COMMISSION
EUROPÉENNE

Bruxelles, le 13.3.2024
C(2024) 1532 final

RÈGLEMENT DÉLÉGUÉ (UE) …/... DE LA COMMISSION

du 13.3.2024

complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant les outils, méthodes, processus et politiques de gestion du risque lié aux TIC et le cadre simplifié de gestion du risque lié aux TIC

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE L'ACTE DÉLÉGUÉ

L'un des objectifs du règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier (DORA) est d'établir des exigences uniformes en matière de sécurité des réseaux et des systèmes d'information des entreprises et organisations opérant dans le secteur financier. Il crée donc un cadre réglementaire pour la résilience opérationnelle numérique, qui prévoit que toutes les entités financières doivent s'assurer qu'elles peuvent affronter tous les types de perturbations et de menaces liées aux TIC, y répondre et les surmonter. Ces exigences sont homogènes dans l'ensemble de l'UE, dans le but de prévenir et d'atténuer les cybermenaces.

À cet égard, l'article 15 du règlement DORA prévoit que «*[l]es AES élaborent, par l'intermédiaire du comité mixte, en concertation avec l'Agence de l'Union européenne pour la cybersécurité (ENISA), des projets communs de normes techniques de réglementation*» afin de parvenir à une «*harmonisation accrue des outils, méthodes, processus et politiques de gestion du risque lié aux TIC*» et, en vertu de son article 16, d'élaborer pour certaines entités financières un cadre simplifié de gestion de ce risque. L'ENISA a donc participé au sous-comité du comité mixte des AES sur la résilience opérationnelle numérique (JC SC DOR).

Le présent règlement délégué correspond à ce mandat et a été transmis à la Commission le 17 janvier 2024.

2. CONSULTATION AVANT L'ADOPTION DE L'ACTE

Dans le cadre de l'élaboration des normes énoncées dans le présent projet de règlement, les AES ont publié leur projet de normes techniques de réglementation le 19 juin 2023, pour une période de consultation de trois mois qui s'est achevée le 11 septembre 2023. Elles ont reçu 120 réponses de divers acteurs du marché de l'ensemble du secteur financier. Leur rapport final donne un aperçu complet de ces réponses[1].

Les participants à la consultation publique ont formulé des observations sur les aspects suivants du projet de normes techniques de réglementation proposé:

- demandes de prolongation du délai de mise en œuvre;
- demandes visant à obtenir une plus grande proportionnalité (par exemple une proportionnalité dans les deux sens, c'est-à-dire tenant compte aussi bien de l'augmentation que de la réduction de la complexité et des risques; ou une approche plus sectorielle avec davantage de proportionnalité pour, par exemple, les entreprises d'assurance, etc.);
- demandes visant à ce que les aspects liés à la gouvernance soient exclus du projet de normes techniques de réglementation parce qu'ils ne font pas partie du mandat confié aux AES; et
- demandes visant à ce qu'il ne soit pas introduit de mesures supplémentaires concernant les ressources d'informatique en nuage.

[1] Autorités européennes de surveillance (2024), «Final report on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554».

À la lumière des observations reçues, les AES ont apporté des modifications au projet de normes techniques de réglementation. Ces modifications ont consisté, par exemple, à renforcer la proportionnalité, à supprimer des exigences du régime général l'article sur la gouvernance et à clarifier certaines dispositions, en particulier celles qui figurent dans les articles relatifs à la sécurité des réseaux, au chiffrement, au contrôle d'accès et à la continuité des activités. Les AES se sont prononcées contre l'inclusion d'éléments spécifiques à l'informatique en nuage, afin de respecter le principe de neutralité technologique. En revanche, les AES ont décidé d'élargir les exigences envisagées pour couvrir les actifs de TIC ou services TIC fournis par des prestataires tiers de services TIC en général. Toutefois, en ce qui concerne les délais de mise en œuvre, les AES n'ont envisagé aucun changement, ces délais étant fixés au niveau 1 par le règlement DORA.

3. ÉLÉMENTS JURIDIQUES DE L'ACTE DÉLÉGUÉ

Le titre I, chapitre I, établit les principaux principes et éléments à prendre en considération lors de l'élaboration et de la mise en œuvre des politiques, procédures, protocoles et outils de sécurité des TIC (article 1er).

Le titre II, chapitre II, fixe les conditions d'une harmonisation accrue des outils, méthodes, processus et politiques de gestion du risque lié aux TIC, en imposant: les éléments généraux des politiques, procédures, protocoles et outils de sécurité des TIC (section 1); les éléments spécifiques des politiques, procédures, protocoles et outils de sécurité des TIC (section 2): niveau de tolérance au risque, méthodes d'évaluation du risque lié aux TIC et mesures de traitement du risque lié aux TIC; une politique de gestion des actifs de TIC (section 3); une politique en matière de chiffrement et de contrôles cryptographiques (section 4); une politique de sécurité des opérations de TIC (section 5); une politique de gestion de la sécurité des réseaux (section 6); une politique de gestion des projets TIC (section 7); une politique de sécurité physique et environnementale visant à préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données (section 8). Le chapitre II précise tous les éléments de sécurité des TIC que les entités financières doivent inclure dans leurs politiques en matière de ressources humaines et de contrôle d'accès. Le chapitre III précise tous les éléments d'une politique de détection des incidents liés aux TIC et de réponse à ces incidents que les entités financières doivent élaborer et mettre en œuvre. Le chapitre IV définit le contenu et le format du rapport sur le réexamen du cadre de gestion du risque lié aux TIC que les entités financières sont tenues d'établir et de présenter.

Le titre III établit un cadre simplifié de gestion du risque lié aux TIC, prévoyant la mise en place d'un cadre de gouvernance et de contrôle (chapitre I), un mécanisme et des exigences en matière d'accès et de contrôle (chapitre II), l'établissement d'un plan de continuité des activités de TIC (chapitre III), et le contenu et le format du rapport sur le réexamen du cadre de gestion du risque lié aux TIC que les entités financières sont tenues d'établir et de présenter (chapitre IV).

Le titre IV contient les dispositions finales relatives à l'entrée en vigueur de l'acte (article 42).

RÈGLEMENT DÉLÉGUÉ (UE) …/... DE LA COMMISSION

du 13.3.2024

complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant les outils, méthodes, processus et politiques de gestion du risque lié aux TIC et le cadre simplifié de gestion du risque lié aux TIC

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

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011[2], et notamment son article 15, quatrième alinéa, et son article 16, paragraphe 3, quatrième alinéa,

considérant ce qui suit:

(1) Le règlement (UE) 2022/2554 couvre un large éventail d'entités financières qui diffèrent par leur taille, leur structure, leur organisation interne, ainsi que par la nature et la complexité de leurs activités, et qui présentent donc des facteurs plus ou moins grands de complexité ou de risque. Afin que cette diversité soit dûment prise en considération, toute exigence relative aux politiques, procédures, protocoles et outils de sécurité des TIC, ainsi qu'à un cadre simplifié de gestion du risque lié aux TIC, devrait être proportionnée à la taille, à la structure, à l'organisation interne, à la nature et à la complexité de ces entités financières, ainsi qu'aux risques correspondants.

(2) Pour la même raison, les entités financières soumises au règlement (UE) 2022/2554 devraient disposer d'une certaine souplesse dans la manière de se conformer aux exigences concernant les politiques, procédures, protocoles et outils de sécurité des TIC et à un éventuel cadre simplifié de gestion du risque lié aux TIC. C'est pourquoi elles devraient être autorisées à utiliser tout document dont elles disposent déjà pour se conformer aux obligations de documentation découlant de ces exigences. Il s'ensuit que l'élaboration, la documentation et la mise en œuvre de politiques spécifiques en matière de sécurité des TIC ne devraient être requises que pour certains éléments essentiels, en tenant compte, entre autres, des pratiques de pointe du secteur et des normes applicables. En outre, il est nécessaire d'élaborer, de documenter et de mettre en œuvre des procédures de sécurité des TIC couvrant des aspects spécifiques de la mise en œuvre technique, notamment la gestion des capacités et des performances, la

[2] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj?locale=fr).

gestion de la vulnérabilité et des correctifs, la sécurité des données et des systèmes, et la journalisation.

(3) Afin de garantir la mise en œuvre correcte, sur la durée, des politiques, procédures, protocoles et outils de sécurité des TIC visés au titre II, chapitre I, du présent règlement, il importe que les entités financières attribuent correctement et maintiennent tous les rôles et responsabilités liés à la sécurité des TIC, et qu'elles définissent les conséquences du non-respect des politiques ou procédures en matière de sécurité des TIC.

(4) Afin de limiter le risque de conflits d'intérêts, les entités financières devraient veiller à la séparation des tâches lors de l'attribution de rôles et de responsabilités dans le domaine des TIC.

(5) Dans un souci de souplesse et pour simplifier le cadre de contrôle des entités financières, ces dernières ne devraient pas être tenues d'élaborer des dispositions spécifiques sur les conséquences du non-respect des politiques, procédures et protocoles de sécurité des TIC visés au titre II, chapitre I, du présent règlement si de telles dispositions sont déjà prévues dans une autre politique ou procédure.

(6) Dans un environnement dynamique où les risques liés aux TIC évoluent constamment, il importe que les entités financières élaborent l'ensemble de leurs politiques de sécurité des TIC sur la base de pratiques de pointe et, le cas échéant, de normes telles que définies à l'article 2, point 1), du règlement (UE) nº 1025/2012 du Parlement européen et du Conseil[3]. Cela devrait permettre aux entités financières visées au titre II du présent règlement de rester informées et préparées dans un contexte appelé à évoluer.

(7) Afin de garantir leur résilience opérationnelle numérique, les entités financières visées au titre II du présent règlement devraient, dans le cadre de leurs politiques, procédures, protocoles et outils de sécurité des TIC, élaborer et mettre en œuvre une politique de gestion des actifs de TIC, des procédures de gestion des capacités et des performances, ainsi que des politiques et procédures pour les opérations de TIC. Ces politiques et procédures sont nécessaires pour assurer le suivi de l'état des actifs de TIC tout au long de leur cycle de vie, de sorte que ces actifs soient utilisés et entretenus de manière efficace (gestion des actifs de TIC). Ces politiques et procédures devraient également garantir l'optimisation du fonctionnement des systèmes de TIC et faire en sorte que les performances des systèmes de TIC et des capacités en matière de TIC répondent aux objectifs établis en matière de sécurité des activités et de l'information (gestion des capacités et des performances). Enfin, ces politiques et procédures devraient garantir une gestion et une exploitation quotidiennes efficaces et fluides des systèmes de TIC (et des opérations de TIC), afin de réduire le risque de perte de confidentialité, d'intégrité et de disponibilité des données. Ces politiques et procédures sont donc nécessaires pour garantir la sécurité des réseaux, fournir des garanties adéquates contre les intrusions et les utilisations abusives des données et préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données.

---

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

(8) Afin de garantir une bonne gestion du risque lié aux systèmes de TIC hérités, les entités financières devraient enregistrer et surveiller les dates d'expiration des services TIC d'appui fournis par des tiers. En raison des conséquences potentielles qu'une perte de confidentialité, d'intégrité ou de disponibilité des données peut avoir, les entités financières devraient, lorsqu'elles enregistrement et suivent ces dates d'expiration, se concentrer sur les actifs ou systèmes de TIC qui sont critiques pour le fonctionnement de l'entreprise.

(9) Les contrôles cryptographiques peuvent garantir la disponibilité, l'authenticité, l'intégrité et la confidentialité des données. Les entités financières visées au titre II du présent règlement devraient donc définir et mettre en œuvre ces contrôles sur la base d'une approche fondée sur les risques. À cette fin, les entités financières devraient chiffrer les données concernées, au repos, en transit ou, si nécessaire, en cours d'utilisation, sur la base des résultats d'un processus en deux volets, à savoir la classification des données et une évaluation complète du risque lié aux TIC. Compte tenu de la complexité du chiffrement des données en cours d'utilisation, les entités financières visées au titre II du présent règlement ne devraient chiffrer les données en cours d'utilisation que lorsque cela est approprié à la lumière des résultats de l'évaluation du risque lié aux TIC. Les entités financières visées au titre II du présent règlement devraient toutefois être en mesure, lorsque le chiffrement des données en cours d'utilisation n'est pas possible ou est trop complexe, de protéger la confidentialité, l'intégrité et la disponibilité des données concernées au moyen d'autres mesures de sécurité des TIC. Compte tenu de la rapidité de l'évolution technologique dans le domaine des techniques cryptographiques, les entités financières visées au titre II du présent règlement devraient se tenir informées des évolutions qui les concernent en matière de cryptanalyse et tenir compte des pratiques de pointe et des normes existantes. Elles devraient donc suivre une approche souple, fondée sur l'atténuation et la surveillance des risques, pour s'adapter au paysage changeant des menaces cryptographiques, y compris des menaces résultant des progrès de l'informatique quantique.

(10) La sécurité des opérations de TIC et les politiques, procédures, protocoles et outils opérationnels sont essentiels pour garantir la confidentialité, l'intégrité et la disponibilité des données. Un aspect essentiel est la séparation stricte entre les environnements de production des TIC, d'une part, et les environnements dans lesquels les systèmes de TIC sont développés et testés, ou les autres environnements hors production, d'autre part. Cette séparation devrait constituer une mesure importante de sécurisation des TIC contre les accès non désirés et non autorisés aux données ainsi que contre les modifications et les suppressions non désirées et non autorisées de données dans l'environnement de production, qui pourraient entraîner des perturbations majeures des activités métiers des entités financières visées au titre II du présent règlement. Toutefois, compte tenu des pratiques actuelles de développement des systèmes de TIC, les entités financières devraient être autorisées, dans des circonstances exceptionnelles, à réaliser des tests dans des environnements de production, à condition qu'elles justifient ces tests et obtiennent l'approbation requise.

(11) Compte tenu de l'évolution rapide des TIC, des vulnérabilités des TIC et des cybermenaces, il est nécessaire d'adopter une approche proactive et globale pour identifier, évaluer et éliminer ces vulnérabilités. En l'absence d'une telle approche, les entités financières, leurs clients, leurs utilisateurs ou leurs contreparties peuvent être exposés à des risques graves mettant en péril leur résilience opérationnelle numérique, la sécurité de leurs réseaux, ainsi que la disponibilité, l'authenticité, l'intégrité et la

confidentialité des données que les politiques et procédures de sécurité des TIC sont censées protéger. Les entités financières visées au titre II du présent règlement devraient donc identifier les vulnérabilités qui peuvent exister dans leur environnement de TIC et y remédier, et tant les entités financières que leurs prestataires tiers de services TIC devraient appliquer un cadre de gestion des vulnérabilités cohérent, transparent et responsable. Pour la même raison, les entités financières devraient surveiller les vulnérabilités des TIC en utilisant des ressources fiables et des outils automatisés, et en vérifiant que les prestataires tiers de services TIC garantissent une action rapide contre les vulnérabilités des services TIC fournis.

(12) La gestion des correctifs devrait être un élément essentiel des politiques et procédures de sécurité des TIC qui, grâce aux tests et au déploiement dans un environnement contrôlé, doivent permettre de remédier aux vulnérabilités identifiées et d'éviter des perturbations lors de l'installation de correctifs.

(13) Afin de garantir une communication rapide et transparente concernant les menaces potentielles pour la sécurité susceptibles d'avoir un impact sur l'entité financière et ses parties prenantes, les entités financières devraient établir des procédures pour une divulgation responsable des vulnérabilités des TIC à leurs clients, à leurs contreparties et au public. Lors de l'établissement de ces procédures, les entités financières devraient tenir compte de facteurs tels que la gravité de la vulnérabilité, son impact potentiel de cette vulnérabilité sur les parties prenantes et les solutions ou mesures d'atténuation disponibles.

(14) Afin de permettre l'attribution de droits d'accès aux utilisateurs, chacune des entités financières visées au titre II du présent règlement devrait mettre en place des mesures fortes pour garantir l'identification unique des personnes et des systèmes qui auront accès à ses informations. À défaut, elle s'exposerait au risque d'accès non autorisés, de violations de données et d'activités frauduleuses, ce qui compromettrait la confidentialité, l'intégrité et la disponibilité de données financières sensibles. L'utilisation de comptes génériques ou de comptes partagés devrait être autorisée à titre exceptionnel dans des circonstances définies par les entités financières, mais celles-ci devraient veiller à ce que la responsabilité des actions effectuées via ces comptes soit maintenue. Sans cette garantie, d'éventuels utilisateurs malveillants auraient la possibilité d'entraver des mesures d'enquête et de correction, ce qui exposerait les entités financières vulnérables à des actes de malveillance non détectés ou à des sanctions pour non-conformité.

(15) Afin de gérer les progrès rapides des environnements TIC, les entités financières visées au titre II du présent règlement devraient mettre en œuvre de solides politiques et procédures de gestion des projets TIC afin de préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données. Ces politiques et procédures de gestion de projets TIC devraient identifier les éléments nécessaires pour bien gérer ces projets, notamment les modifications et acquisitions de systèmes de TIC par l'entité financière, ainsi que la maintenance et l'évolution de ces systèmes quelle que soit la méthode de gestion de projets TIC choisie par cette dernière. Dans le cadre de ces politiques et procédures, les entités financières devraient adopter des pratiques et des méthodes de test qui répondent à leurs besoins, tout en respectant une approche fondée sur les risques et en veillant au maintien d'un environnement TIC sûr, fiable et résilient. Afin de garantir la mise en œuvre en toute sécurité d'un projet de TIC, les entités financières devraient veiller à ce que le personnel chargé des différents secteurs d'activité ou rôles influencés ou concernés par ce projet puisse fournir les informations et l'expertise nécessaires. Afin d'assurer une surveillance efficace, les rapports sur les

projets TIC, en particulier sur les projets touchant des fonctions critiques ou importantes et sur les risques qui y sont associés, devraient être soumis à l'organe de direction. Les entités financières devraient adapter la fréquence et le détail des examens et rapports systématiques et continus à l'importance et à la taille des projets TIC concernés.

(16) Il est nécessaire de veiller à ce que les progiciels que les entités financières visées au titre II du présent règlement acquièrent et développent soient intégrés de manière efficace et sécurisée dans l'environnement TIC existant, conformément aux objectifs établis en matière de sécurité des activités et de l'information. Les entités financières devraient donc procéder à une évaluation approfondie de ces progiciels. À cette fin, et pour pouvoir identifier les vulnérabilités et les lacunes potentielles en matière de sécurité, tant dans les progiciels que dans les systèmes de TIC au sens large, les entités financières devraient effectuer des tests de sécurité des TIC. Pour évaluer l'intégrité d'un logiciel et s'assurer que son utilisation ne présente pas de risques pour la sécurité des TIC, les entités financières devraient également examiner les codes sources des logiciels qu'elles acquièrent, y compris, lorsque cela est faisable, des logiciels propriétaires fournis par des prestataires tiers de services TIC, en utilisant des méthodes de test aussi bien statiques que dynamiques.

(17) Tout changement, quelle que soit son échelle, comporte des risques inhérents et peut comporter des risques importants de perte de confidentialité, d'intégrité et de disponibilité des données, et entraîner par ricochet de graves perturbations des activités. Afin de protéger les entités financières des vulnérabilités et faiblesses potentielles en matière de TIC qui pourraient les exposer à des risques importants, un processus de vérification rigoureux est nécessaire pour confirmer que tous les changements apportés satisfont aux exigences nécessaires en matière de sécurité des TIC. Les entités financières visées au titre II du présent règlement devraient donc disposer, en tant qu'élément essentiel de leurs politiques et procédures en matière de sécurité des TIC, de solides politiques et procédures de gestion des changements dans les TIC. Afin de préserver l'objectivité et l'efficacité du processus de gestion des changements dans les TIC, de prévenir les conflits d'intérêts et de garantir une évaluation objective des changements apportés aux TIC, il est nécessaire de séparer les fonctions chargées d'approuver ces changements des fonctions qui les demandent et les mettent en œuvre. Pour assurer des transitions efficaces, une mise en œuvre contrôlée des changements de TIC et des perturbations minimales du fonctionnement des systèmes de TIC, les entités financières devraient assigner clairement des rôles et responsabilités garantissant que les changements apportés aux TIC seront planifiés, testés de manière adéquate, et de qualité. Pour veiller à ce que les systèmes de TIC continuent de fonctionner efficacement, et pour fournir un filet de sécurité aux entités financières, il convient par ailleurs que celles-ci élaborent et mettent en œuvre des procédures de secours. Les entités financières devraient clairement définir ces procédures de secours et assigner les responsabilités nécessaires à une réaction rapide et efficace en cas de changements infructueux dans les TIC.

(18) Pour détecter, gérer et notifier les incidents liés aux TIC, les entités financières visées au titre II du présent règlement devraient se doter d'une politique en matière d'incidents liés aux TIC qui inclue les composantes d'un processus de gestion des incidents liés aux TIC. À cette fin, les entités financières devraient identifier tous les contacts pertinents, à l'intérieur et à l'extérieur de l'organisation, susceptibles de faciliter la bonne coordination et la bonne mise en œuvre des différentes phases de ce processus. Afin d'optimiser la détection des incidents liés aux TIC et la réponse à ces

incidents, et pour cerner les tendances que révèlent ces incidents et qui constituent une source précieuse d'informations permettant aux entités financières d'identifier les causes profondes et les problèmes et d'y remédier de manière efficace, les entités financières devraient en particulier analyser en détail les incidents liés aux TIC qu'elles jugent les plus importants, notamment en raison de leur répétition régulière.

(19) Afin de garantir une détection précoce et efficace des activités anormales, les entités financières visées au titre II du présent règlement devraient collecter, surveiller et analyser les différentes sources d'information et devraient attribuer les rôles et responsabilités correspondants. En ce qui concerne les sources d'information internes, les journaux sont une source extrêmement pertinente, mais qui ne devrait pas être la seule sur laquelle les entités financières s'appuient. Ainsi, les entités financières devraient prendre en considération l'ensemble des informations dont elles peuvent disposer, y compris celles obtenues grâce à d'autres fonctions internes, lesquelles constituent souvent une source précieuse d'informations pertinentes. Pour la même raison, les entités financières devraient analyser et surveiller les informations recueillies auprès de sources externes, notamment les informations fournies par des prestataires tiers de services TIC sur les incidents touchant leurs systèmes et réseaux, et auprès d'autres sources qu'elles jugent pertinentes. Dans la mesure où ces informations constituent des données à caractère personnel, le droit de l'Union en matière de protection des données s'applique. Les données à caractère personnel devraient être limitées à ce qui est nécessaire à la détection d'incidents.

(20) Afin de faciliter la détection des incidents liés aux TIC, les entités financières devraient conserver les preuves de ces incidents. Pour que ces preuves soient conservées suffisamment longtemps, et pour s'éviter une charge réglementaire excessive, les entités financières devraient déterminer la durée de conservation en tenant compte, entre autres, de la criticité des données et des exigences en matière de conservation imposées par le droit de l'Union.

(21) Pour que les incidents liés aux TIC soient détectés à temps, il convient que les entités financières visées au titre II du présent règlement considèrent comme non exhaustifs les critères définis pour le déclenchement de la détection des incidents liés aux TIC et des réponses à ces incidents. En outre, les entités financières devraient certes tenir compte de chacun de ces critères, mais elles ne devraient pas considérer que les circonstances qu'ils décrivent doivent nécessairement exister simultanément, et l'importance des services TIC concernés devrait être dûment prise en considération pour déclencher les processus de détection des incidents liés aux TIC et de réponse à ces incidents.

(22) Lorsqu'elles élaborent une politique de continuité des activités de TIC, les entités financières visées au titre II du présent règlement devraient tenir compte des éléments essentiels de la gestion du risque lié aux TIC, notamment des stratégies de gestion et de communication en matière d'incidents liés aux TIC, du processus de gestion des changements dans les TIC et des risques associés aux prestataires tiers de services TIC.

(23) Il est nécessaire de définir l'ensemble des scénarios que les entités financières visées au titre II du présent règlement devraient prendre en compte tant pour mettre en œuvre des plans de réponse et de rétablissement des TIC que pour tester des plans de continuité des activités de TIC. Ces scénarios devraient leur servir de point de départ pour analyser aussi bien la pertinence et la plausibilité de chaque scénario que la nécessité d'en élaborer d'autres. Les entités financières devraient se concentrer sur les

scénarios dans lesquels les investissements dans les mesures de résilience pourraient être les plus efficaces et les plus efficients. En testant le basculement entre l'infrastructure de TIC principale et toute capacité redondante, les sauvegardes et les installations redondantes, les établissements financiers devraient évaluer si cette capacité, ces sauvegardes et ces installations redondantes fonctionnent efficacement pendant une durée suffisante et s'assurer que le fonctionnement normal de l'infrastructure de TIC principale est restauré conformément aux objectifs de rétablissement.

(24) Il est nécessaire de fixer des exigences en matière de risque opérationnel, et plus particulièrement en matière de gestion des projets TIC, de gestion des changements dans les TIC et de gestion de la continuité des activités de TIC, en s'appuyant sur les exigences qui s'appliquent déjà aux contreparties centrales, aux dépositaires centraux de titres et aux plates-formes de négociation en vertu, respectivement, des règlements (UE) nº 648/2012[4], (UE) nº 600/2014[5] et (UE) nº 909/2014[6] du Parlement européen et du Conseil.

(25) L'article 6, paragraphe 5, du règlement (UE) 2022/2554 impose aux entités financières de réexaminer leur cadre de gestion du risque lié aux TIC et de présenter à leur autorité compétente un rapport sur ce réexamen. Afin de permettre aux autorités compétentes de traiter facilement les informations contenues dans ces rapports et de garantir une transmission adéquate de ces informations, les entités financières devraient présenter ces rapports sous un format électronique interrogeable.

(26) Les exigences applicables aux entités financières qui sont soumises au cadre simplifié de gestion du risque lié aux TIC prévu à l'article 16 du règlement (UE) 2022/2554 devraient se concentrer sur les domaines et éléments essentiels qui, compte tenu de l'échelle, du risque, de la taille et de la complexité de ces entités financières, constituent le minimum nécessaire pour garantir la confidentialité, l'intégrité, la disponibilité et l'authenticité des données et des services de ces entités. Dans ce contexte, ces entités financières devraient disposer d'un cadre de gouvernance et de contrôle interne définissant clairement les responsabilités claires, afin que le cadre de gestion des risques soit efficace et solide. En outre, afin de réduire leur charge administrative et opérationnelle, ces entités financières ne devraient élaborer et documenter qu'une seule politique, à savoir une politique de sécurité de l'information, qui précise les principes et règles généraux nécessaires pour protéger la confidentialité, l'intégrité, la disponibilité et l'authenticité des données et des services de ces entités.

(27) Les dispositions du présent règlement portent sur le domaine dont relève le cadre de gestion du risque lié aux TIC, puisqu'elles détaillent les éléments spécifiques applicables aux entités financières conformément à l'article 15 du règlement (UE) 2022/2554 et définissent le cadre simplifié de gestion du risque lié aux TIC pour les

---

[4] Règlement (UE) nº 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (JO L 201 du 27.7.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj?locale=fr).

[5] Règlement (UE) nº 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) nº 648/2012 (JO L 173 du 12.6.2014, p. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj?locale=fr).

[6] Règlement (UE) nº 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres et modifiant les directives 98/26/CE et 2014/65/UE et le règlement (UE) nº 236/2012 (JO L 257 du 28.8.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj?locale=fr).

entités financières prévu à l'article 16, paragraphe 1, dudit règlement. Afin de garantir la cohérence entre le cadre ordinaire et le cadre simplifié de gestion du risque lié aux TIC, et compte tenu du fait que ces dispositions devraient devenir applicables en même temps, il convient d'inclure ces dispositions dans un acte législatif unique.

(28) Le présent règlement se fonde sur les projets de normes techniques de réglementation soumis à la Commission par l'Autorité bancaire européenne, l'Autorité européenne des assurances et des pensions professionnelles et l'Autorité européenne des marchés financiers (les «autorités européennes de surveillance»), en concertation avec l'Agence de l'Union européenne pour la cybersécurité (ENISA).

(29) Le comité mixte des autorités européennes de surveillance visé à l'article 54 du règlement (UE) nº 1093/2010 du Parlement européen et du Conseil[7], à l'article 54 du règlement (UE) nº 1094/2010 du Parlement européen et du Conseil[8] et à l'article 54 du règlement (UE) nº 1095/2010 du Parlement européen et du Conseil[9] a procédé à des consultations publiques ouvertes sur les projets de normes techniques de réglementation sur lesquels se fonde le présent règlement, analysé les coûts et avantages potentiels des normes proposées et sollicité l'avis du groupe des parties intéressées au secteur bancaire institué en application de l'article 37 du règlement (UE) nº 1093/2010, du groupe des parties intéressées à l'assurance et la réassurance et du groupe des parties intéressées aux pensions professionnelles institués en application de l'article 37 du règlement (UE) nº 1094/2010 et du groupe des parties intéressées au secteur financier institué en application de l'article 37 du règlement (UE) nº 1095/2010.

(30) Dans la mesure où le traitement de données à caractère personnel est requis pour satisfaire aux obligations énoncées dans le présent acte, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 devraient s'appliquer pleinement. Par exemple, le principe de minimisation des données devrait être respecté lorsque des données à caractère personnel sont collectées, afin d'assurer une détection appropriée des incidents. Le Contrôleur européen de la protection des données a également été consulté sur le projet de texte du présent acte,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

---

7 Règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj?locale=fr).

8 Règlement (UE) nº 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/79/CE de la Commission (JO L 331 du 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj?locale=fr).

9 Règlement (UE) nº 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission (JO L 331 du 15.12.2010, p. 84, ELI: https://eur-lex.europa.eu/eli/reg/2010/1095/oj?locale=fr).

TITRE I
PRINCIPE GÉNÉRAL

Article premier
Profil de risque global et complexité

Lors de l'élaboration et de la mise en œuvre des politiques, procédures, protocoles et outils de sécurité de TIC visés au titre II et du cadre simplifié de gestion du risque lié aux TIC visé au titre III, il est tenu compte de la taille et du profil de risque global de l'entité financière, ainsi que de la nature, de l'échelle et des éléments tendant à accroître ou réduire la complexité de ses services, activités et opérations, notamment des éléments concernant:

(a) le chiffrement et la cryptographie;

(b) la sécurité des opérations de TIC;

(c) la sécurité des réseaux;

(d) la gestion des projets TIC et des changements dans les TIC;

(e) l'incidence potentielle du risque lié aux TIC sur la confidentialité, l'intégrité et la disponibilité des données, et l'incidence potentielle des perturbations sur la continuité et la disponibilité des activités de l'entité financière.

TITRE II
HARMONISATION ACCRUE DES OUTILS, MÉTHODES, PROCESSUS ET POLITIQUES DE GESTION DU RISQUE LIÉ AUX TIC CONFORMÉMENT À L'ARTICLE 15 DU RÈGLEMENT (UE) 2022/2554

CHAPITRE I
POLITIQUES, PROCÉDURES, PROTOCOLES ET OUTILS DE SÉCURITÉ DES TIC

SECTION 1

Article 2

Éléments généraux des politiques, procédures, protocoles et outils de sécurité des TIC

1. Les entités financières veillent à ce que leurs politiques de sécurité des TIC, la sécurité de l'information et les procédures, protocoles et outils y afférents visés à l'article 9, paragraphe 2, du règlement (UE) 2022/2554 soient intégrés dans leur cadre de gestion du risque lié aux TIC. Les entités financières établissent les politiques, procédures, protocoles et outils de sécurité des TIC prévus au présent chapitre qui:

   (a) garantissent la sécurité des réseaux;

   (b) comportent des garanties contre les intrusions et les utilisations abusives des données;

   (c) préservent la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, y compris en recourant à des techniques cryptographiques;

   (d) garantissent une transmission précise et rapide des données sans perturbation majeure et sans retard injustifié.

2. Les entités financières veillent à ce que les politiques de sécurité des TIC visées au paragraphe 1:

   (a) soient alignées sur les objectifs de l'entité financière en matière de sécurité de l'information définis dans la stratégie de résilience opérationnelle numérique visée à l'article 6, paragraphe 8, du règlement (UE) 2022/2554;

   (b) indiquent la date de l'approbation formelle des politiques de sécurité des TIC par l'organe de direction;

   (c) contiennent des indicateurs et des mesures pour

      i) suivre la mise en œuvre des politiques, procédures, protocoles et outils de sécurité des TIC;

      ii) enregistrer les exceptions à cette mise en œuvre;

iii) veiller à ce que la résilience opérationnelle numérique de l'entité financière soit assurée en cas d'exceptions visées au point ii);

(d) précisent les responsabilités du personnel à tous les niveaux afin d'assurer la sécurité des TIC de l'entité financière;

(e) précisent les conséquences du non-respect, par le personnel de l'entité financière, des politiques de sécurité des TIC, lorsque des dispositions à cet effet ne sont pas prévues dans d'autres politiques de l'entité financière;

(f) répertorient les documents à tenir à jour;

(g) précisent les modalités de séparation des fonctions dans le cadre du modèle reposant sur trois lignes de défense ou d'un autre modèle interne de gestion et de contrôle des risques, selon le cas, afin d'éviter les conflits d'intérêts;

(h) tiennent compte des pratiques de pointe et, le cas échéant, des normes telles que définies à l'article 2, point 1), du règlement (UE) nº 1025/2012;

(i) définissent les rôles et les responsabilités en ce qui concerne l'élaboration, la mise en œuvre et la maintenance des politiques, procédures, protocoles et outils de sécurité des TIC;

(j) soient réexaminées conformément à l'article 6, paragraphe 5, du règlement (UE) 2022/2554;

(k) tiennent compte des changements importants concernant l'entité financière, notamment des changements importants intervenant dans ses activités ou processus, dans l'éventail des cybermenaces ou dans les obligations légales applicables.

SECTION 2

Article 3
Gestion du risque lié aux TIC

Les entités financières élaborent, documentent et mettent en œuvre des politiques et procédures de gestion du risque lié aux TIC qui contiennent l'ensemble des éléments suivants:

(a) l'indication de l'approbation du niveau de tolérance au risque lié aux TIC déterminé conformément à l'article 6, paragraphe 8, point b), du règlement (UE) 2022/2554;

(b) une procédure et une méthode d'évaluation du risque lié aux TIC, précisant:

i) les vulnérabilités et les menaces qui affectent ou peuvent affecter les fonctions opérationnelles soutenues et les systèmes de TIC et actifs de TIC qui les soutiennent;

ii) les indicateurs quantitatifs ou qualitatifs à utiliser pour mesurer l'incidence et la probabilité des vulnérabilités et des menaces visées au point i);

(c) la procédure de détermination, de mise en œuvre et de documentation des mesures de traitement du risque lié aux TIC pour les risques liés aux TIC qui ont été identifiés et évalués, y compris la définition des mesures de traitement du risque lié aux TIC nécessaires pour ramener ce risque dans les limites du niveau de tolérance au risque visé au point a);

(d) pour les risques résiduels liés aux TIC qui sont toujours présents à l'issue de la mise en œuvre des mesures de traitement du risque lié aux TIC visées au point c):

i) des dispositions relatives à l'identification de ces risques résiduels liés aux TIC;

ii) l'attribution des rôles et des responsabilités concernant:

(1) l'acceptation des risques résiduels liés aux TIC qui dépassent le niveau de tolérance au risque de l'entité financière visé au point a);

(2) le processus de réexamen visé au point iv) du présent point d);

iii) l'établissement d'un inventaire des risques résiduels liés aux TIC qui ont été acceptés, accompagné d'une justification de leur acceptation;

iv) des dispositions relatives au réexamen, au moins une fois par an, des risques résiduels liés aux TIC qui ont été acceptés, comprenant:

1) l'indication de tout changement dans les risques résiduels liés aux TIC;

2) l'évaluation des mesures d'atténuation disponibles;

3) une évaluation indiquant si les raisons justifiant l'acceptation des risques résiduels liés aux TIC sont toujours valables et applicables à la date du réexamen;

(e) des dispositions qui prévoient le suivi:

i) de tout changement dans l'éventail des risques liés aux TIC et des cybermenaces;

ii) des vulnérabilités et menaces internes et externes;

iii) du risque lié aux TIC de l'entité financière, et qui permettent de détecter rapidement les changements susceptibles d'avoir une incidence sur son profil de risque lié aux TIC;

(f) des dispositions relatives à un processus garantissant la prise en compte de toute modification de la stratégie commerciale et de la stratégie de résilience opérationnelle numérique de l'entité financière.

La procédure visée au point c) du premier alinéa garantit, aux fins dudit point:

(a) le suivi de l'efficacité des mesures de traitement du risque lié aux TIC qui sont mises en œuvre;

(b) une évaluation indiquant si les niveaux de tolérance au risque établis pour l'entité financière ont été atteints;

(c) une évaluation indiquant si l'entité financière a pris, si nécessaire, des mesures pour corriger ou améliorer ces mesures.

SECTION 3
GESTION DES ACTIFS DE TIC

Article 4
Politique de gestion des actifs de TIC

1. Dans le cadre des politiques, procédures, protocoles et outils de sécurité des TIC visés à l'article 9, paragraphe 2, du règlement (UE) 2022/2554, les entités financières élaborent, documentent et mettent en œuvre une politique de gestion des actifs de TIC.

2. La politique de gestion des actifs de TIC visée au paragraphe 1:

(a) prescrit le suivi et la gestion du cycle de vie des actifs de TIC identifiés et classés conformément à l'article 8, paragraphe 1, du règlement (UE) 2022/2554;

(b) prescrit la tenue par l'entité financière d'un registre de tous les éléments suivants:

i) l'identifiant unique de chaque actif de TIC;

ii) des informations sur la localisation, physique ou logique, de tous les actifs de TIC;

iii) le classement de tous les actifs de TIC, tel que prévu par l'article 8, paragraphe 1, du règlement (UE) 2022/2254;

iv) l'identité des propriétaires d'actifs de TIC;

v) les fonctions ou services «métiers» soutenus par l'actif de TIC;

vi) les exigences en matière de continuité des activités de TIC, notamment les objectifs en matière de délai de rétablissement et de point de rétablissement;

vii) une mention précisant si l'actif de TIC est ou peut être exposé à des réseaux externes, y compris l'internet;

viii) les liens et interdépendances existant entre les actifs de TIC et les fonctions «métiers» qui utilisent chacun de ces actifs;

ix) le cas échéant, pour tous les actifs de TIC, les dates d'expiration des services d'appui réguliers, étendus et sur mesure fournis par des prestataires tiers de services TIC, après lesquelles ces actifs de TIC ne sont plus pris en charge par leur fournisseur ou par un prestataire tiers de services TIC;

(c) prescrit la tenue, par les entités financières autres que des microentreprises, d'un registre des informations nécessaires pour procéder à l'évaluation spécifique du risque lié aux TIC sur tous les systèmes de TIC hérités prévue par l'article 8, paragraphe 7, du règlement (UE) 2022/2554.

Article 5
Procédure de gestion des actifs de TIC

1. Les entités financières élaborent, documentent et mettent en œuvre une procédure de gestion des actifs de TIC.

2. La procédure de gestion des actifs de TIC visée au paragraphe 1 précise les critères utilisés pour procéder à l'évaluation de la criticité des actifs d'information et des actifs de TIC soutenant des fonctions «métiers». Cette évaluation tient compte:

(a) du risque lié aux TIC associé à ces fonctions «métiers» et de leur dépendance à l'égard des actifs d'information ou des actifs de TIC;

(b) de l'incidence que la perte de confidentialité, d'intégrité et de disponibilité de ces actifs d'information et actifs de TIC aurait sur les processus opérationnels et les activités des entités financières.

SECTION 4
CHIFFREMENT ET CRYPTOGRAPHIE

Article 6
Chiffrement et contrôles cryptographiques

1. Dans le cadre de leurs politiques, procédures, protocoles et outils de sécurité de TIC visés à l'article 9, paragraphe 2, du règlement (UE) 2022/2554, les entités financières élaborent, documentent et mettent en œuvre une politique en matière de chiffrement et de contrôles cryptographiques.

2. Les entités financières conçoivent la politique en matière de chiffrement et de contrôles cryptographiques visée au paragraphe 1 sur la base des résultats d'une classification des données approuvée et de l'évaluation du risque lié aux TIC. Cette politique contient des règles pour tous les éléments suivants:

   (a) le chiffrement des données au repos et en transit;

   (b) le chiffrement des données en cours d'utilisation, si nécessaire;

   (c) le chiffrement des connexions internes au réseau et du trafic avec des tiers;

   (d) la gestion des clés cryptographiques visée à l'article 7, y compris des règles relatives à la bonne utilisation, à la protection et au cycle de vie des clés cryptographiques.

   Aux fins du point b), lorsque le chiffrement des données en cours d'utilisation n'est pas possible, les entités financières traitent ces données dans un environnement séparé et protégé, ou prennent des mesures équivalentes pour garantir la confidentialité, l'intégrité, l'authenticité et la disponibilité des données.

3. Les entités financières incluent dans la politique en matière de chiffrement et de contrôles cryptographiques visée au paragraphe 1 des critères de sélection des techniques cryptographiques et des pratiques d'utilisation, tenant compte des pratiques de pointe, ainsi que des normes définies à l'article 2, point 1), du règlement (UE) nº 1025/2012, et de la classification des actifs de TIC concernés effectuée conformément à l'article 8, paragraphe 1, du règlement (UE) 2022/2554. Les entités financières qui ne sont pas en mesure d'appliquer les pratiques de pointe ou les normes, ou d'utiliser les techniques les plus fiables, adoptent des mesures d'atténuation et de suivi qui garantissent la résilience face aux cybermenaces.

4. Les entités financières incluent dans la politique en matière de chiffrement et de contrôles cryptographiques visée au paragraphe 1 des dispositions relatives à la mise à jour ou à la modification, si nécessaire, de la technologie cryptographique, en fonction de l'évolution de la cryptanalyse. Ces mises à jour ou modifications garantissent que la technologie cryptographique reste résiliente face aux cybermenaces, comme l'exige l'article 10, paragraphe 2, point a). Les entités financières qui ne sont pas en mesure de mettre à jour ou de modifier la technologie cryptographique adoptent des mesures d'atténuation et de suivi qui garantissent la résilience face aux cybermenaces.

5. Les entités financières incluent dans la politique en matière de chiffrement et de contrôles cryptographiques visée au paragraphe 1 l'obligation d'enregistrer l'adoption des mesures d'atténuation et de suivi adoptées conformément aux paragraphes 3 et 4 et de fournir une explication motivée des raisons pour lesquelles elles procèdent ainsi.

Article 7
Gestion des clés cryptographiques

1. Les entités financières incluent dans la politique de gestion des clés cryptographiques visée à l'article 6, paragraphe 2, point d), des exigences relatives à la gestion des clés cryptographiques tout au long de leur cycle de vie, notamment en ce qui concerne la génération, le renouvellement, le stockage, la sauvegarde, l'archivage, la récupération, la transmission, le retrait, la révocation et la destruction de ces clés cryptographiques.

2. Les entités financières définissent et mettent en œuvre des contrôles visant à protéger les clés cryptographiques tout au long de leur cycle de vie contre la perte, les accès non autorisés, la divulgation et la modification. Les entités financières conçoivent ces contrôles sur la base des résultats de la classification des données approuvée et de l'évaluation du risque lié aux TIC.

3. Les entités financières élaborent et mettent en œuvre des méthodes pour remplacer les clés cryptographiques en cas de perte ou lorsque ces clés sont compromises ou endommagées.

4. Les entités financières créent et tiennent un registre de tous les certificats et dispositifs de stockage de certificats pour au moins les actifs de TIC qui soutiennent des fonctions critiques ou importantes. Les entités financières tiennent ce registre à jour.

5. Les entités financières veillent au renouvellement en temps utile des certificats avant leur expiration.

SECTION 5
SÉCURITÉ DES OPÉRATIONS DE TIC

Article 8
Politiques et procédures pour les opérations de TIC

1. Dans le cadre des politiques, procédures, protocoles et outils de sécurité des TIC visés à l'article 9, paragraphe 2, du règlement (UE) 2022/2554, les entités financières élaborent, documentent et mettent en œuvre des politiques et des procédures pour gérer les opérations de TIC. Ces politiques et procédures précisent la manière dont les entités financières gèrent, suivent, contrôlent et restaurent leurs actifs de TIC, y compris la documentation relative aux opérations de TIC.

2. Les politiques et procédures relatives aux opérations de TIC visées au paragraphe 1 contiennent l'ensemble des éléments suivants:

   (a) une description des actifs de TIC, comprenant l'ensemble des éléments suivants:

      i) des exigences relatives à la sécurité de l'installation, de la maintenance, de la configuration et de la désinstallation d'un système de TIC;

      ii) des exigences relatives à la gestion des actifs informationnels utilisés par les actifs de TIC, y compris leur traitement et leur gestion, tant automatisés que manuels;

      iii) des exigences relatives à l'identification et au contrôle des systèmes de TIC hérités;

(b) des contrôles et un suivi des systèmes de TIC, comprenant l'ensemble des éléments suivants:

i) des exigences de sauvegarde et de restauration des systèmes de TIC;

ii) des exigences de programmation dans le temps, tenant compte des interdépendances entre les systèmes de TIC;

iii) des protocoles pour les informations de la piste d'audit et du journal du système;

iv) des exigences visant à garantir que la réalisation d'audits internes et d'autres tests perturbe le moins possible les activités;

v) des exigences relatives à la séparation entre les environnements de production des TIC, d'une part, et les environnements de développement, de tests et les autres environnements hors production, d'autre part;

vi) des exigences imposant que le développement et les tests aient lieu dans des environnements séparés de l'environnement de production;

vii) les exigences à respecter pour développer et tester en environnement de production;

(c) le traitement des erreurs concernant les systèmes de TIC, comprenant l'ensemble des éléments suivants:

i) des procédures et protocoles de traitement des erreurs;

ii) les interlocuteurs à contacter pour un appui technique et la remontée d'informations, y compris les interlocuteurs à contacter pour un appui technique externe en cas de problèmes opérationnels ou techniques imprévus;

iii) les procédures de redémarrage, de reprise et de rétablissement des systèmes de TIC à appliquer en cas de dysfonctionnement des systèmes de TIC.

Aux fins du point b) v), la séparation tient compte de toutes les composantes de l'environnement, notamment des comptes, données ou connexions, comme l'exige l'article 13, paragraphe 1, point a).

Aux fins du point b) vii), les politiques et procédures visées au paragraphe 1 prévoient que les cas de réalisation de tests dans un environnement de production soient clairement identifiés et motivés, d'une durée limitée et approuvés par la fonction compétente conformément à l'article 16, paragraphe 6. Les entités financières garantissent la disponibilité, la confidentialité, l'intégrité et l'authenticité des systèmes de TIC et des données de production lors des activités de développement et de test dans l'environnement de production.

Article 9
Gestion des capacités et des performances

1. Dans le cadre des politiques, procédures, protocoles et outils de sécurité des TIC visés à l'article 9, paragraphe 2, du règlement (UE) 2022/2554, les entités financières élaborent, documentent et mettent en œuvre des procédures de gestion des capacités et des performances pour:

(a) l'identification des besoins en capacités de leurs systèmes de TIC;

(b) la mise en œuvre de l'optimisation des ressources;

(c) les procédures de suivi visant à maintenir et à améliorer:

i) la disponibilité des données et des systèmes de TIC;

ii) l'efficience des systèmes de TIC;

iii) la prévention des déficits de capacités en matière de TIC.

2. Les procédures de gestion des capacités et des performances visées au paragraphe 1 garantissent que les entités financières prennent des mesures adéquates pour tenir compte des spécificités des systèmes de TIC soumis à des processus de passation de marchés ou d'approbation longs ou complexes ou des systèmes de TIC qui requièrent des ressources importantes.

Article 10
Gestion des vulnérabilités et des correctifs

1. Dans le cadre des politiques, procédures, protocoles et outils de sécurité des TIC visés à l'article 9, paragraphe 2, du règlement (UE) 2022/2554, les entités financières élaborent, documentent et mettent en œuvre des procédures de gestion des vulnérabilités.

2. Les procédures de gestion des vulnérabilités visées au paragraphe 1:

(a) identifient et tiennent à jour des ressources d'information pertinentes et fiables pour renforcer et maintenir la sensibilisation aux vulnérabilités;

(b) prévoient des scans et évaluations automatisés des vulnérabilités des actifs de TIC, la fréquence et le champ d'application de ces activités étant proportionnés à la classification établie conformément à l'article 8, paragraphe 1, du règlement (UE) 2022/2554 et au profil de risque global de l'actif de TIC;

(c) vérifient:

i) si les prestataires tiers de services TIC traitent les vulnérabilités liées aux services TIC fournis à l'entité financière;

ii) si ces prestataires de services informent l'entité financière, en temps utile, au moins des vulnérabilités critiques, ainsi que des statistiques et tendances;

(d) tracent l'utilisation:

i) de bibliothèques tierces, y compris de bibliothèques à code source ouvert, utilisées par les services TIC qui soutiennent des fonctions critiques ou importantes;

ii) de services TIC développés par l'entité financière elle-même, ou spécifiquement adaptés ou développés pour elle par un prestataire tiers de services TIC;

(e) établissent des procédures pour une divulgation responsable des vulnérabilités aux clients, aux contreparties et au public;

(f) donnent la priorité au déploiement de correctifs et d'autres mesures d'atténuation pour remédier aux vulnérabilités décelées;

(g) suivent et vérifient la correction des vulnérabilités;

(h) exigent l’enregistrement de toute vulnérabilité détectée touchant les systèmes de TIC et le suivi de leur résolution.

Aux fins du point b), les entités financières effectuent au moins une fois par semaine les scans et évaluations automatisés des vulnérabilités des actifs de TIC qui soutiennent des fonctions critiques ou importantes.

Aux fins du point c), les entités financières demandent aux prestataires tiers de services TIC d’enquêter sur les vulnérabilités concernées, d’en déterminer les causes profondes et de mettre en œuvre des mesures d’atténuation appropriées.

Aux fins du point d), les entités financières surveillent, le cas échéant en collaboration avec le prestataire tiers de services TIC, les versions et mises à jour éventuelles des bibliothèques tierces. Dans le cas d’actifs de TIC prêts à l’emploi ou de composants d’actifs de TIC acquis et utilisés dans le cadre de l’exploitation de services TIC qui ne soutiennent pas des fonctions critiques ou importantes, les entités financières tracent, dans la mesure du possible, l’utilisation de bibliothèques tierces, y compris des bibliothèques à code source ouvert.

Aux fins du point f), les entités financières tiennent compte de la criticité des vulnérabilités, de la classification établie conformément à l’article 8, paragraphe 1, du règlement (UE) 2022/2554 et du profil de risque des actifs de TIC concernés par les vulnérabilités décelées.

3. Dans le cadre des politiques, procédures, protocoles et outils de sécurité des TIC visés à l’article 9, paragraphe 2, du règlement (UE) 2022/2554, les entités financières élaborent, documentent et mettent en œuvre des procédures de gestion des correctifs.

4. Les procédures de gestion des correctifs visées au paragraphe 3:

(a) dans la mesure du possible, identifient et évaluent les correctifs et mises à jour logiciels et matériels disponibles à l’aide d’outils automatisés;

(b) définissent des procédures d’urgence pour l’application des correctifs et des mises à jour des actifs de TIC;

(c) testent et déploient les correctifs logiciels et matériels et les mises à jour visées à l’article 8, paragraphe 2, point b) v), vi) et vii);

(d) fixent des délais pour l’installation des correctifs et mises à jour logiciels et matériels, ainsi que des procédures de remontée d'informations lorsque ces délais ne peuvent pas être respectés.

Article 11
Sécurité des données et des systèmes

1. Dans le cadre des politiques, procédures, protocoles et outils de sécurité des TIC visés à l’article 9, paragraphe 2, du règlement (UE) 2022/2554, les entités financières élaborent, documentent et mettent en œuvre une procédure de sécurité des données et des systèmes.

2. La procédure de sécurité des données et des systèmes visée au paragraphe 1 contient tous les éléments suivants relatifs à la sécurité des données et des systèmes de TIC, conformément à la classification établie en application de l’article 8, paragraphe 1, du règlement (UE) 2022/2554:

(a) les restrictions d’accès, visées à l’article 21 du présent règlement, appuyant les exigences de protection prévues pour chaque niveau de classification;

(b) l'identification d'une configuration sécurisée de référence pour les actifs de TIC qui réduise à un minimum l'exposition de ces actifs aux cybermenaces, et des mesures visant à vérifier régulièrement que ces références sont effectivement déployées;

(c) la définition de mesures de sécurité visant à garantir que seuls des logiciels autorisés sont installés dans les systèmes de TIC et les périphériques de point de terminaison;

(d) la définition de mesures de sécurité contre les codes malveillants;

(e) la définition de mesures de sécurité visant à garantir que seuls des supports de stockage de données, des systèmes et des périphériques de point de terminaison autorisés sont utilisés pour transférer et stocker les données de l'entité financière;

(f) les exigences suivantes, pour sécuriser l'utilisation de périphériques de point de terminaison portables et de périphériques de point de terminaison non portables privés:

  i) l'obligation d'utiliser une solution de gestion qui permet de gérer à distance les périphériques de point de terminaison et d'effacer à distance les données de l'entité financière;

  ii) l'obligation d'utiliser des mécanismes de sécurité qui ne peuvent pas être modifiés, supprimés ou contournés sans autorisation par des membres du personnel ou par des prestataires tiers de services TIC;

  iii) l'obligation de n'utiliser des dispositifs de stockage de données amovibles que lorsque le risque résiduel lié aux TIC reste dans les limites du niveau de tolérance au risque de l'entité financière visé à l'article 3, paragraphe 1, point a);

(g) le processus d'effacement sécurisé des données, présentes dans les locaux de l'entité financière ou stockées à l'extérieur, que l'entité financière n'a plus besoin de collecter ou de stocker;

(h) le processus d'élimination ou de déclassement en toute sécurité des dispositifs de stockage de données, présents dans les locaux de l'entité financière ou stockés à l'extérieur, qui contiennent des informations confidentielles;

(i) la définition et la mise en œuvre, pour les systèmes et les périphériques de point de terminaison, de mesures de sécurité visant à prévenir la perte et la fuite de données;

(j) la mise en œuvre de mesures de sécurité visant à garantir que le télétravail et l'utilisation de périphériques de point de terminaison privés n'aient pas d'incidence négative sur la sécurité des TIC de l'entité financière;

(k) pour les actifs de TIC ou les services TIC exploités par un prestataire tiers de services TIC, la définition et la mise en œuvre d'exigences visant à maintenir la résilience opérationnelle numérique, conformément aux résultats de la classification des données et de l'évaluation du risque lié aux TIC.

La configuration sécurisée de référence visée au point b) tient compte, aux fins dudit point, des pratiques de pointe et des techniques appropriées définies dans les normes visées à l'article 2, point 1), du règlement (UE) nº 1025/2012.

Aux fins du point k), les entités financières prennent en considération les éléments suivants:

(a) l'application de paramètres recommandés par le vendeur aux éléments exploités par l'entité financière;

(b) une attribution claire des rôles et des responsabilités en matière de sécurité de l'information entre l'entité financière et le prestataire tiers de services TIC, conformément au principe, défini à l'article 28, paragraphe 1, point a), du règlement (UE) 2022/2554, selon lequel l'entité financière est pleinement responsable de son prestataire tiers de services TIC, et conformément à la politique de l'entité financière relative à l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes, pour les entités financières visées à l'article 28, paragraphe 2, dudit règlement;

(c) la nécessité de garantir et de maintenir des compétences adéquates au sein de l'entité financière en matière de gestion et de sécurité du service utilisé;

(d) des mesures techniques et organisationnelles visant à réduire à un minimum les risques liés à l'infrastructure utilisée par le prestataire tiers de services TIC pour ses services TIC, compte tenu des pratiques de pointe et des normes telles que définies à l'article 2, point 1), du règlement (UE) nº 1025/2012.

Article 12
Journalisation

1. Dans le cadre des garanties contre les intrusions et l'utilisation abusive de données, les entités financières élaborent, documentent et mettent en œuvre des procédures, protocoles et outils de journalisation.

2. Les procédures, protocoles et outils de journalisation visés au paragraphe 1 contiennent l'ensemble des éléments suivants:

(a) l'identification des événements à enregistrer dans le journal, la durée de conservation des journaux et les mesures visant à sécuriser et à gérer les données des journaux, en tenant compte de la finalité pour laquelle les journaux sont créés;

(b) l'alignement du niveau de détail des journaux sur leur finalité et leur utilisation, afin de permettre la détection effective des activités anormales visées à l'article 24;

(c) l'obligation de consigner dans les journaux les événements relatifs à l'ensemble des éléments suivants:

i) le contrôle de l'accès logique et physique, tel que visé à l'article 21, et la gestion de l'identité;

ii) la gestion des capacités;

iii) la gestion des modifications.

iv) les opérations de TIC, y compris les activités liées aux systèmes de TIC;

v) le trafic réseau, y compris les performances des réseaux de TIC;

(d) des mesures visant à protéger les systèmes de journalisation et les informations des journaux contre les manipulations, la suppression et l'accès non autorisé, au repos, en transit et, le cas échéant, en cours d'utilisation;

(e) des mesures visant à détecter les défaillances des systèmes de journalisation;

(f) sans préjudice de toute exigence réglementaire applicable en vertu du droit de l'Union ou du droit national, la synchronisation des horloges de chacun des systèmes de TIC de l'entité financière avec une horloge de référence fiable et documentée.

Aux fins du point a), les entités financières définissent la durée de conservation, en prenant en considération les objectifs en matière de sécurité des activités et de l'information, la raison de l'enregistrement de l'événement dans les journaux et les résultats de l'évaluation du risque lié aux TIC.

SECTION 6
SECURITE DES RESEAUX

Article 13
Gestion de la sécurité des réseaux

1. Dans le cadre des garanties de sécurité des réseaux contre les intrusions et l'utilisation abusive de données, les entités financières élaborent, documentent et mettent en œuvre des politiques, des procédures, des protocoles et des outils de gestion de la sécurité des réseaux comprenant l'ensemble des éléments suivants:

(a) la séparation et la segmentation des systèmes et réseaux de TIC, compte tenu:

i) de la criticité ou de l'importance de la fonction que soutiennent ces systèmes et réseaux de TIC;

ii) de la classification établie conformément à l'article 8, paragraphe 1, du règlement (UE) 2022/2554;

iii) du profil de risque global des actifs de TIC qui utilisent ces systèmes et réseaux de TIC;

(b) la documentation de l'ensemble des connexions réseau et des flux de données de l'entité financière;

(c) l'utilisation d'un réseau distinct et spécifique pour l'administration des actifs de TIC;

(d) la définition et la mise en œuvre de contrôles d'accès au réseau afin de prévenir et de détecter les connexions au réseau de l'entité financière à partir de tout appareil ou système non autorisé, ou de tout point de terminaison ne répondant pas aux exigences de l'entité financière en matière de sécurité;

(e) le chiffrement des connexions au réseau transitant par des réseaux d'entreprise, des réseaux publics, des réseaux nationaux, des réseaux tiers et des réseaux sans fil, pour les protocoles de communication utilisés, en tenant compte des résultats de la classification de données approuvée, des résultats de l'évaluation du risque lié aux TIC et du chiffrement des connexions au réseau prévu par l'article 6, paragraphe 2;

(f) une conception du réseau conforme aux exigences en matière de sécurité des TIC définies par l'entité financière, tenant compte des pratiques de pointe afin de garantir la confidentialité, l'intégrité et la disponibilité du réseau;

(g) la sécurisation du trafic entre les réseaux internes et l'internet et d'autres connexions externes;

(h) la définition des rôles et responsabilités et des étapes de la spécification, de la mise en œuvre, de l'approbation, de la modification et du réexamen des règles de pare-feu et des filtres de connexion;

(i) la réalisation d'examens de l'architecture du réseau et de la conception de la sécurité du réseau une fois par an, et périodiquement pour les microentreprises, afin de détecter les vulnérabilités potentielles;

(j) des mesures visant à isoler temporairement, si nécessaire, les sous-réseaux et les composants et dispositifs de réseau;

(k) la mise en œuvre d'une configuration sécurisée de référence incluant tous les composants du réseau, et le renforcement du réseau et des dispositifs de réseau conformément aux éventuelles instructions du vendeur, aux normes telles que définies à l'article 2, point 1), du règlement (UE) nº 1025/2012, le cas échéant, et aux pratiques de pointe;

(l) les procédures de limitation, de verrouillage et d'arrêt du système et des sessions à distance après une période déterminée d'inactivité;

(m) pour les accords de services de réseau:

i) l'indication et la spécification des mesures de sécurité des TIC et de l'information, des niveaux de service et des exigences en matière de gestion de tous les services de réseau;

ii) une indication précisant si ces services sont fournis par un prestataire intra-groupe de services TIC ou par des prestataires tiers de services TIC.

Aux fins du point h), les entités financières procèdent à un réexamen régulier des règles de pare-feu et des filtres de connexion, conformément à la classification établie en application de l'article 8, paragraphe 1, du règlement (UE) 2022/2554 et au profil de risque global des systèmes de TIC concernés. Pour les systèmes de TIC qui soutiennent des fonctions critiques ou importantes, les entités financières vérifient l'adéquation des règles de pare-feu et des filtres de connexion existants au moins tous les six mois.

Article 14
Sécurisation des informations en transit

1. Dans le cadre des garanties visant à préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, les entités financières élaborent, documentent et mettent en œuvre les politiques, procédures, protocoles et outils de protection des informations en transit. Les entités financières veillent en particulier à l'ensemble des éléments suivants:

(a) la disponibilité, l'authenticité, l'intégrité et la confidentialité des données pendant la transmission sur le réseau, et l'établissement de procédures permettant d'évaluer le respect de ces exigences;

(b) la prévention et la détection des fuites de données et le transfert sécurisé d'informations entre l'entité financière et des parties externes;

(c) la mise en œuvre, la documentation et le réexamen régulier d'exigences relatives à des accords de confidentialité ou de non-divulgation reflétant les besoins de l'entité financière en matière de protection des informations tant pour son personnel que pour les tiers.

2. Les entités financières conçoivent les politiques, procédures, protocoles et outils visant à protéger les informations en transit visées au paragraphe 1 sur la base des résultats de la classification des données approuvée et de l'évaluation du risque lié aux TIC.

SECTION 7
GESTION DES PROJETS DE TIC ET DES CHANGEMENTS DANS LES TIC

Article 15
Gestion des projets de TIC

1. Dans le cadre des garanties visant à préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, les entités financières élaborent, documentent et mettent en œuvre une politique de gestion des projets de TIC.

2. La politique de gestion des projets de TIC visée au paragraphe 1 précise les éléments qui garantissent la gestion efficace des projets de TIC liés à l'acquisition, à la maintenance et, le cas échéant, au développement des systèmes de TIC de l'entité financière.

3. La politique de gestion des projets de TIC visée au paragraphe 1 comporte l'ensemble des éléments suivants:

   (a) les objectifs des projets de TIC;

   (b) la gouvernance des projets de TIC, notamment les rôles et responsabilités;

   (c) la planification, le calendrier et les étapes des projets de TIC;

   (d) l'évaluation des risques liés aux projets de TIC;

   (e) les jalons pertinents;

   (f) les exigences en matière de gestion des changements;

   (g) les tests de toutes les exigences, notamment des exigences de sécurité, et le processus d'approbation correspondant lors du déploiement d'un système de TIC dans l'environnement de production.

4. La politique de gestion des projets de TIC visée au paragraphe 1 garantit la sécurité de la mise en œuvre des projets de TIC grâce à la fourniture des informations et de l'expertise nécessaires par le domaine d'activité ou les fonctions concernées par les projets de TIC.

5. Conformément à l'évaluation des risques liés aux projets de TIC visée au paragraphe 3, point d), la politique de gestion des projets de TIC visée au paragraphe 1 prévoit que la mise en place de projets de TIC ayant une incidence sur les fonctions critiques ou importantes de l'entité financière, l'avancement de ces projets et les risques qui y sont associés sont notifiés à l'organe de direction comme suit:

   (a) individuellement ou de façon groupée, en fonction de l'importance et de la taille des projets de TIC;

   (b) périodiquement et, si nécessaire, chaque fois qu'un évènement l'exige.

Article 16

Acquisition, développement et maintenance des systèmes de TIC

1. Dans le cadre des garanties visant à préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, les entités financières élaborent, documentent et mettent en œuvre une politique régissant l'acquisition, le développement et la maintenance des systèmes de TIC. Cette politique:

   (a) identifie les pratiques en matière de sécurité et les méthodes relatives à l'acquisition, au développement et à la maintenance des systèmes de TIC;

   (b) exige l'identification:

      i) des spécifications techniques et des spécifications techniques des TIC, au sens de l'article 2, points 4) et 5), du règlement (UE) nº 1025/2012;

      ii) des exigences relatives à l'acquisition, au développement et à la maintenance des systèmes de TIC, en accordant une attention particulière aux exigences en matière de sécurité des TIC et à leur approbation par la fonction «métier» concernée et par le propriétaire des actifs de TIC conformément aux dispositifs de gouvernance interne de l'entité financière;

   (c) précise les mesures visant à atténuer le risque d'altération involontaire ou de manipulation intentionnelle des systèmes de TIC lors du développement, de la maintenance et du déploiement de ces systèmes dans l'environnement de production.

2. Les entités financières élaborent, documentent et mettent en œuvre une procédure d'acquisition, de développement et de maintenance des systèmes de TIC pour les tests et l'approbation de tous les systèmes de TIC avant leur utilisation et après les opérations de maintenance, conformément à l'article 8, paragraphe 2, point b) v), vi) et vii). Le niveau des tests doit être proportionné à la criticité des procédures opérationnelles et des actifs de TIC concernés. Les tests sont conçus pour permettre de vérifier que les nouveaux systèmes de TIC sont aptes à fonctionner comme prévu, ainsi que la qualité du logiciel développé en interne.

   En plus de respecter les exigences prévues au premier alinéa, les contreparties centrales associent, s'il y a lieu, à la conception et à la conduite des tests visés au premier alinéa:

   (a) les membres compensateurs et leurs clients;

   (b) les contreparties centrales interopérables;

   (c) les autres parties intéressées.

   En plus de respecter les exigences énoncées au premier alinéa, les dépositaires centraux de titres associent, s'il y a lieu, à la conception et à la conduite des tests visés au premier alinéa:

   (a) les utilisateurs;

   (b) les prestataires de services et fournisseurs de services de réseau essentiels;

   (c) d'autres dépositaires centraux de titres;

   (d) d'autres infrastructures de marché;

(e) d’autres établissements avec lesquels les dépositaires centraux de titres ont constaté des interdépendances dans le cadre de leur politique de continuité des activités.

3. La procédure visée au paragraphe 2 comprend la réalisation d’examens du code source comprenant des tests aussi bien statiques que dynamiques. Ces tests comprennent des tests de sécurité pour les systèmes et applications exposés à l’internet conformément à l’article 8, paragraphe 2, point b) v), vi) et vii). Les entités financières:

(a) identifient et analysent les vulnérabilités et les anomalies dans le code source;

(b) adoptent un plan d’action pour remédier à ces vulnérabilités et anomalies;

(c) suivent la mise en œuvre de ce plan d’action.

4. La procédure visée au paragraphe 2 comprend des tests de sécurité des progiciels au plus tard lors de la phase d’intégration, conformément à l’article 8, paragraphe 2, point b) v), vi) et vii).

5. La procédure visée au paragraphe 2 prévoit que:

(a) les environnements hors production ne stockent que des données de production anonymisées, pseudonymisées ou randomisées;

(b) les entités financières doivent protéger l’intégrité et la confidentialité des données dans les environnements hors production.

6. Par dérogation au paragraphe 5, la procédure visée au paragraphe 2 peut prévoir que les données de production ne sont stockées que pour des situations de test spécifiques, pendant des durées limitées, et après approbation par la fonction compétente et la notification de ces situations à la fonction de gestion du risque lié aux TIC.

7. La procédure visée au paragraphe 2 comprend la mise en œuvre de contrôles visant à protéger l’intégrité du code source des systèmes de TIC qui sont développés en interne ou développés par un prestataire tiers de services TIC et fournis à l’entité financière par ce prestataire.

8. La procédure visée au paragraphe 2 prévoit que les logiciels propriétaires et, dans la mesure du possible, le code source fourni par des prestataires tiers de services TIC ou provenant de projets à code source ouvert doivent être analysés et testés conformément au paragraphe 3 avant leur déploiement dans l’environnement de production.

9. Les paragraphes 1 à 8 du présent article s’appliquent également aux systèmes de TIC développés ou gérés par des utilisateurs extérieurs à la fonction TIC, selon une approche fondée sur les risques.

Article 17
Gestion des changements dans les TIC

1. Dans le cadre des garanties visant à préserver la disponibilité, l’authenticité, l’intégrité et la confidentialité des données, les entités financières incluent dans les procédures de gestion des changements dans les TIC visées à l’article 9, paragraphe 4, point e), du règlement (UE) 2022/2554, en ce qui concerne tous les changements apportés aux logiciels, au matériel, aux composants de micrologiciels, aux systèmes ou aux paramètres de sécurité, l’ensemble des éléments suivants:

(a) une vérification du respect des exigences en matière de sécurité des TIC;

(b) des mécanismes visant à garantir l'indépendance des fonctions qui approuvent les changements et des fonctions responsables de la demande et de la mise en œuvre de ces changements;

(c) une description claire des rôles et des responsabilités afin de garantir:

i) que les changements sont définis et planifiés;

ii) qu'une transition adéquate est conçue;

iii) que les changements sont testés et finalisés de manière contrôlée;

iv) qu'il existe une assurance de la qualité efficace;

(d) la documentation et la communication des détails des changements, notamment:

i) de l'objectif et de la portée du changement;

ii) du calendrier de mise en œuvre du changement;

iii) des résultats attendus;

(e) l'identification des procédures et responsabilités de repli, notamment des procédures et responsabilités pour l'abandon des changements ou le rétablissement à la suite de changements qui n'ont pas été mis en œuvre avec succès;

(f) des procédures, protocoles et outils de gestion des changements d'urgence qui offrent des garanties adéquates;

(g) des procédures de documentation, de réévaluation, d'évaluation et d'approbation des changements d'urgence après leur mise en œuvre, y compris des solutions de contournement et des correctifs;

(h) l'identification de l'incidence potentielle d'un changement sur les mesures existantes en matière de sécurité des TIC et une évaluation visant à déterminer si ce changement nécessite l'adoption de mesures supplémentaires en matière de sécurité des TIC.

2. Après avoir apporté des changements importants à leurs systèmes de TIC, les contreparties centrales et les dépositaires centraux de titres soumettent leurs systèmes de TIC à des tests rigoureux, en simulant des situations de crise.

Les contreparties centrales associent, s'il y a lieu, à la conception et à la conduite des tests visés au premier alinéa:

(a) les membres compensateurs et leurs clients;

(b) les contreparties centrales interopérables;

(c) les autres parties intéressées.

Les dépositaires centraux de titres associent, s'il y a lieu, à la conception et à la conduite des tests visés au premier alinéa:

(a) les utilisateurs;

(b) les prestataires de services et fournisseurs de services de réseau essentiels;

(c) d'autres dépositaires centraux de titres;

(d) d’autres infrastructures de marché;

(e) d’autres établissements avec lesquels les dépositaires centraux de titres ont constaté des interdépendances dans le cadre de leur politique de continuité des activités de TIC.

SECTION 8

Article 18
Sécurité physique et environnementale

1. Dans le cadre des garanties visant à préserver la disponibilité, l’authenticité, l’intégrité et la confidentialité des données, les entités financières précisent, documentent et mettent en œuvre une politique de sécurité physique et environnementale. Les entités financières conçoivent cette politique à la lumière de l’éventail des cybermenaces, conformément à la classification établie en application de l’article 8, paragraphe 1, du règlement (UE) 2022/2554, et à la lumière du profil de risque global des actifs de TIC et des actifs informationnels accessibles.

2. La politique de sécurité physique et environnementale visée au paragraphe 1 comporte l’ensemble des éléments suivants:

(a) une référence à la section de la politique relative au contrôle des droits de gestion des accès visé à l’article 21, paragraphe 1, point g);

(b) des mesures de protection des locaux, des centres de données de l’entité financière et des zones sensibles désignées par l’entité financière, où se trouvent les actifs de TIC et les actifs informationnels, contre les attaques, les accidents et les menaces et dangers environnementaux;

(c) des mesures visant à sécuriser les actifs de TIC, tant à l’intérieur qu’à l’extérieur des locaux de l’entité financière, en tenant compte des résultats de l’évaluation du risque lié aux TIC portant sur les actifs de TIC concernés;

(d) des mesures visant à garantir la disponibilité, l’authenticité, l’intégrité et la confidentialité des actifs de TIC, des actifs informationnels et des dispositifs de contrôle de l’accès physique de l’entité financière grâce à une maintenance appropriée;

(e) des mesures visant à préserver la disponibilité, l’authenticité, l’intégrité et la confidentialité des données, notamment:

i) une politique du bureau propre pour les documents;

ii) une politique de l’écran vide pour les installations de traitement de l’information.

Aux fins du point b), les mesures de protection contre les menaces et dangers environnementaux sont proportionnées à l’importance des locaux, des centres de données, des zones sensibles désignées et à la criticité des opérations ou des systèmes de TIC qui y sont situés.

Aux fins du point c), la politique de sécurité physique et environnementale visée au paragraphe 1 comporte des mesures visant à assurer une protection appropriée des actifs de TIC laissés sans surveillance.

Chapitre II
POLITIQUE DES RESSOURCES HUMAINES ET CONTRÔLE D'ACCÈS

Article 19
Politique des ressources humaines

Les entités financières incluent dans leur politique en matière de ressources humaines ou dans d'autres politiques pertinentes tous les éléments suivants liés à la sécurité des TIC:

(a) l'identification et l'attribution de toute responsabilité spécifique en matière de sécurité des TIC;

(b) l'obligation pour les membres du personnel de l'entité financière et des prestataires tiers de services TIC qui utilisent des actifs de TIC de l'entité financière ou qui y ont accès:

i) d'être informés des politiques, procédures et protocoles de sécurité des TIC de l'entité financière et de les respecter;

ii) de connaître les canaux de notification mis en place par l'entité financière pour la détection des comportements anormaux, y compris, le cas échéant, les canaux de signalement établis conformément à la directive (UE) 2019/1937 du Parlement européen et du Conseil[10];

iii) de restituer à l'entité financière, après la cessation de leur emploi, tous les actifs de TIC et tous les actifs informationnels matériels en leur possession qui appartiennent à l'entité financière.

Article 20
Gestion de l'identité

1. Dans le cadre de leur contrôle des droits de gestion des accès, les entités financières élaborent, documentent et mettent en œuvre des politiques et procédures de gestion de l'identité qui garantissent l'identification et l'authentification uniques des personnes physiques et des systèmes ayant accès aux informations des entités financières afin de permettre l'attribution de droits d'accès aux utilisateurs conformément à l'article 21.

2. Les politiques et procédures de gestion de l'identité visées au paragraphe 1 comportent l'ensemble des éléments suivants:

(a) sans préjudice de l'article 21, paragraphe 1, point c), une identité unique correspondant à un compte d'utilisateur unique est attribuée à chaque membre du personnel de l'entité financière ou du personnel des prestataires tiers de services TIC qui ont accès aux actifs informationnels et aux actifs de TIC de l'entité financière;

[10] Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (JO L 305 du 26.11.2019, p. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj?locale=fr).

(b) un processus de gestion du cycle de vie pour les identités et les comptes régissant la création, la modification, le réexamen et la mise à jour, la désactivation temporaire et la clôture de tous les comptes.

Aux fins du point a), les entités financières tiennent des registres de toutes les attributions d'identité. Ces registres sont conservés à la suite d'une réorganisation de l'entité financière ou après la fin d'une relation contractuelle, sans préjudice des exigences en matière de conservation prévues par le droit de l'Union et le droit national applicables.

Aux fins du point b), les entités financières déploient, lorsque cela est possible et approprié, des solutions automatisées pour le processus de gestion de l'identité tout au long du cycle de vie.

Article 21
Contrôle d'accès

Dans le cadre de leur contrôle des droits de gestion des accès, les entités financières élaborent, documentent et mettent en œuvre une politique qui comporte l'ensemble des éléments suivants:

(a) l'attribution de droits d'accès aux actifs de TIC selon les principes du besoin d'en connaître, du besoin d'en disposer et du moindre privilège, y compris pour l'accès à distance et l'accès d'urgence;

(b) une séparation des tâches visant à empêcher un accès injustifié à des données critiques ou à empêcher l'attribution de combinaisons de droits d'accès susceptibles d'être utilisées pour contourner les contrôles;

(c) des dispositions sur la responsabilité des utilisateurs, en limitant, dans la mesure du possible, l'utilisation de comptes utilisateurs génériques ou partagés et en veillant à ce que les utilisateurs soient à tout moment identifiables pour les actions effectuées dans les systèmes de TIC;

(d) des dispositions sur les restrictions d'accès aux actifs de TIC, prévoyant des contrôles et des outils pour empêcher tout accès non autorisé;

(e) des procédures de gestion de comptes permettant d'accorder, de modifier ou de révoquer des droits d'accès pour les comptes d'utilisateurs et les comptes génériques, y compris les comptes génériques d'administrateur, comportant des dispositions relatives à tous les éléments suivants:

i) l'attribution des rôles et des responsabilités pour l'octroi, le réexamen et la révocation des droits d'accès;

ii) l'attribution d'accès privilégiés, d'urgence et d'administrateur uniquement sur la base du besoin d'en disposer ou au cas par cas pour tous les systèmes de TIC;

iii) le retrait des droits d'accès sans retard injustifié à la fin de l'emploi ou lorsque l'accès n'est plus nécessaire;

iv) la mise à jour des droits d'accès lorsque des modifications sont nécessaires et au moins une fois par an pour tous les systèmes de TIC autres que les systèmes de TIC qui soutiennent des fonctions critiques ou importantes et au moins tous les six mois pour les systèmes de TIC qui soutiennent des fonctions critiques ou importantes;

(f) des méthodes d'authentification, comprenant l'ensemble des éléments suivants:

i) l'utilisation de méthodes d'authentification proportionnées à la classification établie conformément à l'article 8, paragraphe 1, du règlement (UE) 2022/2554 et au profil de risque global des actifs de TIC et tenant compte des pratiques de pointe;

ii) l'utilisation de méthodes d'authentification forte conformément aux pratiques et techniques de pointe pour l'accès à distance au réseau de l'entité financière, pour les accès privilégiés, pour l'accès aux actifs de TIC soutenant des fonctions critiques ou importantes ou aux actifs de TIC accessibles au public;

(g) des mesures de contrôle de l'accès physique comprenant:

i) l'identification et la journalisation des personnes physiques autorisées à accéder aux locaux, aux centres de données et aux zones sensibles désignées par l'entité financière où sont situés les actifs de TIC et les actifs informationnels;

ii) l'octroi de droits d'accès physique aux actifs de TIC critiques uniquement aux personnes autorisées, conformément aux principes du besoin d'en connaître et du moindre privilège, et au cas par cas;

iii) le suivi de l'accès physique aux locaux, aux centres de données et aux zones sensibles désignées par l'entité financière où sont situés les actifs de TIC, les actifs informationnels ou les deux types d'actifs;

iv) le réexamen des droits d'accès physique afin de veiller à ce que les droits d'accès inutiles soient rapidement révoqués.

Aux fins du point e) i), les entités financières définissent la durée de conservation en prenant en considération les objectifs en matière de sécurité des activités et de l'information, les raisons de l'enregistrement de l'événement dans les journaux et les résultats de l'évaluation du risque lié aux TIC.

Aux fins du point e) ii), les entités financières utilisent, dans la mesure du possible, des comptes spécifiques pour l'exécution de tâches administratives relatives aux systèmes de TIC. Lorsque cela est possible et approprié, les entités financières déploient des solutions automatisées pour la gestion des accès privilégiés.

Aux fins du point g) i), l'identification et la journalisation sont proportionnées à l'importance des locaux, des centres de données et des zones sensibles désignées et à la criticité des opérations ou des systèmes de TIC qui y sont situés.

Aux fins du point g) iii), le suivi est proportionné à la classification établie conformément à l'article 8, paragraphe 1, du règlement (UE) 2022/2554 et à la criticité de la zone accessible.

CHAPITRE III
DÉTECTION DES INCIDENTS LIÉS AUX TIC ET RÉPONSE À CES INCIDENTS

Article 22
Politique de gestion des incidents liés aux TIC

Dans le cadre des mécanismes de détection des activités anormales, y compris des problèmes de performance des réseaux de TIC et des incidents liés aux TIC, les entités financières

élaborent, documentent et mettent en œuvre une politique en matière d'incidents liés aux TIC dans le cadre de laquelle elles:

(a) documentent le processus de gestion des incidents liés aux TIC visé à l'article 17 du règlement (UE) 2022/2554;

(b) établissent une liste des contacts pertinents avec les fonctions internes et les parties prenantes externes qui sont directement associées à la sécurité des opérations de TIC, notamment en ce qui concerne:

  i) la détection et le suivi des cybermenaces;

  ii) la détection des activités anormales;

  iii) la gestion des vulnérabilités;

(c) établissent, mettent en œuvre et gèrent des mécanismes techniques, organisationnels et opérationnels pour soutenir le processus de gestion des incidents liés aux TIC, notamment des mécanismes permettant de détecter rapidement les activités et comportements anormaux conformément à l'article 23 du présent règlement;

(d) conservent tous les éléments de preuve relatifs aux incidents liés aux TIC pendant une durée qui n'excède pas celle nécessaire à la réalisation des finalités pour lesquelles les données sont collectées, et qui est proportionnée à la criticité des fonctions «métiers», des processus d'appui et des actifs de TIC et informationnels affectés, conformément à l'article [15] du règlement délégué (UE) […]/[…] de la Commission [règlement délégué de la Commission sur la classification des incidents liés aux TIC][11] et à toute exigence en matière de conservation applicable en vertu du droit de l'Union;

(e) établissent et mettent en œuvre des mécanismes permettant d'analyser les incidents importants ou récurrents liés aux TIC et les caractéristiques relatives au nombre et à la fréquence des incidents liés aux TIC.

Aux fins du point d), les entités financières conservent les éléments de preuve visés audit point de manière sécurisée aux fins dudit point.

Article 23

Détection des activités anormales et critères pour la détection des incidents liés aux TIC et la réponse à ces incidents

1. Les entités financières définissent clairement les rôles et les responsabilités pour ce qui est de détecter efficacement les incidents liés aux TIC et les activités anormales et d'y répondre.

2. Le mécanisme permettant de détecter rapidement les activités anormales, y compris les problèmes de performance des réseaux de TIC et les incidents liés aux TIC, visé à l'article 10, paragraphe 1, du règlement (UE) 2022/2554, permet aux entités financières:

  (a) de collecter, suivre et analyser l'ensemble des éléments suivants:

    i) les facteurs internes et externes, y compris au moins les journaux collectés conformément à l'article 12 du présent règlement, les informations provenant des fonctions «métiers» et des fonctions TIC, et tout problème signalé par les utilisateurs de l'entité financière;

[11] (OP: prière d'insérer [référence et titre de ce règlement délégué de la Commission])

ii) les cybermenaces potentielles internes et externes, en tenant compte des scénarios couramment utilisés par les acteurs de la menace et des scénarios fondés sur les activités de renseignement sur les menaces;

iii) les notifications, par un prestataire tiers de services TIC de l'entité financière, d'incidents liés aux TIC détectés dans les systèmes et réseaux de TIC du prestataire tiers de services TIC et susceptibles d'affecter l'entité financière;

(b) d'identifier les activités et les comportements anormaux et de mettre en œuvre des outils générant des alertes pour les activités et comportements anormaux, au moins pour les actifs de TIC et les actifs informationnels qui soutiennent des fonctions critiques ou importantes;

(c) de hiérarchiser les alertes visées au point b) afin de permettre que les incidents liés aux TIC détectés soient gérés dans le délai de résolution prévu, tel que spécifié par les entités financières, tant pendant les heures de travail qu'en dehors de celles-ci;

(d) d'enregistrer, analyser et évaluer, automatiquement ou manuellement, toutes les informations pertinentes sur l'ensemble des activités et comportements anormaux.

Aux fins du point b), les outils visés audit point comprennent des outils qui fournissent des alertes automatisées selon des règles prédéfinies afin de détecter les anomalies affectant l'exhaustivité et l'intégrité des sources de données ou de la collecte de journaux.

3. Les entités financières protègent tout enregistrement d'activités anormales contre toute falsification et tout accès non autorisé au repos, en transit et, le cas échéant, en cours d'utilisation.

4. Les entités financières journalisent, pour chaque activité anormale détectée, toutes les informations pertinentes permettant:

(a) de déterminer la date et l'heure de survenance de l'activité anormale;

(b) de déterminer la date et l'heure de détection de l'activité anormale;

(c) de déterminer le type d'activité anormale.

5. Pour déclencher les processus de détection des incidents liés aux TIC et de réponse à ces incidents visés à l'article 10, paragraphe 2, du règlement (UE) 2022/2554, les entités financières tiennent compte de l'ensemble des critères suivants:

(a) des éléments indiquant qu'une activité malveillante est susceptible d'avoir été menée dans un système ou un réseau de TIC, ou que ce système ou réseau de TIC est susceptible d'avoir été compromis;

(b) des pertes de données détectées en lien avec la disponibilité, l'authenticité, l'intégrité et la confidentialité des données;

(c) une incidence négative détectée sur les transactions et opérations de l'entité financière;

(d) l'indisponibilité des systèmes et réseaux de TIC.

6. Aux fins du paragraphe 5, les entités financières tiennent également compte de la criticité des services affectés.

CHAPITRE IV
GESTION DE LA CONTINUITÉ DES ACTIVITÉS DE TIC

Article 24
Composantes de la politique de continuité des activités de TIC

1. Les entités financières incluent dans leur politique de continuité des activités de TIC visée à l'article 11, paragraphe 1, du règlement (UE) 2022/2554 l'ensemble des éléments suivants:

   (a) une description:

      i) des objectifs de la politique de continuité des activités de TIC, notamment l'interaction entre la continuité des activités de TIC et la continuité globale des activités, en tenant compte des résultats de l'analyse des incidences sur les activités visée à l'article 11, paragraphe 5, du règlement (UE) 2022/2554;

      ii) du champ d'application des dispositifs, plans, procédures et mécanismes de continuité des activités de TIC, y compris des limitations et exclusions;

      iii) de la période de temps à couvrir par les dispositifs, plans, procédures et mécanismes de continuité des activités de TIC;

      iv) des critères d'activation et de désactivation des plans de continuité des activités de TIC, des plans de réponse et de rétablissement des TIC, ainsi que des plans de communication en situation de crise;

   (b) des dispositions concernant:

      i) la gouvernance et l'organisation nécessaires à la mise en œuvre de la politique de continuité des activités de TIC, y compris les rôles, les responsabilités et les procédures de remontée des informations, en veillant à ce que des ressources suffisantes soient disponibles;

      ii) l'alignement entre les plans de continuité des activités de TIC et les plans globaux de continuité des activités, en ce qui concerne au moins l'ensemble des éléments suivants:

         1) les scénarios de défaillance potentielle, notamment les scénarios visés à l'article 26, paragraphe 2, du présent règlement;

         2) les objectifs de rétablissement, en précisant que l'entité financière doit être en mesure de rétablir les opérations de ses fonctions critiques ou importantes après des perturbations en respectant un objectif en matière de délai de rétablissement et un objectif en matière de point de rétablissement;

      iii) l'élaboration de plans de continuité des activités de TIC en cas de graves perturbations des activités dans le cadre de ces plans, et la hiérarchisation des mesures de continuité des activités de TIC selon une approche fondée sur les risques;

      iv) l'élaboration, le test et l'examen des plans de réponse et de rétablissement des TIC, conformément aux articles 25 et 26 du présent règlement;

v) l’examen de l’efficacité des dispositifs, plans, procédures et mécanismes de continuité des activités de TIC mis en œuvre, conformément à l’article 26 du présent règlement;

vi) l’alignement de la politique de continuité des activités de TIC sur:

1) la politique de communication visée à l’article 14, paragraphe 2, du règlement (UE) 2022/2554;

2) les mesures de communication et de communication de crise visées à l’article 11, paragraphe 2, point e), du règlement (UE) 2022/2554.

2. En plus de respecter les exigences prévues au paragraphe 1, les contreparties centrales veillent à ce que leur politique de continuité des activités de TIC:

(a) prévoie, pour leurs fonctions critiques, un délai de rétablissement maximal ne dépassant pas deux heures;

(b) tienne compte des liens extérieurs et des interdépendances au sein des infrastructures financières, y compris les plates-formes de négociation compensées par la contrepartie centrale, les systèmes de règlement et de paiement des opérations sur titres, et les établissements de crédit utilisés par la contrepartie centrale ou par une contrepartie centrale à laquelle elle est liée;

(c) exige la mise en place de dispositifs pour:

i) assurer la continuité des fonctions critiques ou importantes de la contrepartie centrale sur la base de scénarios de sinistres;

ii) maintenir un site de traitement secondaire capable d’assurer la continuité des fonctions critiques ou importantes de la même manière que le site primaire;

iii) maintenir ou avoir un accès immédiat à un site opérationnel secondaire permettant au personnel d’assurer la continuité du service si le site opérationnel principal n’est pas disponible;

iv) évaluer la nécessité de mettre en place des sites de traitement supplémentaires, en particulier lorsque la diversité des profils de risque des sites primaire et secondaire ne permet pas de garantir avec suffisamment de certitude que les objectifs de continuité des activités de la contrepartie centrale seront atteints dans tous les cas de figure.

Aux fins du point a), les contreparties centrales finalisent les procédures et les paiements de fin de journée à l’heure et à la date requises, et cela en toutes circonstances.

Aux fins du point c) i), les dispositifs visés audit point garantissent la disponibilité de ressources humaines adéquates, une durée maximale d’indisponibilité des fonctions critiques ainsi qu’un transfert automatique et une reprise des activités sur un site secondaire.

Aux fins du point c) ii), le site secondaire de traitement visé audit point présente un profil de risque géographique distinct de celui du site primaire.

3. En plus de respecter les exigences prévues au paragraphe 1, les dépositaires centraux de titres veillent à ce que leur politique de continuité des activités de TIC:

(a) tienne compte des liens et interdépendances avec les utilisateurs, les prestataires de services et fournisseurs de services de réseau essentiels, les autres dépositaires centraux de titres et les autres infrastructures de marché;

(b) exige que ses dispositifs de continuité des activités de TIC garantissent que l'objectif en matière de délai de rétablissement des fonctions critiques ou importantes ne dépasse pas deux heures.

4. En plus de respecter les exigences prévues au paragraphe 1, les plates-formes de négociation veillent à ce que leur politique de continuité des activités de TIC garantisse:

(a) qu'après un incident perturbateur, la négociation peut reprendre dans les deux heures, ou dans un délai proche de deux heures;

(b) que la quantité maximale de données susceptibles d'être perdues par un service informatique de la plate-forme de négociation après un incident perturbateur est proche de zéro.

Article 25
Tests des plans de continuité des activités de TIC

1. Lorsqu'elles testent les plans de continuité des activités de TIC conformément à l'article 11, paragraphe 6, du règlement (UE) 2022/2554, les entités financières tiennent compte de l'analyse des incidences sur les activités de l'entité financière et de l'évaluation du risque lié aux TIC visée à l'article 3, premier alinéa, point b), du présent règlement.

2. Les entités financières évaluent, au moyen des tests de leurs plans de continuité des activités de TIC visés au paragraphe 1, si elles sont en mesure d'assurer la continuité de leurs fonctions critiques ou importantes. Ces tests:

(a) sont réalisés sur la base de scénarios de test simulant des perturbations potentielles, y compris un ensemble adéquat de scénarios graves mais plausibles;

(b) comprennent, le cas échéant, des tests des services TIC fournis par des prestataires tiers de services TIC;

(c) pour les entités financières, autres que les microentreprises, visées à l'article 11, paragraphe 6, deuxième alinéa, du règlement (UE) 2022/2554, comprennent des scénarios de basculement entre l'infrastructure de TIC principale et la capacité redondante, les sauvegardes et les installations redondantes;

(d) sont conçus pour éprouver les hypothèses sur lesquelles se fondent les plans de continuité des activités, y compris les dispositifs de gouvernance et les plans de communication en situation de crise;

(e) comportent des procédures visant à vérifier la capacité du personnel des entités financières, des prestataires tiers de services TIC, des systèmes de TIC et des services TIC à répondre de manière adéquate aux scénarios dûment pris en considération conformément à l'article 26, paragraphe 2.

Aux fins du point a), les entités financières incluent toujours dans les tests les scénarios envisagés pour l'élaboration des plans de continuité des activités.

Aux fins du point b), les entités financières tiennent dûment compte des scénarios liés à l'insolvabilité ou aux défaillances des prestataires tiers de services TIC ou aux risques politiques dans les juridictions des prestataires tiers de services TIC, le cas échéant.

Aux fins du point c), les tests permettent de vérifier si au moins les fonctions critiques ou importantes peuvent être exercées de manière appropriée pendant une durée suffisante et si le fonctionnement normal peut être rétabli.

3. En plus de respecter les exigences prévues au paragraphe 2, les contreparties centrales associent aux tests de leurs plans de continuité des activités de TIC visés au paragraphe 1:

(a) les membres compensateurs;

(b) les prestataires externes;

(c) les établissements de l'infrastructure financière avec lesquels les contreparties centrales ont constaté des interdépendances dans le cadre de leur politique de continuité des activités.

4. En plus de respecter les exigences prévues au paragraphe 2, les dépositaires centraux de titres associent, le cas échéant, aux tests de leurs plans de continuité des activités de TIC visés au paragraphe 1:

(a) les utilisateurs des dépositaires centraux de titres;

(b) les prestataires de services et fournisseurs de services de réseau essentiels;

(c) d'autres dépositaires centraux de titres;

(d) d'autres infrastructures de marché;

(e) d'autres établissements avec lesquels les dépositaires centraux de titres ont constaté des interdépendances dans le cadre de leur politique de continuité des activités.

5. Les entités financières documentent les résultats des tests visés au paragraphe 1. Toute défaillance constatée à la suite de ces tests est analysée, traitée et notifiée à l'organe de direction.

Article 26
Plans de réponse et de rétablissement des TIC

1. Lorsqu'elles élaborent les plans de réponse et de rétablissement des TIC visés à l'article 11, paragraphe 3, du règlement (UE) 2022/2554, les entités financières tiennent compte des résultats de l'analyse des incidences sur les activités de l'entité financière. Ces plans de réponse et de rétablissement des TIC:

(a) définissent les conditions qui déclenchent leur activation ou désactivation, ainsi que toute exception à cette activation ou désactivation;

(b) décrivent les mesures à prendre pour garantir la disponibilité, l'intégrité, la continuité et le rétablissement au moins des systèmes et services TIC qui soutiennent des fonctions critiques ou importantes de l'entité financière;

(c) sont conçus pour atteindre les objectifs de rétablissement des opérations des entités financières;

(d) sont documentés et mis à la disposition du personnel participant à l'exécution des plans de réponse et de rétablissement des TIC et sont facilement accessibles en cas d'urgence;

(e) prévoient des options de rétablissement à court et à long terme, y compris de rétablissement partiel des systèmes;

(f) définissent les objectifs des plans de réponse et de rétablissement des TIC et les conditions permettant de déclarer que ces plans ont été exécutés avec succès.

Aux fins du point d), les entités financières précisent clairement les rôles et responsabilités.

2. Les plans de réponse et de rétablissement des TIC visés au paragraphe 1 recensent les scénarios pertinents, y compris les scénarios de graves perturbations des activités et de probabilité accrue de survenance d'une perturbation. Ces plans établissent des scénarios fondés sur les informations actuelles sur les menaces et sur les enseignements tirés des perturbations des activités survenues antérieurement. Les entités financières tiennent dûment compte de tous les scénarios suivants:

(a) des cyberattaques et des basculements entre l'infrastructure de TIC principale et la capacité redondante, les sauvegardes et les installations redondantes;

(b) les scénarios dans lesquels la qualité de l'exécution d'une fonction critique ou importante se détériore à un niveau inacceptable, en prenant alors dûment en considération les incidences potentielles de l'insolvabilité ou d'autres défaillances de tout prestataire tiers de services TIC concerné;

(c) la défaillance partielle ou totale des locaux, notamment des locaux de bureau et des locaux commerciaux, et des centres de données;

(d) une défaillance substantielle des actifs de TIC ou de l'infrastructure de communication;

(e) l'indisponibilité d'un nombre critique de membres du personnel ou de personnes chargées de garantir la continuité des opérations;

(f) les incidences des événements liés au changement climatique et à la dégradation de l'environnement, des catastrophes naturelles, des pandémies et des attaques physiques, y compris des intrusions et des attentats terroristes;

(g) les attaques internes;

(h) l'instabilité politique et sociale, y compris, le cas échéant, dans la juridiction du prestataire tiers de services TIC et à l'endroit où les données sont stockées et traitées;

(i) les coupures de courant à une grande échelle.

3. Lorsque les mesures de rétablissement primaires sont susceptibles de ne pas être réalisables à court terme en raison des coûts, des risques, de problèmes logistiques ou de circonstances imprévues, les plans de réponse et de rétablissement des TIC visés au paragraphe 1 envisagent d'autres options.

4. Dans le cadre des plans de réponse et de rétablissement des TIC visés au paragraphe 1, les entités financières étudient et mettent en œuvre des mesures de continuité pour atténuer les conséquences des défaillances des prestataires tiers de services TIC qui fournissent des services TIC à l'appui de fonctions critiques ou importantes de l'entité financière.

CHAPITRE V
RAPPORT SUR LE RÉEXAMEN DU CADRE DE GESTION DU RISQUE LIÉ AUX TIC

Article 27

Format et contenu du rapport sur le réexamen du cadre de gestion du risque lié aux TIC

1. Les entités financières présentent le rapport sur le réexamen du cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 5, du règlement (UE) 2022/2554 dans un format électronique interrogeable.

2. Les entités financières incluent l'ensemble des informations suivantes dans le rapport visé au paragraphe 1:

   (a) une partie introductive qui:

      i) identifie clairement l'entité financière faisant l'objet du rapport et décrit sa structure de groupe, le cas échéant;

      ii) décrit le contexte du rapport en ce qui concerne la nature, l'échelle et la complexité des services, activités et opérations de l'entité financière, son organisation, ses fonctions critiques recensées, sa stratégie, ses grands projets ou activités en cours, ses relations et sa dépendance à l'égard de services et systèmes de TIC internes ou sous-traités, ou les conséquences qu'une perte totale ou une dégradation grave de ces systèmes engendrerait en ce qui concerne les fonctions critiques ou importantes et l'efficience du marché;

      iii) résume les changements majeurs dont le cadre de gestion du risque lié aux TIC a fait l'objet depuis le rapport précédent;

      iv) présente une synthèse du profil de risque lié aux TIC actuel et à court terme, due l'éventail des menaces, de l'évaluation de l'efficacité de ses contrôles et de la posture de sécurité de l'entité financière;

   (b) la date d'approbation du rapport par l'organe de direction de l'entité financière;

   (c) une description de la raison du réexamen du cadre de gestion du risque lié aux TIC engagé conformément à l'article 6, paragraphe 5, du règlement (UE) 2022/2554;

   (d) les dates de début et de fin de la période examinée;

   (e) l'indication de la fonction responsable du réexamen;

   (f) une description des principales modifications et améliorations dont le cadre de gestion du risque lié aux TIC a fait l'objet depuis le réexamen précédent;

   (g) un résumé des conclusions du réexamen ainsi qu'une analyse et une évaluation détaillées de la gravité des faiblesses, des défaillances et des lacunes du cadre de gestion du risque lié aux TIC au cours de la période examinée;

   (h) une description des mesures prises face aux faiblesses, défaillances et lacunes constatées, comprenant l'ensemble des éléments suivants:

      i) un résumé des mesures prises pour remédier aux faiblesses, défaillances et lacunes constatées;

ii) une date prévue pour la mise en œuvre des mesures et des dates relatives au contrôle interne de la mise en œuvre, y compris des informations sur l'état d'avancement de la mise en œuvre de ces mesures à la date de rédaction du rapport, en expliquant, le cas échéant, s'il existe un risque que les délais ne soient pas respectés;

iii) les outils à utiliser et l'identification de la fonction responsable de l'exécution des mesures, en précisant si les outils et les fonctions sont internes ou externes;

iv) une description de l'incidence des modifications envisagées dans les mesures sur les ressources budgétaires, humaines et matérielles de l'entité financière, y compris sur les ressources consacrées à la mise en œuvre de toute mesure corrective;

v) des informations sur le processus d'information de l'autorité compétente, le cas échéant;

vi) lorsque les faiblesses, défaillances ou lacunes recensées ne font pas l'objet de mesures correctives, une explication détaillée des critères appliqués pour analyser leur incidence et évaluer le risque résiduel lié aux TIC qui leur est associé, ainsi que des critères appliqués pour accepter ce risque résiduel;

(i) des informations sur les nouvelles évolutions prévues du cadre de gestion du risque lié aux TIC;

(j) les conclusions résultant du réexamen du cadre de gestion du risque lié aux TIC;

(k) des informations sur les réexamens antérieurs, comprenant:

i) une liste des réexamens antérieurs;

ii) le cas échéant, un état d'avancement de la mise en œuvre des mesures correctives déterminées dans le dernier rapport;

iii) lorsque les mesures correctives proposées lors des réexamens précédents se sont révélées inefficaces ou ont créé des difficultés inattendues, une description de la manière dont ces mesures correctives pourraient être améliorées ou de ces difficultés imprévues;

(l) les sources d'information utilisées pour l'élaboration du rapport, y compris l'ensemble des éléments suivants:

i) pour les entités financières, autres que les microentreprises, visées à l'article 6, paragraphe 6, du règlement (UE) 2022/2554, les résultats des audits internes;

ii) les résultats des évaluations de la conformité;

iii) les résultats des tests de résilience opérationnelle numérique et, le cas échéant, les résultats des tests avancés des outils de TIC, des systèmes de TIC et des processus de TIC sur la base de tests de pénétration fondés sur la menace;

iv) les sources externes.

Aux fins du point c), lorsque le réexamen a été engagé à la suite d'instructions des autorités de surveillance ou à la suite des conclusions tirées des tests de résilience

opérationnelle numérique ou des processus d'audit pertinents, le rapport contient des références explicites à ces instructions ou conclusions, permettant d'identifier la raison du réexamen. Lorsque le réexamen a été engagé à la suite d'incidents liés aux TIC, le rapport contient la liste de tous les incidents liés aux TIC accompagnée d'une analyse de la cause originelle des incidents.

Aux fins du point f), la description contient une analyse de l'incidence des modifications sur la stratégie de résilience opérationnelle numérique de l'entité financière, sur le cadre de contrôle interne des TIC de l'entité financière et sur la gouvernance de la gestion du risque lié aux TIC de l'entité financière.

TITRE III — CADRE SIMPLIFIÉ DE GESTION DU RISQUE LIÉ AUX TIC POUR LES ENTITÉS FINANCIÈRES VISÉES À L'ARTICLE 16, PARAGRAPHE 1, DU RÈGLEMENT (UE) 2022/2554

CHAPITRE I
CADRE SIMPLIFIÉ DE GESTION DU RISQUE LIÉ AUX TIC

Article 28
Gouvernance et organisation

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 disposent d'un cadre de gouvernance et de contrôle interne qui garantit une gestion efficace et prudente du risque lié aux TIC, en vue d'atteindre un niveau élevé de résilience opérationnelle numérique.

2. Les entités financières visées au paragraphe 1 veillent, au titre de leur cadre simplifié de gestion du risque lié aux TIC, à ce que leur organe de direction:

   (a) assume la responsabilité globale de veiller à ce que le cadre simplifié de gestion du risque lié aux TIC permette de réaliser la stratégie d'entreprise de l'entité financière conformément à l'appétit pour le risque de cette entité financière, et veille à ce que le risque lié aux TIC soit pris en considération dans ce contexte;

   (b) définisse clairement les rôles et les responsabilités pour toutes les tâches relatives aux TIC;

   (c) définisse les objectifs en matière de sécurité de l'information et les exigences en matière de TIC;

   (d) approuve, supervise et réexamine périodiquement:

      i) la classification des actifs informationnels de l'entité financière visée à l'article 30, paragraphe 1, du présent règlement, la liste des principaux risques identifiés et l'analyse des incidences sur les activités ainsi que les politiques connexes;

      ii) les plans de continuité des activités de l'entité financière ainsi que les mesures de réponse et de rétablissement visés à l'article 16, paragraphe 1, point f), du règlement (UE) 2022/2554;

   (e) alloue et réexamine au moins une fois par an le budget nécessaire pour satisfaire les besoins de l'entité financière en matière de résilience opérationnelle numérique pour tous les types de ressources, y compris les programmes pertinents de sensibilisation à la sécurité des TIC et les formations pertinentes à la résilience opérationnelle numérique et les compétences en matière de TIC pour l'ensemble du personnel;

   (f) précise et met en œuvre les politiques et mesures prévues aux chapitres I, II et III du présent titre permettant d'identifier, d'évaluer et de gérer le risque lié aux TIC auquel l'entité financière est exposée;

(g) définit et met en œuvre les procédures, les protocoles TIC et les outils nécessaires à la protection de tous les actifs informationnels et de TIC;

(h) veille au maintien à jour d'un niveau suffisant de connaissances et de compétences du personnel de l'entité financière permettant à ce dernier de comprendre et d'évaluer le risque lié aux TIC et son incidence sur les opérations de l'entité financière, de façon proportionnée au risque lié aux TIC géré;

(i) établit des modalités d'établissement de rapports, y compris la fréquence, la forme et le contenu des rapports à l'organe de direction sur la sécurité de l'information et la résilience opérationnelle numérique.

3. Les entités financières visées au paragraphe 1 peuvent, conformément au droit de l'Union et au droit sectoriel national, externaliser les tâches de vérification du respect des exigences en matière de gestion du risque lié aux TIC à des prestataires de services TIC intra-groupe ou à des prestataires tiers de services TIC. Dans le cas d'une telle externalisation, les entités financières demeurent pleinement responsables de la vérification du respect des exigences en matière de gestion du risque lié aux TIC.

4. Les entités financières visées au paragraphe 1 garantissent une séparation et une indépendance adéquates des fonctions de contrôle et des fonctions d'audit interne.

5. Les entités financières visées au paragraphe 1 veillent à ce que leur cadre simplifié de gestion du risque lié aux TIC fasse l'objet d'un audit interne réalisé par des auditeurs conformément au plan d'audit de ces entités financières. Ces auditeurs disposent de connaissances, de compétences et d'une expertise suffisantes en matière de risque lié aux TIC, et sont indépendants. La fréquence et l'objectif des audits des TIC sont proportionnés au risque lié aux TIC de l'entité financière.

6. Sur la base des résultats de l'audit visé au paragraphe 5, les entités financières visées au paragraphe 1 veillent à la vérification et à la correction en temps utile des constatations d'importance critique de l'audit des TIC.

Article 29

Politique et mesures en matière de sécurité de l'information

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 élaborent, documentent et mettent en œuvre une politique de sécurité de l'information dans le contexte du cadre simplifié de gestion du risque lié aux TIC. Cette politique de sécurité de l'information précise les principes et règles généraux visant à protéger la confidentialité, l'intégrité, la disponibilité et l'authenticité des données et des services fournis par ces entités financières.

2. Sur la base de leur politique en matière de sécurité de l'information visée au paragraphe 1, les entités financières visées au paragraphe 1 établissent et mettent en œuvre des mesures de sécurité des TIC pour atténuer leur exposition au risque lié aux TIC, y compris des mesures d'atténuation mises en œuvre par des prestataires tiers de services TIC.

Les mesures de sécurité des TIC comprennent toutes les mesures visées aux articles 30 à 38.

Article 30
Classification des actifs informationnels et des actifs de TIC

1. Au titre du cadre simplifié de gestion du risque lié aux TIC visé à l'article 16, paragraphe 1, point a), du règlement (UE) 2022/2554, les entités financières visées au paragraphe 1 dudit article identifient, classent et documentent toutes les fonctions critiques ou importantes, les actifs informationnels et les actifs de TIC qui les soutiennent ainsi que leurs interdépendances. Les entités financières réexaminent cette identification et cette classification en tant que de besoin.

2. Les entités financières visées au paragraphe 1 identifient toutes les fonctions critiques ou importantes soutenues par des prestataires tiers de services TIC.

Article 31
Gestion du risque lié aux TIC

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 incluent dans leur cadre simplifié de gestion du risque lié aux TIC l'ensemble des éléments suivants:

   (a) une détermination des niveaux de tolérance au risque lié aux TIC, en fonction de l'appétit pour le risque de l'entité financière;

   (b) l'identification et l'évaluation des risques liés aux TIC auxquels l'entité financière est exposée;

   (c) la définition de stratégies d'atténuation, au moins pour les risques liés aux TIC qui dépassent les niveaux de tolérance au risque de l'entité financière;

   (d) le suivi de l'efficacité des stratégies d'atténuation visées au point c);

   (e) l'identification et l'évaluation de tout risque lié aux TIC ou en matière de sécurité de l'information résultant de tout changement majeur dans les systèmes de TIC ou les services TIC, les processus ou les procédures, ou révélé par les résultats des tests de sécurité des TIC ou après tout incident majeur lié aux TIC.

2. Les entités financières visées au paragraphe 1 effectuent et documentent périodiquement l'évaluation du risque lié aux TIC, de façon proportionnée à leur profil de risque lié aux TIC.

3. Les entités financières visées au paragraphe 1 surveillent en permanence les menaces et les vulnérabilités qui concernent leurs fonctions critiques ou importantes, ainsi que les actifs informationnels et les actifs de TIC, et réexaminent régulièrement les scénarios de risque ayant une incidence sur ces fonctions critiques ou importantes.

4. Les entités financières visées au paragraphe 1 définissent des seuils d'alerte et des critères de déclenchement et de lancement des processus de réponse en cas d'incident lié aux TIC.

Article 32
Sécurité physique et environnementale

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 définissent et mettent en œuvre des mesures de sécurité physique conçues sur la base de l'éventail des menaces et conformément à la classification visée à

l'article 30, paragraphe 1, du présent règlement, au profil de risque global des actifs de TIC et aux actifs informationnels accessibles.

2. Les mesures visées au paragraphe 1 protègent les locaux des entités financières et, le cas échéant, les centres de données des entités financières dans lesquels les actifs de TIC et les actifs informationnels sont situés contre les accès non autorisés, les attaques et les accidents, ainsi que contre les menaces et dangers environnementaux.

3. La protection contre les menaces et dangers environnementaux est proportionnée à l'importance des locaux concernés et, le cas échéant, des centres de données et à la criticité des opérations ou des systèmes de TIC qui y sont situés.

CHAPITRE II
AUTRES ÉLÉMENTS DES SYSTÈMES, PROTOCOLES ET OUTILS VISANT À RÉDUIRE AU MINIMUM L'INCIDENCE DU RISQUE LIÉ AUX TIC

Article 33
Contrôle d'accès

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 élaborent, documentent et mettent en œuvre des procédures de contrôle des accès logiques et physiques, et appliquent, contrôlent et réexaminent périodiquement ces procédures. Ces procédures comportent les éléments suivants de contrôle des accès logiques et physiques:

   (a) les droits d'accès aux actifs informationnels, aux actifs de TIC et aux fonctions que ces actifs soutiennent, ainsi qu'aux sites critiques d'exploitation de l'entité financière, sont gérés selon les principes du besoin d'en connaître, du besoin d'en disposer et du droit d'accès minimal, y compris pour l'accès à distance et l'accès d'urgence;

   (b) la responsabilité des utilisateurs, qui garantit que les utilisateurs peuvent être identifiés pour les actions effectuées dans les systèmes de TIC;

   (c) les procédures de gestion des comptes permettant d'accorder, de modifier ou de révoquer des droits d'accès pour les comptes d'utilisateurs et les comptes génériques, y compris les comptes génériques d'administrateur;

   (d) des méthodes d'authentification proportionnées à la classification visée à l'article 30, paragraphe 1, et au profil de risque global des actifs de TIC, et reposant sur les pratiques de pointe;

   (e) les droits d'accès sont réexaminés périodiquement et retirés lorsqu'ils ne sont plus nécessaires.

   Aux fins du point c), l'entité financière attribue des accès privilégiés, d'urgence et d'administrateur uniquement sur la base du besoin d'en disposer ou au cas par cas pour tous les systèmes de TIC. Ces accès sont journalisés conformément à l'article 34, paragraphe 1, point f).

   Aux fins du point d), les entités financières utilisent des méthodes d'authentification forte reposant sur les pratiques de pointe pour l'accès à distance à leurs réseaux, pour tout accès privilégié et pour l'accès aux actifs de TIC soutenant des fonctions critiques ou importantes qui sont accessibles au public.

Article 34
Sécurité des opérations de TIC

Dans le cadre de leurs systèmes, protocoles et outils, et pour tous les actifs de TIC, les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554:

(a) suivent et gèrent le cycle de vie de tous les actifs de TIC;

(b) surveillent si les actifs de TIC sont pris en charge par des prestataires tiers de services TIC des entités financières, le cas échéant;

(c) définissent les besoins en capacités de leurs actifs de TIC et les mesures visant à maintenir et à améliorer la disponibilité et l'efficacité des systèmes de TIC et à prévenir les déficits de capacités en matière de TIC avant qu'ils ne se concrétisent;

(d) effectuent des scans et évaluations automatisés des vulnérabilités des actifs de TIC de façon proportionnée à leur classification visée à l'article 30, paragraphe 1, et au profil de risque global de l'actif de TIC, et déploient des correctifs pour remédier aux vulnérabilités identifiées;

(e) gèrent les risques liés aux actifs de TIC obsolètes, non pris en charge ou hérités;

(f) journalisent les événements liés au contrôle des accès logiques et physiques, aux opérations de TIC, y compris aux activités liées aux systèmes et au trafic réseau, et à la gestion des changements dans les TIC;

(g) définissent et mettent en œuvre des mesures de suivi et d'analyse des informations sur les activités et comportements anormaux pour les opérations de TIC critiques ou importantes;

(h) mettent en œuvre des mesures de suivi des informations pertinentes et actualisées sur les cybermenaces;

(i) mettent en œuvre des mesures visant à détecter les éventuelles fuites d'informations, les codes malveillants et les autres menaces pour la sécurité, ainsi que les vulnérabilités de notoriété publique dans les logiciels et le matériel, et vérifient la disponibilité de nouvelles mises à jour de sécurité correspondantes.

Aux fins du point f), les entités financières adaptent le niveau de détail des journaux en fonction de leur finalité et de leur utilisation des actifs de TIC produisant ces journaux.

Article 35
Sécurité des données, des systèmes et des réseaux

Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 élaborent et mettent en œuvre, dans le cadre de leurs systèmes, protocoles et outils, des garanties pour assurer la protection des réseaux contre les intrusions et les utilisations abusives des données et préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données. En particulier, les entités financières mettent en place, en tenant compte de la classification visée à l'article 30, paragraphe 1, du présent règlement, l'ensemble des éléments suivants:

(a) la définition et la mise en œuvre de mesures visant à protéger les données en cours d'utilisation, en transit et au repos;

(b) la définition et la mise en œuvre de mesures de sécurité concernant l'utilisation de logiciels, de supports de stockage de données, de systèmes et de périphériques de point de terminaison qui transfèrent et stockent des données de l'entité financière;

(c) la définition et la mise en œuvre de mesures visant à prévenir et à détecter les connexions non autorisées au réseau de l'entité financière et à sécuriser le trafic réseau entre les réseaux internes de l'entité financière et l'internet et d'autres connexions externes;

(d) la définition et la mise en œuvre de mesures garantissant la disponibilité, l'authenticité, l'intégrité et la confidentialité des données lors des transmissions sur le réseau;

(e) un processus permettant de supprimer de manière sécurisée les données dans les locaux, ou stockées à l'extérieur, que l'entité financière n'a plus besoin de collecter ou de stocker;

(f) un processus permettant d'éliminer ou de déclasser de manière sécurisée des dispositifs de stockage de données dans les locaux, ou des dispositifs de stockage des données stockés à l'extérieur, qui contiennent des informations confidentielles;

(g) la définition et la mise en œuvre de mesures visant à garantir que le télétravail et l'utilisation de périphériques de point de terminaison privés n'ont pas d'incidence négative sur la capacité de l'entité financière à mener ses activités critiques de manière adéquate, rapide et sûre.

Article 36
Tests de sécurité des TIC

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 établissent et mettent en œuvre un plan de tests de sécurité des TIC afin de confirmer l'efficacité de leurs mesures de sécurité des TIC élaborées conformément aux articles 33, 34 et 35 et aux articles 37 et 38 du présent règlement. Les entités financières veillent à ce que ce plan tienne compte des menaces et des vulnérabilités identifiées au titre du cadre simplifié de gestion du risque lié aux TIC visé à l'article 31 du présent règlement.

2. Les entités financières visées au paragraphe 1 examinent, évaluent et testent les mesures de sécurité des TIC, en tenant compte du profil de risque global des actifs de TIC de l'entité financière.

3. Les entités financières visées au paragraphe 1 suivent et évaluent les résultats des tests de sécurité et mettent à jour leurs mesures de sécurité en conséquence, sans retard injustifié, lorsque les systèmes de TIC concernés soutiennent des fonctions critiques ou importantes.

Article 37
Acquisition, développement et maintenance des systèmes de TIC

Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 conçoivent et mettent en œuvre, le cas échéant, une procédure régissant l'acquisition, le développement et la maintenance de systèmes de TIC selon une approche fondée sur les risques. Cette procédure:

(a) prévoit que, avant toute acquisition ou tout développement de systèmes de TIC, les exigences fonctionnelles et non fonctionnelles, y compris les exigences en matière de sécurité de l'information, sont clairement définies et approuvées par la fonction «métier» concernée;

(b) prévoit que les systèmes de TIC sont testés et approuvés avant leur première utilisation et avant l'introduction de changements dans l'environnement de production;

(c) définit les mesures visant à atténuer le risque d'altération involontaire ou de manipulation intentionnelle des systèmes de TIC lors du développement et de la mise en œuvre dans l'environnement de production.

Article 38
Gestion des projets de TIC et des changements dans les TIC

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 élaborent, documentent et mettent en œuvre une procédure de gestion des projets de TIC et précisent les rôles et responsabilités liés à sa mise en œuvre. Cette procédure couvre tous les stades des projets de TIC, depuis leur lancement jusqu'à leur clôture.

2. Les entités financières visées au paragraphe 1 élaborent, documentent et mettent en œuvre une procédure de gestion des changements dans les TIC, afin de garantir que tous les changements apportés aux systèmes de TIC sont consignés, testés, évalués, approuvés, mis en œuvre et vérifiés de manière contrôlée et avec les garanties adéquates pour préserver la résilience opérationnelle numérique de l'entité financière.

Chapitre III
GESTION DE LA CONTINUITÉ DES ACTIVITÉS DE TIC

Article 39
Composantes du plan de continuité des activités de TIC

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 élaborent leurs plans de continuité des activités de TIC en prenant en considération les résultats de l'analyse de leurs expositions aux graves perturbations des activités et de leurs incidences potentielles, ainsi que les scénarios auxquels leurs actifs de TIC qui soutiennent des fonctions critiques ou importantes pourraient être exposés, y compris un scénario de cyberattaque.

2. Les plans de continuité des activités de TIC visés au paragraphe 1:

   (a) sont approuvés par l'organe de direction de l'entité financière;

   (b) sont documentés et facilement accessibles en cas d'urgence ou de crise;

   (c) affectent des ressources suffisantes à leur exécution;

   (d) établissent les niveaux de rétablissement et les délais prévus pour le rétablissement et la reprise des fonctions et des principales relations de dépendance internes et externes, y compris les prestataires tiers de services TIC;

   (e) définissent les conditions susceptibles de déclencher l'activation des plans de continuité des activités de TIC et les mesures à prendre pour garantir la disponibilité, la continuité et le rétablissement des actifs de TIC des entités financières qui soutiennent des fonctions critiques ou importantes;

(f) définissent les mesures de restauration et de rétablissement pour les fonctions «métiers» critiques ou importantes, les processus de soutien, les actifs informationnels et leurs interdépendances afin d'éviter des effets préjudiciables sur le fonctionnement des entités financières;

(g) définissent des procédures et mesures de sauvegarde qui précisent l'étendue des données concernées par la sauvegarde ainsi que la fréquence minimale de celle-ci, selon la criticité de la fonction qui utilise ces données;

(h) prévoient d'autres options pour le cas où le rétablissement ne serait pas réalisable à court terme en raison des coûts, des risques, de problèmes logistiques ou de circonstances imprévues;

(i) précisent les modalités de communication interne et externe, y compris les plans de remontée des informations;

(j) sont actualisés en fonction des enseignements tirés des incidents, des tests, des nouveaux risques et des menaces identifiés, des changements des objectifs de rétablissement, des changements majeurs apportés à l'organisation de l'entité financière et aux actifs de TIC qui soutiennent des fonctions critiques ou des fonctions «métiers».

Aux fins du point f), les mesures visées audit point prévoient l'atténuation des défaillances des prestataires tiers critiques.

Article 40
Tests des plans de continuité des activités

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 testent leurs plans de continuité des activités visés à l'article 39 du présent règlement, y compris les scénarios visés audit article, au moins une fois par an pour les procédures de sauvegarde et de restauration, ou à chaque modification majeure du plan de continuité des activités.

2. Les tests des plans de continuité des activités visés au paragraphe 1 doivent démontrer que les entités financières visées audit paragraphe sont en mesure de maintenir la viabilité de leurs activités jusqu'à ce que les opérations critiques soient rétablies et détecter toute lacune de ces plans.

3. Les entités financières visées au paragraphe 1 documentent les résultats des tests des plans de continuité des activités et toute lacune constatée à la suite de ces tests est analysée, traitée et notifiée à l'organe de direction.

CHAPITRE IV
RAPPORT SUR LE RÉEXAMEN DU CADRE SIMPLIFIÉ DE GESTION DU RISQUE LIÉ AUX TIC

Article 41
Format et contenu du rapport sur le réexamen du cadre simplifié de gestion du risque lié aux TIC

1. Les entités financières visées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554 présentent le rapport sur le réexamen du cadre de gestion du risque lié aux TIC visé au paragraphe 2 dudit article dans un format électronique interrogeable.

2. Le rapport visé au paragraphe 1 contient l'ensemble des informations suivantes:

(a) une partie introductive contenant:

i) une description du contexte du rapport en ce qui concerne la nature, l'échelle et la complexité des services, activités et opérations de l'entité financière, son organisation, ses fonctions critiques recensées, sa stratégie, ses grands projets ou activités en cours, ses relations et sa dépendance à l'égard des services et systèmes de TIC internes ou sous-traités, ou les conséquences qu'une perte totale ou une dégradation grave de ces systèmes engendrerait en ce qui concerne les fonctions critiques ou importantes et l'efficience du marché;

ii) une synthèse du risque lié aux TIC actuel et à court terme qui a été identifié, de l'éventail des menaces, de l'évaluation de l'efficacité de ses contrôles et de la posture de sécurité de l'entité financière;

iii) des informations sur le domaine faisant l'objet du rapport;

iv) un résumé des changements majeurs dont le cadre de gestion du risque lié aux TIC a fait l'objet depuis le rapport précédent;

v) un résumé et une description de l'incidence des changements dont le cadre simplifié de gestion du risque lié aux TIC a fait l'objet depuis le rapport précédent;

(b) le cas échéant, la date d'approbation du rapport par l'organe de direction de l'entité financière;

(c) une description des raisons du réexamen, notamment:

i) lorsque le réexamen a été engagé à la suite d'instructions des autorités de surveillance, la preuve de ces instructions;

ii) lorsque le réexamen a été engagé à la suite d'incidents liés aux TIC, la liste de ces incidents accompagnée d'une analyse de leur cause originelle;

(d) les dates de début et de fin de la période examinée;

(e) la personne responsable du réexamen;

(f) un résumé des constatations et une autoévaluation, comprenant une analyse détaillée, de la gravité des faiblesses, des défaillances et des lacunes identifiées du cadre de gestion du risque lié aux TIC pour la période examinée;

(g) les mesures définies pour remédier aux faiblesses, aux défaillances et aux lacunes du cadre simplifié de gestion du risque lié aux TIC, ainsi que la date prévue pour la mise en œuvre de ces mesures, y compris les suites données aux faiblesses, défaillances et lacunes identifiées dans les rapports précédents, lorsqu'il n'y a pas encore été remédié;

(h) les conclusions générales du réexamen du cadre simplifié de gestion du risque lié aux TIC, y compris les nouvelles évolutions prévues.

TITRE IV — DISPOSITIONS FINALES

Article 42
Entrée en vigueur

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

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tous les États membres.

Fait à Bruxelles, le 13.3.2024

Par la Commission
La présidente
Ursula VON DER LEYEN