respect des exigences en matière de sauvegarde et de redondance.

4.2.6. Les entités concernées procèdent régulièrement à des tests de récupération des copies de sauvegarde et des ressources redondantes afin de s'assurer que, dans des conditions de rétablissement, elles puissent être utilisées de manière fiable et englober les copies, les procédures et les connaissances nécessaires pour procéder à un rétablissement efficace. Les entités concernées consignent les résultats des tests et, si nécessaire, adoptent des mesures correctrices.

4.3. *Gestion des crises*

4.3.1. Les entités concernées mettent en place une procédure de gestion des crises.

4.3.2. Les entités concernées veillent à ce que la procédure de gestion des crises porte au moins sur les aspects suivants:

a) les rôles et responsabilités du personnel et, s'il est besoin, des fournisseurs et des prestataires de services, en précisant la répartition des rôles dans les situations de crise, y compris les étapes spécifiques à suivre;

b) des moyens de communication appropriés entre les entités concernées et les autorités compétentes concernées;

c) l'application de mesures appropriées pour garantir le maintien de la sécurité des réseaux et des systèmes d'information dans les situations de crise.

Aux fins du point b), le flux d'informations entre les entités concernées et les autorités compétentes concernées comprend tant les communications obligatoires, telles que les rapports d'incidents et les délais correspondants, que les communications non obligatoires.

4.3.3. Les entités concernées appliquent une procédure de gestion et d'utilisation des informations reçues des CSIRT ou, s'il y a lieu, des autorités compétentes, concernant les incidents, les vulnérabilités, les menaces ou les éventuelles mesures d'atténuation.

4.3.4. Les entités concernées testent, réexaminent et, s'il est besoin, mettent à jour le plan de gestion des crises de façon régulière, à la suite d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

5. **Sécurité de la chaîne d'approvisionnement [article 21, paragraphe 2, point d), de la directive (UE) 2022/2555]**

5.1. *Politique de sécurité de la chaîne d'approvisionnement*

5.1.1. Aux fins de l'article 21, paragraphe 2, point d), de la directive (UE) 2022/2555, les entités concernées établissent, mettent en œuvre et appliquent une politique de sécurité de la chaîne d'approvisionnement régissant les relations avec leurs fournisseurs et leurs prestataires de services directs afin d'atténuer les risques identifiés pour la sécurité des réseaux et des systèmes d'information. Dans la politique de sécurité de la chaîne d'approvisionnement, les entités concernées définissent leur rôle dans la chaîne d'approvisionnement et en informent leurs fournisseurs et leurs prestataires de services directs.

5.1.2. Dans le cadre de la politique visée au point 5.1.1, les entités concernées fixent des critères pour la sélection des fournisseurs et des prestataires de services et la passation de contrats avec ces derniers. Ces critères incluent:

a) les pratiques des fournisseurs et des prestataires de services en matière de cybersécurité, y compris leurs procédures de développement sécurisé;

b) la capacité des fournisseurs et des prestataires de services de se conformer aux spécifications de cybersécurité définies par les entités concernées;

c) la qualité et la résilience globales des produits TIC et des services TIC et les mesures de gestion des risques en matière de cybersécurité qui y sont intégrées, y compris les risques et le niveau de classification des produits TIC et des services TIC;

d) la capacité des entités concernées à diversifier les sources d'approvisionnement et à limiter l'effet de verrouillage, s'il y a lieu.

5.1.3. Lorsqu'elles établissent leur politique de sécurité de la chaîne d'approvisionnement, les entités concernées tiennent compte des résultats des évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement critiques effectuées conformément à l'article 22, paragraphe 1, de la directive (UE) 2022/2555, s'il y a lieu.

5.1.4. Sur la base de la politique de sécurité de la chaîne d'approvisionnement et compte tenu des résultats de l'évaluation des risques effectuée conformément au point 2.1 de la présente annexe, les entités concernées veillent à ce que les contrats passés avec les fournisseurs et les prestataires de services précisent, s'il est besoin et le cas échéant au moyen d'accords de niveau de service, les éléments suivants:

a) les exigences en matière de cybersécurité applicables aux fournisseurs ou aux prestataires de services, y compris les exigences relatives à la sécurité de l'acquisition de services TIC ou de produits TIC énoncées au point 6.1;

b) les exigences en matière de sensibilisation, de compétences et de formation et, s'il est besoin, les certifications requises à l'égard du personnel des fournisseurs ou des prestataires de services;

c) les exigences relatives à la vérification des antécédents du personnel des fournisseurs et des prestataires de services;

d) l'obligation pour les fournisseurs et les prestataires de services de notifier sans retard injustifié aux entités concernées les incidents qui présentent un risque pour la sécurité des réseaux et des systèmes d'information de ces entités;

e) le droit d'effectuer des audits ou le droit de recevoir des rapports d'audit;

f) l'obligation pour les fournisseurs et les prestataires de services de gérer les vulnérabilités qui présentent un risque pour la sécurité des réseaux et des systèmes d'information des entités concernées;

g) les exigences relatives à la sous-traitance et, si les entités concernées autorisent la sous-traitance, les exigences en matière de cybersécurité applicables aux sous-traitants conformément aux exigences en matière de cybersécurité visées au point a);

h) les obligations incombant aux fournisseurs et aux prestataires de services au terme du contrat, telles que la récupération et la destruction des informations obtenues par les fournisseurs et les prestataires de services dans l'exercice de leur mission.

5.1.5. Les entités concernées tiennent compte des éléments visés aux points 5.1.2 et 5.1.3 dans le cadre de la procédure de sélection de nouveaux fournisseurs et prestataires de services, ainsi que de la procédure de passation de marchés visée au point 6.1.

5.1.6. Les entités concernées réexaminent la politique de sécurité de la chaîne d'approvisionnement et elles surveillent, évaluent et, si nécessaire, réagissent à l'évolution des pratiques en matière de cybersécurité des fournisseurs et des prestataires de services à intervalles prédéfinis et lorsque des changements majeurs concernant les opérations ou les risques se produisent, ou en cas d'incidents importants liés à la fourniture de services TIC ou ayant un impact sur la sécurité des produits TIC provenant de fournisseurs et de prestataires de services.

5.1.7. Aux fins du point 5.1.6, les entités concernées:

a) passent régulièrement en revue les rapports sur la mise en œuvre des accords de niveau de service, s'il y a lieu;

b) examinent les incidents liés aux produits TIC et aux services TIC provenant de fournisseurs et de prestataires de services;

c) évaluent la nécessité de réexamens non programmés et en consignent les conclusions de manière compréhensible;

d) analysent, en temps utile, les risques présentés par les changements liés aux produits TIC et aux services TIC provenant des fournisseurs et des prestataires de services et, s'il est besoin, prennent des mesures d'atténuation.

5.2. *Annuaire des fournisseurs et des prestataires de services*

Les entités concernées conservent et tiennent à jour un registre de leurs fournisseurs et prestataires de services directs comprenant:

a) les points de contact pour chaque fournisseur et prestataire de services direct;

b) une liste des produits TIC, services TIC et processus TIC fournis aux entités concernées par le fournisseur ou le prestataire de services direct.

6. **Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information [article 21, paragraphe 2, point e), de la directive (UE) 2022/2555]**

6.1. *Sécurité de l'acquisition des services TIC ou des produits TIC*

6.1.1. Aux fins de l'article 21, paragraphe 2, point e), de la directive (UE) 2022/2555, les entités concernées définissent et utilisent des procédures en vue de gérer, sur la base de l'évaluation des risques effectuée conformément au point 2.1, les risques découlant de l'acquisition de services TIC ou de produits TIC auprès de fournisseurs ou de prestataires de services pour des composants qui sont critiques pour la sécurité des réseaux et des systèmes d'information des entités concernées tout au long de leur cycle de vie.

6.1.2. Aux fins du point 6.1.1, les procédures précitées comprennent:

a) les exigences de sécurité applicables aux services TIC ou produits TIC à acquérir;

b) les exigences concernant les mises à jour de sécurité pendant toute la durée de vie des services TIC ou des produits TIC, ou leur remplacement au terme de la période d'assistance;

c) les informations décrivant les composants matériels et logiciels utilisés dans les services TIC ou les produits TIC;

d) les informations décrivant les fonctions de cybersécurité des services TIC ou des produits TIC mises en œuvre et la configuration nécessaire à leur fonctionnement sécurisé;

e) l'assurance que les services TIC ou les produits TIC sont conformes aux exigences de sécurité visées au point a);

f) les méthodes permettant de valider la conformité des services TIC ou des produits TIC fournis aux exigences de sécurité énoncées, ainsi que la consignation des résultats de la validation.

6.1.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour les procédures à intervalles prédéfinis, ainsi qu'en cas d'incidents importants.

6.2. *Cycle de vie du développement sécurisé*

6.2.1. Avant de développer un réseau et un système d'information, y compris des logiciels, les entités concernées établissent des règles pour le développement sécurisé des réseaux et des systèmes d'information et les appliquent lorsqu'elles développent des réseaux et des systèmes d'information en interne ou lorsqu'elles externalisent le développement de réseaux et de systèmes d'information. Les règles couvrent toutes les phases du développement, y compris la spécification, la conception, le développement lui-même, la mise en œuvre et les tests.

6.2.2. Aux fins du point 6.2.1, les entités concernées:

a) effectuent une analyse des exigences de sécurité au cours des phases de spécification et de conception de tout projet de développement ou d'acquisition mené par elles-mêmes ou pour leur compte;

b) appliquent les principes de l'ingénierie des systèmes sécurisés et du codage sécurisé à toute activité de développement de systèmes d'information, tels que la promotion de la cybersécurité dès la conception et les architectures à vérification systématique;

c) énoncent des exigences de sécurité en ce qui concerne les environnements de développement;

d) établissent et utilisent des procédures de tests de sécurité au cours du cycle de vie du développement;

e) sélectionnent, protègent et gèrent de manière appropriée les données relatives aux tests de sécurité;

f) nettoient et anonymisent les données relatives aux tests conformément à l'évaluation des risques effectuée conformément au point 2.1.

6.2.3. Lorsque le développement des réseaux et des systèmes d'information est externalisé, les entités concernées appliquent également les politiques et procédures visées aux points 5 et 6.1.

6.2.4. Les entités concernées réexaminent et, si nécessaire, actualisent à intervalles prédéfinis leurs règles de développement sécurisé.

6.3. *Gestion des configurations*

6.3.1. Les entités concernées prennent les mesures appropriées pour établir, documenter, mettre en œuvre et surveiller les configurations, y compris les configurations de sécurité du matériel, des logiciels, des services et des réseaux.

6.3.2. Aux fins du point 6.3.1, les entités concernées:

a) définissent et appliquent des configurations de sécurité pour leur matériel, leurs logiciels, leurs services et leurs réseaux;

b) définissent et utilisent des procédures et des outils pour assurer le respect des configurations sécurisées définies pour le matériel, les logiciels, les services et les réseaux, pour les systèmes récemment installés ainsi que pour les systèmes déjà en exploitation, pendant toute leur durée de vie.

6.3.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour les configurations à intervalles prédéfinis, ou en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

6.4. *Gestion des changements, réparations et entretien*

6.4.1. Les entités concernées appliquent des procédures de gestion des changements pour encadrer les changements de réseaux et de systèmes d'information. S'il y a lieu, les procédures sont compatibles avec la politique générale des entités concernées en matière de gestion des changements.

6.4.2. Les procédures visées au point 6.4.1 doivent être appliquées pour les nouvelles versions, les modifications et les changements urgents apportés à tout logiciel et matériel en exploitation, ainsi que pour toute modification de la configuration. Les procédures garantissent que ces changements sont consignés et, sur la base de l'évaluation des risques effectuée conformément au point 2.1, qu'ils vont être testés et évalués au regard de leur impact potentiel avant d'être mis en œuvre.

6.4.3. Dans le cas où les procédures habituelles de gestion des changements n'ont pas pu être suivies en raison d'une urgence, les entités concernées consignent le résultat des changements et les raisons pour lesquelles les procédures n'ont pas pu être suivies.

6.4.4. Les entités concernées réexaminent et, s'il est besoin, mettent à jour les procédures à intervalles prédéfinis, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

6.5. *Tests de sécurité*

6.5.1. Les entités concernées établissent, mettent en œuvre et appliquent une politique et des procédures en matière de tests de sécurité.

6.5.2. Les entités concernées:

a) déterminent, sur la base de l'évaluation des risques effectuée conformément au point 2.1, la nécessité, la portée, la fréquence et le type de tests de sécurité;

b) effectuent, selon une méthode de test documentée, des tests de sécurité couvrant les composants identifiés dans le cadre d'une analyse des risques comme étant importants pour une exploitation sûre;

c) consignent le type, la portée, la date et les résultats des tests, y compris l'évaluation de la criticité et des mesures d'atténuation pour chaque constat;

d) appliquent des mesures d'atténuation en cas de constats critiques.

6.5.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour à intervalles prédéfinis leur politique en matière de tests de sécurité.

6.6. *Gestion des correctifs de sécurité*

6.6.1. Les entités concernées précisent et appliquent des procédures compatibles avec les procédures de gestion des changements visées au point 6.4.1, ainsi qu'avec la gestion des vulnérabilités, la gestion des risques et d'autres procédures de gestion pertinentes, pour garantir que:

a) les correctifs de sécurité sont appliqués dans un délai raisonnable après leur mise à disposition;

b) les correctifs de sécurité sont testés avant d'être appliqués dans les systèmes de production;

c) les correctifs de sécurité proviennent de sources fiables et font l'objet d'un contrôle d'intégrité;

d) des mesures supplémentaires sont mises en œuvre et que les risques résiduels sont acceptés lorsqu'un correctif n'est pas disponible ou n'est pas appliqué conformément au point 6.6.2.

6.6.2. Par dérogation au point 6.6.1 a), les entités concernées peuvent choisir de ne pas appliquer de correctifs de sécurité lorsque les inconvénients de leur application l'emportent sur les avantages en matière de cybersécurité. Les entités concernées documentent et justifient dûment les motifs d'un tel choix.

6.7. *Sécurité des réseaux*

6.7.1. Les entités concernées prennent les mesures appropriées pour protéger leurs réseaux et systèmes d'information contre les cybermenaces.

6.7.2. Aux fins du point 6.7.1, les entités concernées:

a) consignent des informations compréhensibles et actualisées sur l'architecture du réseau;

b) déterminent et appliquent des contrôles pour protéger les domaines de réseau internes des entités concernées contre tout accès non autorisé;

c) configurent les contrôles pour empêcher les accès et la communication par réseau qui ne sont pas nécessaires au fonctionnement des entités concernées;

d) déterminent et appliquent des contrôles pour l'accès à distance aux réseaux et aux systèmes d'information, y compris l'accès par des prestataires de services;

e) n'utilisent pas à d'autres fins les systèmes utilisés pour la gestion de la mise en œuvre de la politique de sécurité;

f) interdisent explicitement ou désactivent les connexions et les services non nécessaires;

g) s'il est besoin, autorisent exclusivement l'accès aux réseaux et aux systèmes d'information des entités concernées au moyen de dispositifs autorisés par ces entités;

h) n'autorisent les connexions de prestataires de services qu'à la suite d'une demande d'autorisation et pour une durée déterminée, telle que la durée d'une opération de maintenance;

i) établissent une communication entre des systèmes distincts uniquement par des canaux de confiance isolés des autres canaux de communication au moyen d'une séparation logique, cryptographique ou physique et prévoient une identification assurée de leurs points terminaux et la protection des données du canal contre toute modification ou divulgation;

j) adoptent un plan de mise en œuvre pour la transition complète vers des protocoles de communication de la dernière génération au niveau de la couche réseau d'une manière sûre, appropriée et progressive, et prennent des mesures pour accélérer cette transition;

k) adoptent un plan de mise en œuvre pour le déploiement de normes de communication par courrier électronique modernes, reconnues et interopérables au niveau international, afin de sécuriser les communications par courrier électronique de manière à atténuer les vulnérabilités dues aux menaces liées au courrier électronique et prennent des mesures pour accélérer ce déploiement;

l) appliquent les meilleures pratiques en matière de sécurité du DNS, de sécurité du routage sur internet et d'hygiène du routage pour le trafic en provenance et à destination du réseau.

6.7.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour ces mesures à intervalles prédéfinis, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

6.8. *Segmentation du réseau*

6.8.1. Les entités concernées segmentent les systèmes en réseaux ou en zones conformément aux résultats de l'évaluation des risques visée au point 2.1. Elles segmentent leurs systèmes et réseaux en les isolant des systèmes et réseaux de tiers.

6.8.2. À cette fin, les entités concernées:

a) prennent en considération le lien fonctionnel, logique et physique, y compris la localisation, entre systèmes et services de confiance;

b) accordent l'accès à un réseau ou à une zone sur la base d'une évaluation de ses exigences en matière de sécurité;

c) conservent les systèmes critiques pour leur exploitation ou pour la sécurité dans les zones sécurisées;

d) déploient une zone démilitarisée au sein de leurs réseaux de communication pour assurer une communication sécurisée en provenance ou à destination de leurs réseaux;

e) limitent l'accès et les communications entre les zones et à l'intérieur de celles-ci à ce qui est nécessaire à leur fonctionnement ou à la sécurité;

f) séparent, d'une part, le réseau consacré à l'administration des réseaux et des systèmes d'information et, d'autre part, leur réseau opérationnel;

g) séparent les canaux d'administration du réseau des autres types de trafic réseau;

h) séparent leurs systèmes de production de services des systèmes utilisés pour le développement et les tests, y compris les sauvegardes.

6.8.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour la segmentation du réseau à intervalles prédéfinis, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

6.9. *Protection contre les logiciels malveillants ou non autorisés*

6.9.1. Les entités concernées protègent leurs réseaux et systèmes d'information contre les logiciels malveillants ou non autorisés.

6.9.2. À cette fin, les entités concernées mettent notamment en œuvre des mesures qui permettent de détecter ou d'empêcher l'utilisation de logiciels malveillants ou non autorisés. Les entités concernées veillent, s'il est besoin, à ce que leurs réseaux et systèmes d'information soient équipés de logiciels de détection et de réponse régulièrement mis à jour selon l'évaluation des risques effectuée conformément au point 2.1 et aux accords contractuels conclus avec les fournisseurs.

6.10. *Gestion et divulgation des vulnérabilités*

6.10.1. Les entités concernées obtiennent des informations sur les vulnérabilités techniques de leurs réseaux et systèmes d'information, évaluent leur exposition à ces vulnérabilités et prennent les mesures appropriées pour gérer ces vulnérabilités.

6.10.2. Aux fins du point 6.10.1, les entités concernées:

a) surveillent les informations sur les vulnérabilités par des canaux appropriés, tels que les annonces des CSIRT ou des autorités compétentes ou les informations fournies par les fournisseurs ou les prestataires de services;

b) effectuent, s'il est besoin, des analyses de vulnérabilité et consignent les résultats des analyses, à intervalles prédéfinis;

c) remédient, dans les meilleurs délais, aux vulnérabilités qu'elles identifient comme étant critiques pour leurs opérations;

d) veillent à ce que leur gestion des vulnérabilités soit compatible avec leurs procédures de gestion des changements, de gestion des correctifs de sécurité, de gestion des risques et de gestion des incidents;

e) établissent une procédure de divulgation des vulnérabilités conformément à la politique nationale applicable en matière de divulgation coordonnée des vulnérabilités.

6.10.3. Lorsque l'impact potentiel de la vulnérabilité le justifie, les entités concernées élaborent et mettent en œuvre un plan visant à atténuer la vulnérabilité. Dans les autres cas, les entités concernées documentent et justifient la raison pour laquelle il n'est pas nécessaire de remédier à la vulnérabilité.

6.10.4. Les entités concernées réexaminent et, s'il est besoin, mettent à jour à intervalles prédéfinis les canaux qu'elles utilisent pour surveiller les informations relatives à la vulnérabilité.

7. **Politiques et procédures visant à évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité [article 21, paragraphe 2, point f), de la directive (UE) 2022/2555]**

7.1. Aux fins de l'article 21, paragraphe 2, point f), de la directive (UE) 2022/2555, les entités concernées établissent, mettent en œuvre et appliquent une politique et des procédures visant à évaluer si les mesures de gestion des risques en matière de cybersécurité qu'elles ont prises sont effectivement mises en œuvre et maintenues.

7.2. La politique et les procédures visées au point 7.1 tiennent compte des résultats de l'évaluation des risques visée au point 2.1 et des incidents importants passés. Les entités concernées déterminent:

a) quelles mesures de gestion des risques en matière de cybersécurité doivent faire l'objet d'un suivi et d'un mesurage, y compris les procédures et les contrôles;

b) quelles méthodes de suivi, de mesurage, d'analyse et d'évaluation, selon le cas, doivent assurer la validité des résultats;

c) quand le suivi et le mesurage doivent être effectués;

d) qui est responsable du suivi et du mesurage de l'efficacité des mesures de gestion des risques en matière de cybersécurité;

e) quand les résultats du suivi et du mesurage doivent être analysés et évalués;

f) qui doit analyser et évaluer ces résultats.

7.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour la politique et les procédures à intervalles prédéfinis, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

8. **Pratiques de base en matière de cyberhygiène et formation à la sécurité [article 21, paragraphe 2, point g), de la directive (UE) 2022/2555]**

8.1. *Sensibilisation et pratiques de base en matière de cyberhygiène*

8.1.1. Aux fins de l'article 21, paragraphe 2, point g), de la directive (UE) 2022/2555, les entités concernées veillent à ce que leurs employés, y compris les membres des organes de direction, ainsi que les fournisseurs et prestataires de services directs soient sensibilisés aux risques, soient informés de l'importance de la cybersécurité et appliquent des pratiques de cyberhygiène.

8.1.2. Aux fins du point 8.1.1, les entités concernées proposent à leurs employés, y compris aux membres des organes de direction, ainsi qu'aux fournisseurs et prestataires de services directs, s'il est besoin conformément au point 5.1.4, un programme de sensibilisation qui:

a) s'échelonne dans le temps de manière à ce que les activités soient répétées et s'adressent aux nouveaux salariés;

b) est établi conformément à la politique de sécurité des réseaux et de l'information, aux politiques concernant des domaines spécifiques et aux procédures pertinentes en matière de sécurité des réseaux et de l'information;

c) couvre les cybermenaces pertinentes, les mesures de gestion des risques en matière de cybersécurité en place, les points de contact et les ressources pour obtenir des informations et des conseils supplémentaires sur les questions de cybersécurité, ainsi que les pratiques de cyberhygiène à l'intention des utilisateurs.

8.1.3. S'il est besoin, l'efficacité du programme de sensibilisation est soumise à des tests. Le programme de sensibilisation est mis à jour et proposé à intervalles prédéfinis en tenant compte de l'évolution des pratiques de cyberhygiène, ainsi que du paysage actuel des menaces et des risques pour les entités concernées.

8.2. *Formation de sécurité*

8.2.1. Les entités concernées identifient les employés dont les rôles nécessitent des compétences et une expertise pertinentes en matière de sécurité, et veillent à ce qu'ils reçoivent régulièrement une formation sur la sécurité des réseaux et des systèmes d'information.

8.2.2. Les entités concernées établissent, mettent en œuvre et appliquent un programme de formation conforme à la politique de sécurité des réseaux et de l'information, aux politiques concernant des domaines spécifiques et aux autres procédures pertinentes en matière de sécurité des réseaux et de l'information, qui définit les besoins de formation pour certains rôles et postes sur la base de critères.

8.2.3. La formation visée au point 8.2.1 est pertinente pour les fonctions exercées par l'employé et son efficacité est évaluée. La formation prend en considération les mesures de sûreté en place et couvre les éléments suivants:

a) instructions concernant la configuration et le fonctionnement sécurisés du réseau et des systèmes d'information, y compris les dispositifs mobiles;

b) informations sur les cybermenaces connues;

c) formation sur le comportement à adopter en cas d'événements touchant à la sécurité.

8.2.4. Les entités concernées dispensent des formations aux membres du personnel qui assument de nouveaux postes ou de nouveaux rôles nécessitant des compétences et une expertise pertinentes en matière de sécurité.

8.2.5. Le programme est mis à jour et organisé périodiquement en tenant compte des politiques et des règles applicables, des rôles et responsabilités assignés, ainsi que des cybermenaces connues et des évolutions technologiques.

9. **Cryptographie [article 21, paragraphe 2, point h), de la directive (UE) 2022/2555]**

9.1. Aux fins de l'article 21, paragraphe 2, point h), de la directive (UE) 2022/2555, les entités concernées établissent, mettent en œuvre et appliquent une politique et des procédures relatives à la cryptographie, en vue de garantir une utilisation adéquate et efficace de la cryptographie afin de protéger la confidentialité, l'authenticité et l'intégrité des données conformément à la classification des actifs des entités concernées et aux résultats de l'évaluation des risques effectuée conformément au point 2.1.

9.2. La politique et les procédures visées au point 9.1 établissent:

a) conformément à la classification des actifs des entités concernées, le type, la solidité et la qualité des mesures cryptographiques requises pour protéger les actifs des entités concernées, y compris les données au repos et les données en transit;

b) sur la base du point a), les protocoles ou familles de protocoles à adopter, ainsi que les algorithmes cryptographiques, la puissance du chiffrement, les solutions cryptographiques et les pratiques d'utilisation à approuver et à utiliser dans les entités concernées, suivant, s'il est besoin, une approche d'agilité cryptographique;

c) l'approche des entités concernées en matière de gestion des clés, y compris, le cas échéant, les méthodes destinées à:

i) générer différentes clés pour les systèmes et applications cryptographiques;

ii) délivrer et obtenir des certificats à clé publique;

iii) distribuer des clés aux entités prévues, y compris la manière d'activer les clés lorsqu'elles sont reçues;

iv) stocker les clés, y compris la manière dont les utilisateurs autorisés obtiennent l'accès aux clés;

v) modifier ou mettre à jour les clés, y compris les règles relatives au moment et à la manière de modifier les clés;

vi) traiter les clés compromises;

vii) révoquer les clés, y compris la manière de retirer ou de désactiver les clés;

viii) récupérer les clés perdues ou corrompues;

ix) effectuer des copies de sauvegarde ou procéder à l'archivage des clés;

x) détruire les clés;

xi) réaliser la journalisation et l'audit des principales activités liées à la gestion;

xii) fixer des dates d'activation et de désactivation pour les clés, afin que celles-ci ne puissent être utilisées que pendant la période spécifiée, conformément aux règles de l'organisation en matière de gestion des clés.

9.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour leur politique et leurs procédures à des intervalles prédéfinis, en tenant compte de l'état des connaissances en matière de cryptographie.

10. **Sécurité des ressources humaines [article 21, paragraphe 2, point i), de la directive (UE) 2022/2555]**

10.1. *Sécurité des ressources humaines*

10.1.1. Aux fins de l'article 21, paragraphe 2, point i), de la directive (UE) 2022/2555, les entités concernées veillent à ce que leurs employés et leurs fournisseurs et prestataires de services directs, s'il est besoin, comprennent et s'engagent à assumer leurs responsabilités en matière de sécurité, selon qu'il convient pour les services et l'emploi proposés et conformément à la politique des entités concernées en matière de sécurité des réseaux et des systèmes d'information.

10.1.2. L'exigence prévue au point 10.1.1 comprend les éléments suivants:

a) des mécanismes garantissant que tous les employés, fournisseurs et prestataires de services directs, s'il y a lieu, comprennent et suivent les pratiques standard de cyberhygiène que les entités concernées appliquent conformément au point 8.1;

b) des mécanismes visant à garantir que tous les utilisateurs ayant un accès d'administration ou privilégié connaissent les rôles, responsabilités et pouvoirs qui leur sont confiés et agissent en conséquence;

c) des mécanismes garantissant que les membres des organes de direction comprennent le rôle, les responsabilités et les pouvoirs qui leur sont confiés en matière de sécurité des réseaux et des systèmes d'information et agissent en conséquence;

d) des mécanismes de recrutement de personnel qualifié pour les rôles respectifs, tels que des contrôles de référence, des procédures de vérification, une validation des certifications ou des épreuves écrites.

10.1.3. Les entités concernées réexaminent l'affectation du personnel aux fonctions spécifiques visées au point 1.2, ainsi que la mobilisation de leurs ressources humaines à cet égard, à intervalles prédéfinis et au moins une fois par an. Elles adaptent l'affectation si nécessaire.

10.2. *Vérification des antécédents*

10.2.1. Les entités concernées veillent dans la mesure du possible à étendre la vérification des antécédents de leurs employés et, le cas échéant, des fournisseurs et prestataires de services directs conformément au point 5.1.4, si leur rôle, leurs responsabilités et leurs autorisations l'exigent.

10.2.2. Aux fins du point 10.2.1, les entités concernées:

a) mettent en place des critères définissant les rôles, les responsabilités et les pouvoirs qui ne peuvent être exercés que par des personnes dont les antécédents ont été vérifiés;

b) veillent à ce que ces personnes fassent l'objet de la vérification visée au point 10.2.1 avant qu'elles commencent à exercer ces rôles, responsabilités et pouvoirs; ces vérifications tiennent compte des lois, réglementations et règles déontologiques applicables en proportion des exigences commerciales, de la classification des actifs visée au point 12.1 et des réseaux et systèmes d'information auxquels il convient d'accéder, ainsi que des risques perçus.

10.2.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour leur politique à intervalles prédéfinis et lorsque cela est nécessaire.

10.3. *Procédures en cas de cessation ou de changement d'emploi*

10.3.1. Les entités concernées veillent à ce que les responsabilités et les tâches en matière de sécurité des réseaux et des systèmes d'information qui restent valables après la cessation ou le changement d'emploi de leur personnel soient définies et exécutées contractuellement.

10.3.2. Aux fins du point 10.3.1, les entités concernées incluent dans les conditions d'emploi, le contrat ou la convention conclus avec la personne concernée les responsabilités et les tâches qui restent valables après la cessation de l'emploi ou du contrat, telles que les clauses de confidentialité.

10.4. *Procédure disciplinaire*

10.4.1. Les entités concernées établissent, communiquent et maintiennent une procédure disciplinaire pour le traitement des violations des politiques de sécurité des réseaux et des systèmes d'information. La procédure tient compte des exigences légales, statutaires, contractuelles et commerciales pertinentes.

10.4.2. Les entités concernées réexaminent et, s'il est besoin, mettent à jour les procédures disciplinaires à intervalles prédéfinis, ainsi que lorsque des changements législatifs ou des changements majeurs concernant les opérations ou les risques l'imposent.

11. **Contrôle d'accès [article 21, paragraphe 2, points i) et j), de la directive (UE) 2022/2555]**

11.1. *Politique de contrôle des accès*

11.1.1. Aux fins de l'article 21, paragraphe 2, point i), de la directive (UE) 2022/2555, les entités concernées établissent, documentent et mettent en œuvre des politiques de contrôle de l'accès logique et physique à leurs réseaux et systèmes d'information, sur la base des exigences commerciales ainsi que des exigences en matière de sécurité des réseaux et des systèmes d'information.

11.1.2. Les politiques visées au point 11.1.1:

a) couvrent l'accès par les personnes, y compris le personnel, les visiteurs et les entités externes telles que les fournisseurs et les prestataires de services;

b) couvrent l'accès par les réseaux et les systèmes d'information;

c) garantissent que l'accès ne soit accordé qu'aux utilisateurs dûment authentifiés.

11.1.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour leurs politiques à intervalles prédéfinis, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

11.2. *Gestion des droits d'accès*

11.2.1. Les entités concernées fournissent, modifient, suppriment et documentent les droits d'accès aux réseaux et aux systèmes d'information conformément à la politique de contrôle d'accès visée au point 11.1.

11.2.2. Les entités concernées:

a) accordent et révoquent les droits d'accès sur la base des principes du besoin d'en connaître, du moindre privilège et de la séparation des fonctions;

b) veillent à ce que les droits d'accès soient modifiés en conséquence en cas de cessation ou de changement d'emploi;

c) veillent à ce que l'accès aux réseaux et aux systèmes d'information soit autorisé par les personnes concernées;

d) veillent à ce que les droits d'accès couvrent adéquatement l'accès des tiers, tels que les visiteurs, les fournisseurs et les prestataires de services, notamment en limitant le champ d'application et la durée des droits d'accès;

e) tiennent un registre des droits d'accès accordés;

f) appliquent la journalisation à la gestion des droits d'accès.

11.2.3. Les entités concernées réexaminent les droits d'accès à intervalles prédéfinis et les modifient en fonction des changements organisationnels. Les entités concernées documentent les résultats du réexamen, y compris les modifications nécessaires des droits d'accès.

11.3. *Comptes privilégiés et comptes d'administration du système*

11.3.1. Les entités concernées maintiennent des politiques de gestion des comptes privilégiés et des comptes d'administration du système dans le cadre de la politique de contrôle d'accès visée au point 11.1.

11.3.2. Les politiques visées au point 11.3.1:

a) établissent des procédures fortes d'identification, d'authentification (telles que l'authentification multifactorielle) et d'autorisation pour les comptes privilégiés et les comptes d'administration du système;

b) créent des comptes spécifiques à utiliser exclusivement pour les opérations d'administration du système, telles que l'installation, la configuration, la gestion ou la maintenance;

c) individualisent et restreignent autant que possible les privilèges d'administration du système,

d) prévoient que les comptes d'administration du système ne soient utilisés que pour se connecter aux systèmes d'administration du système.

11.3.3. Les entités concernées réexaminent les droits d'accès des comptes privilégiés et des comptes d'administration du système à intervalles prédéfinis et les modifient en fonction des changements organisationnels, et elles documentent les résultats du réexamen, y compris les modifications nécessaires des droits d'accès.

11.4. *Systèmes d'administration*

11.4.1. Les entités concernées restreignent et contrôlent l'utilisation des systèmes d'administration du système conformément à la politique de contrôle d'accès visée au point 11.1.

11.4.2. À cette fin, les entités concernées:

a) utilisent uniquement les systèmes d'administration du système à des fins d'administration du système, et non pour d'autres opérations;

b) séparent logiquement ces systèmes des logiciels d'application qui ne sont pas utilisés à des fins d'administration du système,

c) protègent l'accès aux systèmes d'administration du système au moyen de l'authentification et du cryptage.

11.5. *Identification*

11.5.1. Les entités concernées gèrent l'ensemble du cycle de vie des identités des réseaux et systèmes d'information et de leurs utilisateurs.

11.5.2. À cette fin, les entités concernées:

a) mettent en place des identités uniques pour les réseaux et les systèmes d'information et leurs utilisateurs;

b) lient l'identité des utilisateurs à une seule personne;

c) assurent la supervision des identités des réseaux et des systèmes d'information;

d) appliquent la journalisation à la gestion des identités.

11.5.3. Les entités concernées n'autorisent l'attribution d'identités à plusieurs personnes, pouvant prendre la forme d'identités partagées, que lorsqu'elle est nécessaire pour des raisons commerciales ou opérationnelles et qu'elle fait l'objet d'une procédure d'approbation explicite et d'une documentation. Les entités concernées tiennent compte des identités attribuées à plusieurs personnes dans le cadre de gestion des risques de cybersécurité visé au point 2.1.

11.5.4. Les entités concernées réexaminent régulièrement les identités des réseaux et systèmes d'information et de leurs utilisateurs et, si elles ne sont plus nécessaires, les désactivent sans délai.

11.6. *Authentification*

11.6.1. Les entités concernées mettent en œuvre des procédures et des technologies d'authentification sécurisées fondées sur des restrictions d'accès et la politique de contrôle d'accès.

11.6.2. À cette fin, les entités concernées:

a) veillent à ce que la force de l'authentification soit adaptée à la classification de l'actif auquel accéder;

b) contrôlent l'attribution aux utilisateurs et la gestion des informations secrètes relatives à l'authentification par une procédure garantissant la confidentialité des informations, y compris en conseillant le personnel sur le traitement approprié des informations d'authentification;

c) exigent la modification des identifiants d'authentification dès le départ, à des intervalles prédéfinis et en cas de soupçon de compromission des identifiants;

d) exigent la réinitialisation des identifiants d'authentification et le blocage des utilisateurs après un nombre prédéfini de tentatives de connexion infructueuses;

e) mettent un terme aux sessions inactives après une période d'inactivité prédéfinie; et

f) exigent des identifiants distincts pour obtenir un accès privilégié ou accéder à des comptes d'administration.

11.6.3. Les entités concernées utilisent, dans la mesure du possible, les méthodes d'authentification les plus récentes, en fonction du risque associé évalué et de la classification de l'actif auquel accéder, ainsi que des informations d'authentification uniques.

11.6.4. Les entités concernées réexaminent les procédures et technologies d'authentification à intervalles prédéfinis.

11.7. *Authentification à plusieurs facteurs*

11.7.1. Les entités concernées veillent à ce que les utilisateurs soient authentifiés par des facteurs d'authentification multiples ou des mécanismes d'authentification continue pour accéder aux réseaux et aux systèmes d'information des entités concernées, le cas échéant, conformément à la classification de l'actif à consulter.

11.7.2. Les entités concernées veillent à ce que la force de l'authentification soit adaptée à la classification de l'actif auquel accéder.

12. **Gestion des actifs [article 21, paragraphe 2, point i), de la directive (UE) 2022/2555]**

12.1. *Classification des actifs*

12.1.1. Aux fins de l'article 21, paragraphe 2, point i), de la directive (UE) 2022/2555, les entités concernées fixent les niveaux de classification de tous les actifs, y compris l'information, couverts par leurs réseaux et leurs systèmes d'information pour le niveau de protection requis.

12.1.2. Aux fins du point 12.1.1, les entités concernées:

a) établissent un système de niveaux de classification des actifs;

b) associent tous les actifs à un niveau de classification, sur la base des exigences de confidentialité, d'intégrité, d'authenticité et de disponibilité, afin d'indiquer la protection requise en fonction de leur sensibilité, de leur criticité, de leur risque et de leur valeur commerciale;

c) alignent les exigences de disponibilité des actifs sur les objectifs de résultats et de rétablissement fixés dans leur plan de continuité de l'activité et leur plan de rétablissement.

12.1.3. Les entités concernées procèdent à des réexamens périodiques des niveaux de classification des actifs et les mettent à jour, s'il est besoin.

12.2. *Gestion des actifs*

12.2.1. Les entités concernées établissent, mettent en œuvre et appliquent une politique de gestion appropriée des actifs, y compris l'information, conformément à leur politique de sécurité des réseaux et de l'information, et communiquent ladite politique à toute personne qui utilise ou gère des actifs.

12.2.2. Cette politique:

a) couvre l'ensemble du cycle de vie des actifs, y compris l'acquisition, l'utilisation, le stockage, le transport et la destruction;

b) prévoit des règles concernant l'utilisation sûre, le stockage en toute sécurité, le transport en toute sécurité et la suppression et la destruction irréversibles des actifs;

c) prévoit que le transfert a lieu de manière sécurisée, en fonction du type d'actif à transférer.

12.2.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour leur politique à intervalles prédéfinis, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

12.3. *Politique en matière de supports amovibles*

12.3.1. Les entités concernées établissent, mettent en œuvre et appliquent une politique de gestion des supports de stockage amovibles et la communiquent aux membres de leur personnel et aux tiers qui manipulent des supports de stockage amovibles dans les locaux des entités concernées ou dans d'autres lieux où ces supports sont connectés aux réseaux et aux systèmes d'information des entités concernées.

12.3.2. Cette politique:

a) prévoit une interdiction technique de connecter des supports amovibles, à moins que leur utilisation ne soit justifiée par une raison d'organisation;

b) prévoit le blocage de l'autoexécution à partir de ces supports et la détection de codes malveillants dans les supports avant qu'ils ne soient utilisés sur les systèmes des entités concernées;

c) prévoit des mesures de contrôle et de protection des dispositifs de stockage portables contenant des données pendant le transit et le stockage;

d) s'il est besoin, prévoit des mesures pour l'utilisation de techniques cryptographiques pour protéger les données sur les supports de stockage amovibles.

12.3.3. Les entités concernées réexaminent et, s'il est besoin, mettent à jour leur politique à intervalles prédéfinis, ainsi qu'en cas d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

12.4. *Inventaire des actifs*

12.4.1. Les entités concernées élaborent et tiennent à jour un inventaire complet, précis, actualisé et cohérent de leurs actifs. Elles enregistrent de manière traçable les modifications apportées aux entrées de l'inventaire.

12.4.2. Le niveau de détail de l'inventaire des actifs est adapté aux besoins des entités concernées. L'inventaire comprend les éléments suivants:

a) la liste des opérations et des services et leur description,

b) la liste des réseaux et systèmes d'information et des autres actifs associés soutenant les activités et les services des entités concernées.

12.4.3. Les entités concernées réexaminent et mettent à jour régulièrement l'inventaire et leurs actifs et documentent l'historique des changements.

12.5. *Dépôt, restitution ou suppression d'actifs en cas de cessation d'emploi*

Les entités concernées établissent, mettent en œuvre et appliquent des procédures garantissant que leurs actifs qui sont sous la garde de leur personnel sont déposés, restitués ou supprimés à la cessation de l'emploi dudit personnel, et documentent le dépôt, la restitution et la suppression de ces actifs. Lorsque le dépôt, la restitution ou la suppression d'actifs n'est pas possible, les entités concernées veillent à ce que les actifs ne puissent plus accéder à leurs réseaux et systèmes d'information conformément au point 12.2.2.

13. **Sécurité environnementale et physique [article 21, paragraphe 2, points c), e) et i), de la directive (UE) 2022/2555]**

13.1. *Services d'utilité publique*

13.1.1. Aux fins de l'article 21, paragraphe 2, point c), de la directive (UE) 2022/2555, les entités concernées préviennent la perte, la détérioration ou la compromission des réseaux et des systèmes d'information ou l'interruption de leurs opérations causées par la défaillance et la perturbation des services d'utilité publique.

13.1.2. À cette fin, les entités concernées, s'il est besoin:

a) protègent les installations contre les pannes d'électricité et autres perturbations causées par des défaillances des services d'utilité publique tels que l'électricité, les télécommunications, l'approvisionnement en eau ou en gaz, l'évacuation des eaux usées, la ventilation et la climatisation;

b) envisagent le recours à la redondance dans les services d'utilité publique;

c) protègent les services d'utilité publique liés à l'électricité et aux télécommunications, qui transportent des données ou fournissent des réseaux et des systèmes d'information, contre les interceptions et les détériorations;

d) surveillent les services d'utilité publique visés au point c) et signalent aux membres compétents du personnel interne ou externe les événements qui se situent au-dessous et au-dessus des seuils de contrôle minimaux et maximaux visés au point 13.2.2 b) et qui ont un impact sur les services d'utilité publique;

e) concluent des contrats d'alimentation d'urgence avec les services correspondants, par exemple pour le carburant destiné à l'alimentation électrique de secours;

f) veillent à l'efficacité ininterrompue, surveillent, entretiennent et testent l'alimentation du réseau et des systèmes d'information nécessaires au fonctionnement du service proposé, en particulier le contrôle de l'électricité, de la température et de l'humidité, les télécommunications et la connexion internet.

13.1.3. Les entités concernées testent, réexaminent et, s'il est besoin, mettent à jour les mesures de protection de façon régulière, à la suite d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

13.2. *Protection contre les menaces physiques et environnementales*

13.2.1. Aux fins de l'article 21, paragraphe 2, point e), de la directive (UE) 2022/2555, les entités concernées préviennent ou réduisent les conséquences d'événements résultant de menaces physiques et environnementales, telles que les catastrophes naturelles et d'autres menaces intentionnelles ou non intentionnelles, sur la base des résultats de l'évaluation des risques effectuée conformément au point 2.1.

13.2.2. À cette fin, les entités concernées, s'il est besoin:

a) conçoivent et mettent en œuvre des mesures de protection contre les menaces physiques et environnementales;

b) fixent des seuils de contrôle minimaux et maximaux pour les menaces physiques et environnementales;

c) surveillent les paramètres environnementaux et signalent aux membres compétents du personnel interne ou externe les événements qui se situent au-dessous et au-dessus des seuils de contrôle minimaux et maximaux visés au point b).

13.2.3. Les entités concernées testent, réexaminent et, s'il est besoin, mettent à jour les mesures de protection contre les menaces physiques et environnementales de façon régulière, à la suite d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.

13.3. *Périmètre et contrôle d'accès physique*

13.3.1. Aux fins de l'article 21, paragraphe 2, point i), de la directive (UE) 2022/2555, les entités concernées préviennent et surveillent l'accès physique non autorisé, les dommages et les interférences affectant leurs réseaux et leurs systèmes d'information.

13.3.2. À cette fin, les entités concernées:

a) établissent et utilisent, sur la base de l'évaluation des risques effectuée conformément au point 2.1, des périmètres de sécurité pour protéger les zones où sont situés les réseaux et systèmes d'information et autres actifs associés;

b) protègent les zones visées au point a) par des contrôles à l'entrée et des points d'accès appropriés;

c) conçoivent et mettent en œuvre la sécurité physique des bureaux, des salles et des installations;

d) surveillent en permanence leurs locaux dans l'hypothèse d'un accès physique non autorisé.

13.3.3. Les entités concernées testent, réexaminent et, s'il est besoin, mettent à jour les mesures de contrôle de l'accès physique de façon régulière, à la suite d'incidents importants ou lorsque des changements majeurs concernant les opérations ou les risques se produisent.