COM(2020) 595 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2020/2021

Reçu à la Présidence de l'Assemblée nationale
le 18 décembre 2020

Enregistré à la Présidence du Sénat
le 18 décembre 2020

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Proposition de règlement du parlement européen et du conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014

E 15409

COMMISSION
EUROPÉENNE

Bruxelles, le 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014

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

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

- Motivation et objectifs de la proposition

La présente proposition fait partie du train de mesures sur la finance numérique, lequel vise à libérer et à renforcer encore davantage le potentiel que la finance numérique peut offrir sur le plan de l'innovation et de la compétitivité, tout en limitant les risques qui en découlent. Elle est conforme aux priorités de la Commission consistant à adapter l'Europe à l'ère du numérique et à bâtir une économie parée pour l'avenir et au service des citoyens. Le train de mesures sur la finance numérique prévoit une nouvelle stratégie en matière de finance numérique pour le secteur financier de l'UE[1] afin que celle-ci embrasse la révolution numérique et en devienne le fer de lance avec l'aide de sociétés européennes innovantes, de manière à faire profiter les entreprises et les consommateurs des avantages de la finance numérique. Outre la présente proposition, le train de mesures comprend également une proposition de règlement sur les marchés de crypto-actifs[2], une proposition de règlement sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués (DLT)[3] et une proposition de directive visant à clarifier ou à modifier certaines dispositions connexes de l'Union sur les services financiers[4]. La numérisation et la résilience opérationnelle du secteur financier sont les deux faces d'une même médaille. Le numérique, ou les technologies de l'information et de la communication (TIC), sont sources à la fois d'opportunités et de risques. Ceux-ci doivent être bien compris et gérés, surtout en période de tensions.

Les décideurs politiques et les autorités de surveillance ont dès lors prêté une attention croissante aux risques découlant de la dépendance aux TIC. Ils ont notamment tenté de renforcer la résilience des entreprises en définissant des normes et en coordonnant les travaux de réglementation ou de surveillance. Ces travaux ont été menés au niveau tant international qu'européen, et aussi bien de manière intersectorielle que pour un certain nombre de secteurs spécifiques, dont les services financiers.

Les risques informatiques continuent néanmoins de menacer la résilience opérationnelle, les performances et la stabilité du système financier de l'UE. La réforme qui a suivi la crise financière de 2008 a principalement renforcé la résilience financière[5] du secteur financier de l'UE, ne s'attaquant qu'indirectement aux risques informatiques dans certains domaines, dans le cadre des mesures visant à remédier plus largement aux risques opérationnels.

Si les modifications apportées après la crise à la législation de l'UE sur les services financiers ont mis en place un corpus réglementaire unique régissant une grande partie des risques

---

1 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur une stratégie en matière de finance numérique pour l'UE du 23 septembre 2020, COM(2020) 591.

2 Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937, COM(2020) 593.

3 Proposition de règlement du Parlement européen et du Conseil sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, COM(2020) 594.

4 Proposition de directive du Parlement européen et du Conseil modifiant les directives 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341, COM(2020) 596.

5 Les différentes mesures adoptées visaient fondamentalement à augmenter la dotation en fonds propres et la liquidité des entités financières, ainsi qu'à réduire les risques de marché et de crédit.

financiers liés aux services financiers, elles n'ont pas traité pleinement la question de la résilience opérationnelle numérique. Les mesures prises à cet égard présentaient un certain nombre de caractéristiques qui en limitaient l'efficacité. Par exemple, elles ont souvent pris la forme de directives d'harmonisation minimale ou de règlements fondés sur des principes, laissant ainsi une place importante à l'adoption d'approches divergentes au sein du marché unique. En outre, les risques informatiques n'ont fait l'objet que d'une attention limitée ou incomplète dans le cadre de la couverture des risques opérationnels. Enfin, ces mesures varient d'une législation sectorielle sur les services financiers à l'autre. Ainsi, l'intervention au niveau de l'Union n'a pas pleinement répondu aux besoins qu'ont les entités financières européennes de gérer les risques opérationnels d'une manière qui leur permette de résister aux conséquences des incidents informatiques, d'y répondre et de s'en remettre. Elle n'a pas non plus fourni aux autorités de surveillance financière les outils les plus appropriés pour s'acquitter de leur mandat consistant à prévenir l'instabilité financière découlant de la matérialisation de ces risques informatiques.

L'absence de règles détaillées et exhaustives sur la résilience opérationnelle numérique au niveau de l'UE a favorisé la prolifération d'initiatives réglementaires (par exemple, sur les tests en matière de résilience opérationnelle numérique) et de pratiques de surveillance (par exemple, en ce qui concerne la dépendance à l'égard de tiers prestataires de services informatiques) au niveau national. L'action au niveau des États membres n'a cependant qu'un effet limité étant donné la nature transfrontière des risques informatiques. En outre, le manque de coordination entre les initiatives nationales a donné lieu à des chevauchements, des incohérences, des exigences redondantes, des coûts administratifs et de mise en conformité élevés – en particulier pour les entités financières transfrontières – ou a laissé des risques informatiques non détectés et, partant, non traités. Cette situation fragmente le marché unique, compromet la stabilité et l'intégrité du secteur financier de l'UE et porte atteinte à la protection des consommateurs et des investisseurs.

Il est par conséquent nécessaire de mettre en place un cadre détaillé et exhaustif sur la résilience opérationnelle numérique pour les entités financières de l'UE. Ce cadre renforcera la dimension numérique de la gestion des risques dans le corpus réglementaire unique. En particulier, il améliorera et rationalisera la gestion des risques informatiques par les entités financières, instaurera une procédure de test approfondi des systèmes informatiques, sensibilisera davantage les autorités de surveillance aux cyberrisques et aux incidents liés à l'informatique auxquels sont confrontées les entités financières, et conférera aux autorités de surveillance financière des pouvoirs leur permettant de superviser les risques découlant de la dépendance des entités financières à l'égard de tiers prestataires de services informatiques. La proposition prévoit d'établir un mécanisme cohérent de notification des incidents, qui contribuera à réduire les charges administratives des entités financières et à renforcer l'efficacité de la surveillance.

- Cohérence avec les dispositions en vigueur dans le domaine d'action

La présente proposition s'inscrit dans le cadre des travaux plus vastes actuellement menés aux niveaux européen et international pour renforcer la cybersécurité dans les services financiers et s'attaquer aux risques opérationnels au sens large[6].

Elle donne également suite à l'avis technique conjoint[7] des autorités européennes de surveillance (AES) de 2019, qui préconisait une approche plus cohérente pour traiter le risque

[6] Comité de Bâle sur le contrôle bancaire, *Cyber-resilience: Range of practices*, décembre 2018 et *Principles for sound management of operational risk (PSMOR)*, octobre 2014.

informatique dans le secteur financier et recommandait à la Commission de renforcer, de manière proportionnée, la résilience opérationnelle numérique du secteur des services financiers par une initiative sectorielle au niveau de l'UE. L'avis des AES était une réponse au plan d'action pour les technologies financières présenté en 2018 par la Commission[8].

- Cohérence avec les autres politiques de l'Union

Ainsi que l'a déclaré la présidente von der Leyen dans ses orientations politiques[9], et comme cela est expliqué dans la communication intitulée «Façonner l'avenir numérique de l'Europe»[10], il est essentiel que l'Europe tire parti de tous les avantages de l'ère numérique et renforce son industrie et sa capacité d'innovation, au sein d'un cadre garant de la sécurité et de l'éthique. La stratégie européenne pour les données[11] définit quatre piliers – la protection des données, les droits fondamentaux, la sûreté et la cybersécurité – comme des conditions préalables essentielles pour une société à laquelle les données confèrent les moyens dont elle a besoin. Plus récemment, le Parlement européen s'est attelé à l'élaboration d'un rapport sur la finance numérique, qui plaide notamment en faveur d'une stratégie commune en matière de cyber-résilience du secteur financier[12]. Un cadre législatif renforçant la résilience opérationnelle numérique des entités financières de l'Union est conforme à ces objectifs stratégiques. La proposition viendrait également appuyer les politiques en faveur de la reprise à la suite du coronavirus, car elle garantirait que la dépendance accrue à l'égard du financement numérique va de pair avec la résilience opérationnelle.

L'initiative préserverait les avantages liés au cadre horizontal sur la cybersécurité (par exemple, la directive sur la sécurité des réseaux et des systèmes d'information, ou directive SRI) en maintenant le secteur financier dans son champ d'application. Le secteur financier demeurerait étroitement associé au groupe de coopération SRI, et les autorités de surveillance financière seraient en mesure d'échanger des informations utiles au sein de l'écosystème SRI existant. L'initiative serait cohérente avec la directive sur les infrastructures critiques européennes (ICE), qui fait actuellement l'objet d'un réexamen afin de renforcer la protection et la résilience des infrastructures critiques contre les menaces non liées à la cybercriminalité. Enfin, cette proposition s'inscrit dans le droit fil de la stratégie pour l'union de la sécurité[13] qui préconisait une initiative sur la résilience opérationnelle numérique pour le

---

7 Avis conjoint des autorités européennes de surveillance à la Commission européenne sur la nécessité d'améliorer la législation relative aux exigences en matière de gestion des risques informatiques dans le secteur financier de l'Union [Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements in the European Union (EU) financial sector], JC 2019 26 (2019).

8 Commission européenne, *Plan d'action pour les technologies financières*, COM(2018) 109 final.

9 Présidente Ursula von der Leyen, Orientations politiques pour la prochaine Commission européenne, 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_fr.pdf.

10 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Façonner l'avenir numérique de l'Europe*, COM(2020) 67 final.

11 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Une stratégie européenne pour les données*, COM(2020) 66 final.

12 «Rapport contenant des recommandations à la Commission concernant la finance numérique: risques émergents liés aux crypto-actifs – enjeux en matière de réglementation et de surveillance dans le domaine des services, institutions et marchés financiers [2020/2034(INL)], https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=fr

13 Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020) 605 final.

secteur financier, compte tenu de sa forte dépendance aux services informatiques et de sa grande vulnérabilité aux cyberattaques.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- Base juridique

La présente proposition de règlement est fondée sur l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE).

Elle supprime des obstacles à l'établissement et au fonctionnement du marché intérieur des services financiers et y apporte des améliorations en harmonisant les règles applicables en matière de gestion des risques informatiques, de notification, de tests et de risques liés aux tiers prestataires de services informatiques. Les disparités actuelles dans ce domaine, tant sur le plan législatif et en matière de surveillance qu'au niveau national et européen, font obstacle au marché unique des services financiers, car les entités financières qui exercent des activités transfrontières sont confrontées à des exigences réglementaires ou à des attentes en matière de surveillance différentes, voire redondantes, susceptibles d'entraver l'exercice de leurs libertés d'établissement et de prestation de services. L'existence de règles différentes fausse également la concurrence entre le même type d'entités financières dans les différents États membres. De plus, dans les domaines où l'harmonisation est absente, partielle ou limitée, l'élaboration de règles ou d'approches nationales divergentes, soit déjà en vigueur, soit en cours d'adoption et de mise en œuvre au niveau national, peut avoir un effet dissuasif sur l'exercice des libertés conférées par le marché unique concernant les services financiers. Cela vaut en particulier pour les cadres relatifs aux tests opérationnels numériques et la supervision des tiers prestataires critiques de services informatiques.

Étant donné que la proposition a une incidence sur plusieurs directives du Parlement européen et du Conseil adoptées sur la base de l'article 53, paragraphe 1, du TFUE, une proposition de directive, intégrant les modifications à apporter à ces directives, est également adoptée en parallèle.

- Subsidiarité

Le degré élevé d'interconnexion des services financiers, l'importante activité transfrontière des entités financières et la forte dépendance du secteur financier dans son ensemble à l'égard des tiers prestataires de services informatiques justifient de garantir une résilience numérique opérationnelle solide, dans l'intérêt commun, afin de préserver la solidité des marchés financiers de l'Union européenne. Les disparités qui résultent de régimes inégaux ou partiels, de chevauchements ou d'exigences multiples applicables aux mêmes entités financières opérant dans un contexte transfrontière ou détenant plusieurs agréments[14] au sein du marché unique ne peuvent être traitées efficacement qu'au niveau de l'Union.

Cette proposition harmonise la composante opérationnelle numérique d'un secteur profondément intégré et interconnecté qui bénéficie déjà d'un ensemble unique de règles et fait déjà l'objet d'une surveillance dans la plupart des autres domaines clés. Pour des questions telles que la notification des incidents liés à l'informatique, seules des règles harmonisées au niveau de l'Union pourraient réduire le niveau des charges administratives et

[14] Une même entité financière peut être détentrice d'un agrément bancaire, d'un agrément en tant qu'entreprise d'investissement et d'un agrément en tant qu'établissement de paiement, chacun délivré par une autorité de surveillance différente dans un ou plusieurs États membres.

des coûts financiers associés à la notification d'un même incident lié à l'informatique à différentes autorités nationales et de l'Union. Une action au niveau de l'Union européenne est aussi nécessaire pour faciliter la reconnaissance mutuelle des résultats des tests de résilience opérationnelle numérique avancés pour les entités exerçant des activités transfrontières, qui, en l'absence de règles de l'Union, sont ou sont susceptibles d'être soumises à des cadres différents dans les différents États membres. Seule une action au niveau de l'Union peut mettre fin aux divergences entre les approches adoptées par les États membres en matière de tests. Une action à l'échelle de l'Union est également nécessaire pour remédier à l'absence de pouvoirs adéquats de supervision des risques découlant des tiers prestataires de services informatiques, notamment les risques de concentration et de contagion pour le secteur financier de l'Union.

- Proportionnalité

Les dispositions proposées n'excèdent pas ce qui est nécessaire pour atteindre les objectifs de la proposition. Elles couvrent uniquement les aspects que les États membres ne peuvent pas réaliser par eux-mêmes et pour lesquels la charge administrative et les coûts sont proportionnés aux objectifs spécifiques et généraux à atteindre.

La proportionnalité est assurée en termes de portée et d'intensité par le recours à des critères d'évaluation qualitatifs et quantitatifs. Ceux-ci visent à garantir que les nouvelles règles, bien qu'étant applicables à l'ensemble des entités financières, sont dans le même temps adaptées aux risques et aux besoins inhérents à leurs caractéristiques propres en matière de taille et de profil d'activité. La proportionnalité est également intégrée dans les dispositions relatives à la gestion des risques informatiques, aux tests de résilience numérique, à la notification des incidents majeurs liés à l'informatique et à la supervision des tiers prestataires critiques de services informatiques.

- Choix de l'instrument

Les mesures devant régir la gestion des risques informatiques, la notification des incidents liés à l'informatique, les tests et la supervision des tiers prestataires critiques de services informatiques doivent être intégrées dans un règlement afin de garantir que les exigences détaillées sont effectivement et directement applicables de manière uniforme, sans préjudice de la proportionnalité et des dispositions spécifiques prévues par le présent règlement. La cohérence dans la gestion des risques opérationnels numériques contribue à renforcer la confiance dans le système financier et préserve sa stabilité. Étant donné que le recours à un règlement contribue à réduire la complexité réglementaire, favorise la convergence en matière de surveillance et accroît la sécurité juridique, le présent règlement contribue également à limiter les coûts de mise en conformité pour les entités financières, en particulier pour celles qui exercent des activités transfrontières, ce qui devrait en retour contribuer à supprimer les distorsions de concurrence.

En outre, le présent règlement élimine les disparités législatives et les approches nationales inégales en matière de réglementation ou de surveillance des risques informatiques et supprime ainsi des obstacles au marché unique des services financiers, notamment ceux qui entravent le plein exercice de la liberté d'établissement et de prestation de services pour les entités financières ayant une assise transfrontière.

Enfin, le corpus réglementaire unique a été principalement élaboré au moyen de règlements, et son actualisation par l'ajout de la composante relative à la résilience opérationnelle numérique devrait se faire selon le même choix d'instrument juridique.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- Évaluations ex post/bilans de qualité de la législation existante

Jusqu'à présent, aucune législation de l'Union sur les services financiers ne s'est concentrée sur la résilience opérationnelle, et aucune n'a traité de manière exhaustive les risques découlant de la numérisation, pas même celles dont les règles traitent plus généralement du risque opérationnel avec le risque informatique comme sous-composante. Jusqu'à présent, l'intervention de l'Union a contribué à répondre aux besoins et aux problèmes qui sont apparus au lendemain de la crise financière de 2008: les établissements de crédit n'étaient pas suffisamment capitalisés, les marchés financiers n'étaient pas suffisamment intégrés, et l'harmonisation était jusqu'alors demeurée minimale. Le risque informatique n'était pas considéré comme une priorité à l'époque et, par conséquent, les cadres juridiques applicables aux différents sous-secteurs financiers ont évolué de manière non coordonnée. Néanmoins, l'action de l'Union a atteint ses objectifs, à savoir garantir la stabilité financière et instaurer un ensemble unique de règles prudentielles et de conduite, harmonisées et applicables aux entités financières dans toute l'Union européenne. Étant donné que les facteurs qui ont motivé l'intervention législative de l'Union dans le passé n'ont pas donné lieu à des dispositions spécifiques ou globales permettant de répondre à l'utilisation généralisée des technologies numériques et aux risques financiers qui en découlent, la réalisation d'une évaluation explicite semble difficile. Chaque pilier du présent règlement repose sur un exercice d'évaluation implicite et sur les modifications législatives correspondantes.

- Consultation des parties intéressées

La Commission a consulté les parties intéressées tout au long du processus d'élaboration de la présente proposition, en particulier:

i) la Commission a procédé à une consultation publique ouverte spécifique (du 19 décembre 2019 au 19 mars 2020)[15];

ii) la Commission a consulté le public dans le cadre d'une analyse d'impact initiale (du 19 décembre 2019 au 16 janvier 2020)[16];

iii) les services de la Commission ont consulté les experts des États membres au sein du groupe d'experts sur la banque, les paiements et l'assurance, à deux reprises (18 mai 2020 et 16 juillet 2020)[17];

iv) les services de la Commission ont organisé un webinaire consacré à la résilience opérationnelle numérique, dans le cadre de la campagne d'information 2020 sur la finance numérique (19 mai 2020).

L'objectif de la consultation publique était d'éclairer la Commission sur l'élaboration d'un éventuel cadre de résilience opérationnelle numérique transsectoriel de l'Union européenne dans le domaine des services financiers. Les réponses recueillies ont fait apparaître un large soutien en faveur de la mise en place d'un cadre spécifique prévoyant des mesures ciblant les

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

quatre domaines soumis à la consultation, tout en soulignant la nécessité de garantir la proportionnalité et d'aborder et d'expliquer avec soin l'interaction avec les règles horizontales de la directive SRI. La Commission a reçu deux réponses sur l'analyse d'impact initiale, dans lesquelles les répondants traitaient d'aspects spécifiques liés à leur domaine d'activité.

Lors de la réunion du groupe d'experts sur la banque, les paiements et l'assurance organisée le 18 mai 2020, les États membres se sont déclarés très favorables au renforcement de la résilience opérationnelle numérique du secteur financier par les mesures envisagées au titre des quatre éléments définis par la Commission. Les États membres ont également insisté sur la nécessité de garantir une articulation claire des nouvelles règles avec celles relatives au risque opérationnel (dans le cadre de la législation européenne sur les services financiers) et avec les règles horizontales sur la cybersécurité (directive SRI). Au cours de la deuxième réunion, certains États membres ont rappelé la nécessité de garantir la proportionnalité et de tenir compte de la situation particulière des petites entreprises ou des filiales de groupes de plus grande taille, ainsi que la nécessité de conférer un mandat solide aux autorités nationales compétentes associées à la supervision.

La proposition s'appuie également sur les retours d'information recueillis lors de réunions avec les parties intéressées et les autorités et institutions de l'Union européenne, et en tient compte. Les parties intéressées, y compris les tiers prestataires de services informatiques, se sont montrées globalement favorables. Les retours d'information reçus font apparaître la nécessité de préserver la proportionnalité et de suivre une approche fondée sur les principes et les risques dans la conception des règles. Sur le plan institutionnel, les principales contributions ont été apportées par le comité européen du risque systémique (CERS), les AES, l'Agence de l'Union européenne pour la cybersécurité (ENISA) et la Banque centrale européenne (BCE), ainsi que par les autorités compétentes des États membres.

- Obtention et utilisation d'expertise

Pour élaborer cette proposition, la Commission s'est appuyée sur des données probantes qualitatives et quantitatives recueillies à partir de sources reconnues, notamment les deux avis techniques conjoints des AES. Ce travail a été complété par des contributions confidentielles et des rapports accessibles au public émanant d'autorités de surveillance, d'organismes internationaux de normalisation et d'instituts de recherche de premier plan, ainsi que par des contributions quantitatives et qualitatives de parties intéressées spécifiques au sein du secteur financier mondial.

- Analyse d'impact

La présente proposition est accompagnée d'une analyse d'impact[18] qui a été soumise au comité d'examen de la réglementation (CER) le 29 avril 2020 et approuvée le 29 mai 2020. Le CER a recommandé d'apporter des améliorations dans certains domaines en vue: i) de fournir davantage d'informations sur la manière dont la proportionnalité serait garantie; ii) de mieux mettre en évidence la mesure dans laquelle l'option privilégiée se distingue de l'avis technique conjoint des AES, et pourquoi cette option constitue la solution optimale; et iii) de préciser davantage la manière dont la proposition interagit avec la législation de l'Union européenne en vigueur, y compris avec les dispositions en cours de révision. L'analyse

[18] Document de travail des services de la Commission – Rapport d'analyse d'impact accompagnant le document: proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014, SWD(2020) 198 du 24.9.2020.

d'impact a été adaptée selon ces observations, en tenant compte également des observations plus détaillées formulées par le CER.

La Commission a envisagé un certain nombre d'options stratégiques pour élaborer un cadre de résilience opérationnelle numérique:

- «ne rien changer»: les règles relatives à la résilience opérationnelle continueraient à reposer sur l'ensemble des dispositions divergentes actuelles de l'Union en matière de services financiers, en partie sur la directive SRI, et sur les régimes nationaux existants ou futurs;
- option 1: le renforcement des coussins de fonds propres: la constitution de coussins de fonds propres supplémentaires, serait imposée, afin d'accroître la capacité des entités financières à absorber les pertes qui pourraient survenir en raison d'un manque de résilience opérationnelle numérique;
- option 2: l'adoption d'un acte législatif sur la résilience opérationnelle numérique des services financiers: cette option consisterait à favoriser la mise en place, au niveau de l'Union, d'un cadre global prévoyant des règles cohérentes qui répondent aux besoins de résilience opérationnelle numérique de toutes les entités financières réglementées et à établir un cadre de supervision pour les tiers prestataires critiques de services informatiques;
- option 3: un acte législatif sur la résilience opérationnelle numérique des services financiers, combiné à une surveillance centralisée des tiers prestataires critiques de services informatiques: outre un acte législatif sur la résilience opérationnelle numérique (option 2), une nouvelle autorité serait créée pour surveiller la prestation de services des tiers prestataires de services informatiques.

La deuxième option a été retenue, car elle permet d'atteindre la plupart des objectifs visés d'une manière efficace, efficiente et cohérente avec les autres politiques de l'Union. La plupart des parties intéressées privilégient également cette option.

L'option retenue entraînerait des coûts de nature tant ponctuelle que récurrente[19]. Les coûts ponctuels sont principalement dus aux investissements requis dans les systèmes informatiques et sont donc difficiles à quantifier étant donné l'état variable des paysages informatiques complexes des entreprises et en particulier de leurs systèmes informatiques patrimoniaux. Quand bien même, ces coûts devraient être limités pour les grandes entreprises, compte tenu des investissements informatiques considérables qu'elles ont déjà réalisés. Les coûts devraient également être limités pour les petites entreprises, car des mesures proportionnées s'appliqueraient du fait du risque plus faible qu'elles présentent.

L'option retenue aurait des effets positifs sur les PME opérant dans le secteur des services financiers du point de vue des incidences économiques, sociales et environnementales. La proposition apportera aux PME de la clarté sur les règles applicables, ce qui réduira les coûts de mise en conformité.

Les principales répercussions sociales de l'option retenue concerneraient les consommateurs et les investisseurs. Des niveaux plus élevés de résilience opérationnelle numérique au sein du

[19] *Ibid, p. 89 à 94.*

système financier de l'Union réduiraient le nombre et le coût moyen des incidents. La société dans son ensemble tirerait profit de la confiance accrue dans le secteur des services financiers.

Enfin, s'agissant des incidences sur l'environnement, l'option stratégique choisie encouragerait une utilisation accrue de la dernière génération d'infrastructures et de services informatiques, qui devraient gagner en durabilité sur le plan environnemental.

- Réglementation affûtée et simplification

La suppression des exigences redondantes en matière de notification des incidents liés à l'informatique permettrait de réduire les charges administratives et les coûts liés. En outre, l'harmonisation des tests de résilience opérationnelle numériques avec reconnaissance mutuelle dans l'ensemble du marché unique permettra fera baisser les coûts, notamment pour les entreprises transfrontières qui, autrement, risqueraient d'être soumises à l'obligation de procéder à de multiples tests dans les différents États membres[20].

- Droits fondamentaux

L'Union européenne a la volonté de respecter des normes élevées de protection des droits fondamentaux. L'ensemble des dispositifs volontaires de partage d'informations entre entités financières promu par le présent règlement s'inscrirait dans des environnements de confiance, dans le plein respect des dispositions de l'Union en matière de protection des données, notamment du règlement (UE) nº 2016/679 du Parlement européen et du Conseil[21], en particulier lorsque le traitement de données à caractère personnel est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement.

4. INCIDENCE BUDGÉTAIRE

En ce qui concerne les incidences budgétaires, étant donné que le présent règlement renforce le rôle des AES en leur conférant le pouvoir de superviser dûment les tiers prestataires critiques de services informatiques, il suppose le déploiement de ressources supplémentaires, notamment pour les missions de supervision (telles que les inspections sur place et en ligne et les exercices d'audit), et le recours à du personnel doté d'une expertise spécifique en matière de sécurité informatique.

L'ampleur et la répartition de ces coûts dépendront de l'étendue des nouveaux pouvoirs de supervision et des tâches (précises) qui seront confiés aux AES. S'agissant de la mise à disposition de nouvelles ressources en personnel, l'ABE, l'AEMF et l'AEAPP auront besoin au total de 18 employés à temps plein (ETP) – six ETP pour chaque autorité – lorsque les différentes dispositions de la proposition entreront en application (pour un coût estimé à 15,71 millions d'EUR pour la période 2022-2027). Les AES supporteront également des coûts informatiques supplémentaires, des frais de mission liés aux inspections sur place et des frais de traduction (estimés à 12 millions d'EUR pour la période 2022-2027), ainsi que d'autres dépenses administratives (estimées à 2,48 millions d'EUR pour la période 2022-2027). Par conséquent, les coûts totaux sont estimés à environ 30,19 millions d'EUR pour la période 2022-2027.

---

20 *Ibid*.

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

Il convient également de noter que, si les effectifs (par exemple, les nouveaux membres du personnel et les autres dépenses liées aux nouvelles tâches) nécessaires à la supervision directe dépendront de l'évolution, au fil du temps, du nombre et de la taille des tiers prestataires critiques de services informatiques à superviser, les dépenses respectives seront entièrement financées par les redevances perçues auprès de ces acteurs du marché. Par conséquent, aucune incidence sur les crédits budgétaires de l'Union n'est prévue (sauf pour le personnel supplémentaire), car ces coûts seront entièrement financés par les redevances.

Les incidences budgétaires et financières de la présente proposition sont expliquées en détail dans la fiche financière législative jointe à celle-ci.

5. AUTRES ÉLÉMENTS

- Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information

La proposition prévoit un plan général de suivi et d'évaluation des incidences sur les objectifs spécifiques. La Commission sera ainsi tenue de procéder à un réexamen au minimum trois ans après l'entrée en vigueur et de rendre compte de ses principales conclusions au Parlement européen et au Conseil.

Le réexamen doit être réalisé conformément aux lignes directrices de la Commission pour une meilleure réglementation.

- Explication détaillée des différentes dispositions de la proposition

La proposition s'articule autour de plusieurs grands axes d'action, qui sont des piliers essentiels interdépendants inclus de manière consensuelle dans les orientations et les bonnes pratiques européennes et internationales destinées à renforcer la cyberrésilience et la résilience opérationnelle du secteur financier.

Champ d'application du règlement et proportionnalité dans l'application des mesures requises (article 2)

Afin de garantir la cohérence des exigences en matière de gestion des risques informatiques applicables au secteur financier, le règlement couvre tout un éventail d'entités financières réglementées au niveau de l'Union, à savoir les établissements de crédit, les établissements de paiement, les établissements de monnaie électronique, les entreprises d'investissement, les prestataires de services sur crypto-actifs, les dépositaires centraux de titres, les contreparties centrales, les plates-formes de négociation, les référentiels centraux, les gestionnaires de fonds d'investissement alternatifs et les sociétés de gestion, les prestataires de services de communication de données, les entreprises d'assurance et de réassurance, les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire, les institutions de retraite professionnelle (IRP), les agences de notation de crédit, les contrôleurs légaux des comptes et les cabinets d'audit, les administrateurs d'indices de référence d'importance critique et les prestataires de services de financement participatif.

Une telle couverture favorise une application homogène et cohérente de l'ensemble des composantes de la gestion des risques dans les domaines liés à l'informatique, tout en garantissant des conditions de concurrence équitables entre les entités financières en ce qui concerne leurs obligations réglementaires en matière de risque informatique. Dans le même temps, le règlement tient compte du fait qu'il existe des différences importantes entre les entités financières du point de vue de leur taille, de leur profil d'activité ou de leur exposition au risque numérique. Étant donné que les grandes entités financières disposent de plus de

ressources, seules les entités financières qui ne sont pas considérées comme des microentreprises devront, par exemple, mettre en place des dispositifs de gouvernance complexes et des fonctions de gestion dédiées, effectuer des évaluations approfondies après l'apport de changements majeurs aux infrastructures de réseau et de système d'information, soumettre régulièrement leurs systèmes informatiques patrimoniaux à des analyses de risque, ainsi qu'étendre les tests de continuité des activités et des plans de réponse et de rétablissement pour y intégrer des scénarios de basculement de leur infrastructure informatique principale aux installations redondantes. En outre, seules les entités financières reconnues comme étant d'importance significative aux fins des tests de résilience numérique avancés seront tenues de procéder à des tests de pénétration fondés sur la menace.

Bien que cette couverture soit large, elle n'est pas exhaustive. Le présent règlement ne couvre notamment pas les opérateurs de système au sens de l'article 2, point p), de la directive 98/26/CE[22] concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres (DCDR), ni aucun participant aux systèmes, à moins que ce participant ne soit lui-même une entité financière réglementée au niveau de l'Union et qu'en tant que tel, il soit couvert par le présent règlement à part entière (c'est-à-dire un établissement de crédit, une entreprise d'investissement, une contrepartie centrale). En outre, le registre de l'Union relatif aux quotas d'émission qui est géré, conformément à la directive 2003/87/CE[23], sous l'égide de la Commission européenne ne relève pas non plus du règlement.

Ces exclusions de la DCDR tiennent compte de la nécessité de procéder à un nouveau réexamen des questions juridiques et des politiques afférentes aux opérateurs de système et aux participants aux systèmes relevant de la DCDR, tout en prenant dûment en considération les incidences des cadres qui s'appliquent actuellement aux systèmes de paiement[24] exploités par les banques centrales. Dans la mesure où ces sujets peuvent englober des aspects qui restent distincts des questions couvertes par le présent règlement, la Commission continuera à évaluer la nécessité et les incidences d'une extension éventuelle du champ d'application du présent règlement aux entités et aux infrastructures informatiques qui ne relèvent actuellement pas de ses dispositions.

Exigences en matière de gouvernance (article 4)

Le présent règlement vise à mieux aligner les stratégies d'entreprise des entités financières, ainsi que leur conduite de la gestion des risques informatiques. À cet effet, l'organe de direction sera tenu de conserver un rôle actif déterminant dans le pilotage du cadre de gestion des risques informatiques et veillera au respect d'une hygiène informatique rigoureuse. La pleine responsabilité de l'organe de direction dans la gestion des risques informatiques de l'entité financière constituera un principe général qui devra se décliner en une série d'exigences spécifiques, telles que l'attribution de rôles et de responsabilités clairs pour toutes les fonctions liées à l'informatique, un engagement continu dans le contrôle du suivi de la

[22] Directive 98/26/CE du Parlement européen et du Conseil du 19 mai 1998 concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres (JO L 166 du 11.6.1998, p. 45).

[23] Directive 2003/87/CE du Parlement européen et du Conseil du 13 octobre 2003 établissant un système d'échange de quotas d'émission de gaz à effet de serre dans la Communauté et modifiant la directive 96/61/CE du Conseil (JO L 275 du 25.10.2003, p. 32).

[24] En particulier, le règlement (UE) nº 795/2014 de la Banque centrale européenne du 3 juillet 2014 concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique.

gestion des risques informatiques, ainsi que dans l'ensemble des processus d'approbation et de contrôle, et une répartition appropriée des investissements et des formations dans le domaine informatique.

Exigences en matière de gestion des risques informatiques (articles 5 à 14)

La résilience opérationnelle numérique est ancrée dans un ensemble de principes et d'exigences clés applicables au cadre de gestion des risques informatiques, conformément à l'avis technique conjoint des AES. Ces exigences, inspirées des normes, des lignes directrices et des recommandations internationales, nationales et sectorielles pertinentes, s'articulent autour de fonctions spécifiques de la gestion des risques informatiques (identification, protection et prévention, détection, réponse et rétablissement, apprentissage et évolution, et communication). Afin de rester en phase avec l'évolution rapide du paysage des cybermenaces, les entités financières sont tenues de mettre en place et de maintenir des systèmes et des outils informatiques résilients qui réduisent au minimum l'incidence des risques informatiques, d'identifier en permanence toutes les sources de risques informatiques, d'adopter des mesures de protection et de prévention, de détecter rapidement les activités anormales, d'instaurer des politiques de continuité des activités et des plans de rétablissement après sinistre spécifiques et complets faisant partie intégrante de la stratégie de continuité des activités opérationnelles. Ces dernières composantes sont nécessaires pour assurer une récupération rapide à la suite d'incidents liés à l'informatique, en particulier des cyberattaques, en limitant les dommages et en donnant la priorité à une reprise sûre des activités. Le règlement n'impose pas lui-même une normalisation spécifique, mais se fonde plutôt sur les bonnes pratiques du secteur ou les normes techniques reconnues à l'échelle européenne et internationale, dans la mesure où elles sont pleinement conformes aux instructions de surveillance relatives à l'utilisation et à l'incorporation de ces normes internationales. Le présent règlement couvre également l'intégrité, la sûreté et la résilience des infrastructures et installations physiques sur lesquelles s'appuient l'utilisation des technologies ainsi que les processus et les personnes concernés par l'informatique, dans le cadre de l'empreinte numérique des activités d'une entité financière.

Notification des incidents liés à l'informatique (articles 15 à 20)

La notification des incidents liés à l'informatique est d'abord harmonisée et rationalisée par l'obligation générale faite aux entités financières d'établir et de mettre en œuvre un processus de gestion permettant de suivre et d'enregistrer les incidents liés à l'informatique, puis par l'obligation de les classer sur la base de critères détaillés dans le règlement et précisés plus avant par les AES par la définition de seuils d'importance significative. Deuxièmement, seuls les incidents liés à l'informatique qui sont jugés majeurs doivent être notifiés aux autorités compétentes. La notification devrait se faire selon un modèle commun et une procédure harmonisée mis au point par les AES. Les entités financières devraient soumettre une notification initiale, un rapport intermédiaire et un rapport final et informer leurs utilisateurs et clients lorsque l'incident a ou est susceptible d'avoir une incidence sur leurs intérêts financiers. Les autorités compétentes devraient fournir les informations pertinentes sur les incidents à d'autres institutions ou autorités: aux AES, à la BCE et aux points de contact uniques désignés en vertu de la directive (UE) 2016/1148.

Afin de susciter un dialogue entre les entités financières et les autorités compétentes qui contribuerait à réduire au minimum les incidences et à définir des solutions appropriées, la notification des incidents majeurs liés à l'informatique devrait être complétée par un retour d'information et des orientations de la part des autorités de surveillance.

Enfin, la possibilité de centraliser au niveau de l'Union les notifications d'incidents liés à l'informatique devrait être examinée plus avant dans un rapport conjoint des AES, de la BCE

et de l'ENISA évaluant dans quelle mesure il serait possible de créer un pôle unique de l'UE pour la notification des incidents majeurs liés à l'informatique par les entités financières.

Test de résilience opérationnelle numérique (articles 21 à 24)

Les capacités et les fonctions intégrées dans le cadre de gestion des risques informatiques doivent être testées à intervalles réguliers afin de vérifier l'état de préparation aux risques et d'identifier les éventuelles faiblesses, défaillances ou lacunes, ainsi que de prendre rapidement des mesures correctives. Le présent règlement prévoit une application proportionnée des exigences en matière de tests de résilience opérationnelle numérique en fonction de la taille, de l'activité et du profil de risque des entités financières: si toutes les entités devraient tester leurs outils et systèmes informatiques, seules celles que les autorités compétentes considèrent (sur la base des critères énoncés dans le présent règlement et précisés par les AES) comme étant d'importance significative et cyber-matures devraient être tenues de procéder à des tests avancés sur la base de tests de pénétration fondés sur la menace. Le présent règlement énonce également les exigences applicables aux testeurs et à la reconnaissance des résultats des tests de pénétration fondés sur la menace dans l'ensemble de l'Union pour les entités financières exerçant leur activité dans plusieurs États membres.

Risque lié aux tiers prestataires de services informatiques (articles 25 à 39)

Le règlement est conçu de manière à garantir un suivi rigoureux du risque lié aux tiers prestataires de services informatiques. La réalisation de cet objectif passera en premier lieu par le respect de règles de principe pour le suivi, par les entités financières, des risques découlant des tiers prestataires de services informatiques. En deuxième lieu, le présent règlement harmonise les éléments fondamentaux du service fourni par les tiers prestataires de services informatiques et de la relation nouée avec eux. Ces éléments couvrent les aspects minimaux jugés indispensables pour permettre un suivi complet, par l'entité financière, du risque associé aux tiers prestataires de services informatiques tout au long des différentes étapes de leur relation, à savoir la conclusion du contrat, son exécution, sa résiliation et la phase post-contractuelle.

Plus particulièrement, les contrats qui régissent cette relation devront comporter les éléments suivants: une description complète des services, l'indication des lieux où les données doivent être traitées, une description complète des niveaux de service accompagnée d'objectifs de performance quantitatifs et qualitatifs, des dispositions pertinentes sur l'accessibilité, la disponibilité, l'intégrité, la sécurité et la protection des données à caractère personnel, des garanties d'accès, de récupération et de restitution en cas de défaillance des tiers prestataires de services informatiques, les délais de préavis et les obligations d'information incombant aux tiers prestataires de services informatiques, les droits d'accès, d'inspection et d'audit par l'entité financière ou un tiers désigné, des droits de résiliation clairs et des stratégies de sortie spécifiques. En outre, puisque certains de ces éléments contractuels peuvent être normalisés, le règlement encourage l'emploi volontaire de clauses contractuelles types qui doivent être élaborées par la Commission pour l'utilisation de services d'informatique en nuage.

Enfin, le règlement vise à promouvoir la convergence des approches prudentielles en matière de risque lié aux tiers prestataires de services informatiques dans le secteur financier, en soumettant les tiers prestataires critiques de services informatiques à un cadre de supervision de l'Union. Grâce à un nouveau cadre législatif harmonisé, l'AES désignée comme superviseur principal pour chacun de ces tiers prestataires critiques de services informatiques se voit conférer des pouvoirs lui permettant de veiller à ce que les prestataires de services technologiques qui jouent un rôle essentiel dans le fonctionnement du secteur financier fassent l'objet d'un suivi adéquat à l'échelle paneuropéenne. Le cadre de supervision prévu par le présent règlement s'appuie sur l'architecture institutionnelle existante dans le domaine

des services financiers, en vertu de laquelle le comité mixte des AES assure une coordination intersectorielle pour toutes les questions relatives aux risques informatiques, conformément aux tâches qui lui incombent en matière de cybersécurité, avec le soutien du sous-comité compétent (forum de supervision), chargé d'effectuer les travaux préparatoires aux fins des décisions individuelles et des recommandations collectives destinées aux tiers prestataires critiques de services.

Partage d'informations (article 40)

Dans le but d'accroître la sensibilisation au risque informatique, de réduire au minimum sa propagation et de renforcer les capacités défensives des entités financières et leurs techniques de détection des menaces, le règlement habilite ces dernières à mettre en place des dispositifs leur permettant d'échanger entre elles des informations et des renseignements sur les cybermenaces.

2020/0266 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis de la Banque centrale européenne[25],

vu l'avis du Comité économique et social européen[26],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) À l'ère numérique, les technologies de l'information et de la communication (TIC) sous-tendent les systèmes complexes qui sont utilisés dans les activités quotidiennes de la société. Elles contribuent à la bonne marche de nos économies dans des secteurs clés, tels que la finance, et améliorent le fonctionnement du marché unique. Le degré croissant de numérisation et d'interconnexion accentue également les risques informatiques, ce qui expose davantage la société dans son ensemble – et le système financier en particulier – aux cybermenaces ou aux dysfonctionnements informatiques. Si l'utilisation généralisée de systèmes informatiques ainsi qu'une numérisation et une connectivité poussées sont aujourd'hui des caractéristiques essentielles de toutes les activités des entités financières de l'Union, la résilience numérique n'est pas encore suffisamment intégrée dans leurs cadres opérationnels.

(2) Au cours des dernières décennies, l'utilisation des TIC est devenue centrale dans le domaine de la finance, et elle revêt aujourd'hui une importance cruciale dans l'exécution des fonctions quotidiennes typiques de toutes les entités financières. La numérisation couvre, par exemple, les paiements, qui ont évolué progressivement de méthodes reposant sur les espèces et le papier vers l'utilisation de solutions numériques, ainsi que la compensation et le règlement des opérations sur titres, le trading électronique et algorithmique, les opérations de prêt et de financement, le financement entre pairs, la notation de crédit, la souscription d'assurance, la gestion de créances et les opérations de post-marché. L'ensemble du secteur financier a non seulement opéré une transition vers le numérique à grande échelle, mais la numérisation a également renforcé les interconnexions et les relations de dépendance

[25] [*ajouter la référence*] JO C du , p. .

[26] [*ajouter la référence*] JO C du , p. .

au sein du secteur financier et avec les tiers prestataires d'infrastructures et de services.

(3) Dans un rapport de 2020 consacré au cyberrisque systémique[27], le Comité européen du risque systémique (CERS) a réaffirmé que le niveau élevé d'interconnexion existant entre les entités financières, les marchés financiers et les infrastructures des marchés financiers, et en particulier les interdépendances de leurs systèmes informatiques, était susceptible de constituer une vulnérabilité systémique, dans la mesure où des cyberincidents localisés pourraient rapidement se propager de l'une des quelque 22 000 entités financières[28] de l'Union à l'ensemble du système financier, sans aucune entrave géographique. Les atteintes graves à la sécurité informatique qui se produisent dans le secteur de la finance ne touchent pas seulement les entités financières prises isolément. Elles facilitent également la propagation de vulnérabilités localisées à travers les canaux de transmission financière et peuvent avoir des conséquences préjudiciables pour la stabilité du système financier de l'Union, en provoquant des fuites de liquidités et une érosion générale de la confiance dans les marchés financiers.

(4) Ces dernières années, les risques informatiques ont attiré l'attention des décideurs politiques, des régulateurs et des organismes de normalisation nationaux, européens et internationaux, dans un effort visant à renforcer la résilience, à définir des normes et à coordonner le travail de réglementation ou de surveillance. Au niveau international, le Comité de Bâle sur le contrôle bancaire, le Comité sur les paiements et les infrastructures de marché, le Conseil de stabilité financière, l'Institut pour la stabilité financière, ainsi que les groupes de pays du G7 et du G20 s'efforcent de fournir aux autorités compétentes et aux opérateurs de marché des différentes juridictions des outils leur permettant de renforcer la résilience de leurs systèmes financiers.

(5) Malgré des initiatives stratégiques et législatives ciblées aux niveaux national et européen, les risques informatiques représentent toujours un défi pour la résilience opérationnelle, la performance et la stabilité du système financier de l'Union. La réforme qui a suivi la crise financière de 2008 a principalement renforcé la résilience financière du secteur financier de l'Union et visait à préserver la compétitivité et la stabilité de l'Union du point de vue économique, prudentiel et des conduites sur le marché. Bien que la sécurité informatique et la résilience numérique fassent partie du risque opérationnel, le programme réglementaire d'après crise leur a accordé moins d'importance, et elles n'ont été développées que dans certains domaines de la politique et du paysage réglementaire des services financiers de l'Union, ou seulement dans quelques États membres.

---

27 Rapport du CERS sur le cyberrisque systémique, février 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 D'après l'analyse d'impact accompagnant le réexamen des autorités européennes de surveillance [SWD(2017) 308], il existe environ 5 665 établissements de crédit, 5 934 entreprises d'investissement, 2 666 entreprises d'assurance, 1 573 IRP, 2 500 entreprises de gestion d'investissements, 350 infrastructures de marché [telles que les CCP, les bourses, les internalisateurs systématiques, les référentiels centraux et les systèmes de négociation multilatérale («Multilateral Trading Facilities» ou MTF)], 45 agences de notation de crédit et 2 500 établissements de paiement et établissements de monnaie électronique agréés. Au total, cela représente environ 21 233 entités, sans compter les entités de financement participatif, les contrôleurs légaux des comptes et les cabinets d'audit, les prestataires de services sur crypto-actifs et les administrateurs d'indices de référence.

(6) Dans son plan d'action de 2018 pour les technologies financières[29], la Commission a souligné l'importance primordiale de rendre le secteur financier de l'Union plus résilient, également d'un point de vue opérationnel, afin de garantir sa sûreté technologique et son bon fonctionnement, ainsi que son rétablissement rapide après des atteintes à la sécurité et des incidents informatiques, de façon à ce que les services financiers puissent être fournis de manière efficace et sans accrocs dans toute l'Union, y compris dans des situations de tension, tout en préservant la confiance des consommateurs et des marchés.

(7) En avril 2019, l'Autorité bancaire européenne (ABE), l'Autorité européenne des marchés financiers (AEMF) et l'Autorité européenne des assurances et des pensions professionnelles (AEAPP) (appelées conjointement les «autorités européennes de surveillance» ou «AES») ont publié deux avis techniques conjoints préconisant une approche cohérente du risque informatique dans le secteur financier et recommandant de renforcer, de manière proportionnée, la résilience opérationnelle numérique de ce secteur dans le cadre d'une initiative sectorielle de l'Union.

(8) Le secteur financier de l'Union est soumis à un corpus réglementaire unique harmonisé, et régi par un système européen de surveillance financière. Néanmoins, les dispositions relatives à la résilience opérationnelle numérique et à la sécurité informatique ne sont pas encore totalement ou systématiquement harmonisées, alors que la résilience opérationnelle numérique est indispensable pour garantir la stabilité financière et l'intégrité du marché à l'ère numérique, et qu'elle n'est pas moins importante que, par exemple, des normes prudentielles ou de conduite communes. Le corpus réglementaire unique et le système de surveillance devraient donc être développés pour couvrir également cette composante, et les mandats des autorités de surveillance financière chargées de surveiller et de protéger la stabilité financière et l'intégrité du marché devraient ainsi être étendus.

(9) Les disparités législatives et les approches nationales inégales en matière de réglementation ou de surveillance du risque informatique créent des obstacles au marché unique des services financiers, lesquels entravent le plein exercice de la liberté d'établissement et la prestation de services des entités financières ayant une assise transfrontière. La concurrence entre le même type d'entités financières opérant dans différents États membres est également susceptible d'être faussée. Notamment dans les domaines où l'harmonisation au niveau de l'Union a été très limitée – comme les tests de résilience opérationnelle numérique – ou inexistante – comme le suivi du risque lié aux tiers prestataires de services informatiques – les disparités découlant des développements prévus au niveau national pourraient créer de nouveaux obstacles au fonctionnement du marché unique, au détriment des acteurs du marché et de la stabilité financière.

(10) L'approche partielle qui a été suivie jusqu'à présent pour les dispositions relatives aux risques liés à l'informatique adoptées au niveau de l'Union présente des lacunes ou des chevauchements dans des domaines importants, tels que la notification des incidents liés à l'informatique et les tests de résilience opérationnelle numérique, et engendre des incohérences imputables à l'émergence de règles nationales divergentes

[29] Communication de la Commission au Parlement européen, au Conseil, à la Banque centrale européenne, au Comité économique et social européen et au Comité des régions, *Plan d'action pour les technologies financières: Pour un secteur financier européen plus compétitif et plus innovant*, COM(2018) 109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

ou une inefficacité par rapport au coût du fait de règles qui se chevauchent. Cette situation est particulièrement préjudiciable pour un utilisateur à forte intensité informatique comme le secteur financier, car les risques technologiques ne connaissent pas de frontières et le secteur financier déploie ses services sur une large base transfrontière à l'intérieur et à l'extérieur de l'Union.

Les entités financières qui exercent des activités transfrontières ou qui détiennent plusieurs agréments (par exemple, une entité financière peut être détentrice d'un agrément bancaire, d'un agrément en tant qu'entreprise d'investissement et d'un agrément en tant qu'établissement de paiement, chacun délivré par une autorité compétente différente dans un ou plusieurs États membres) se heurtent à des difficultés opérationnelles lorsqu'il s'agit de faire face aux risques informatiques et d'atténuer les effets négatifs des incidents informatiques de manière autonome, cohérente et efficace par rapport au coût.

(11) Étant donné que le corpus réglementaire unique n'a pas été accompagné d'un cadre exhaustif applicable aux risques informatiques ou opérationnels, il est nécessaire de procéder à une harmonisation plus poussée des exigences clés en matière de résilience opérationnelle numérique pour toutes les entités financières. Les capacités et la résilience globale que les entités financières, sur la base de ces exigences clés, développeraient en vue de faire face aux interruptions de fonctionnement, contribueraient à préserver la stabilité et l'intégrité des marchés financiers de l'Union et donc à assurer un niveau élevé de protection des investisseurs et des consommateurs dans l'Union. Dans la mesure où le présent règlement se veut une contribution au fonctionnement harmonieux du marché unique, il devrait reposer sur les dispositions de l'article 114 du TFUE, interprétées conformément à la jurisprudence constante de la Cour de justice de l'Union européenne.

(12) Le présent règlement vise tout d'abord à consolider et à mettre à niveau les exigences en matière de risques informatiques, scindées jusqu'à présent dans les différents règlements et directives. Si ces actes juridiques de l'Union couvraient les principales catégories de risques financiers (par exemple, le risque de crédit, le risque de marché, le risque de crédit de contrepartie et le risque de liquidité, le risque lié à la conduite sur le marché), ils ne pouvaient pas, au moment de leur adoption, couvrir de manière exhaustive toutes les composantes de la résilience opérationnelle. Ces actes juridiques de l'Union, lorsqu'ils ont précisé les exigences en matière de risque opérationnel, ont souvent favorisé une approche quantitative classique de la gestion du risque (à savoir, la définition d'une exigence de fonds propres pour couvrir les risques informatiques) plutôt que de définir des exigences qualitatives ciblées visant à renforcer les capacités de protection, détection, confinement, rétablissement et réparation en cas d'incidents liés à l'informatique ou la mise en place de capacités de notification et de tests numériques. Ces directives et règlements étaient principalement destinés à définir les règles essentielles en matière de surveillance prudentielle, d'intégrité du marché ou de conduite sur le marché.

Grâce au présent exercice, qui consolide et actualise les règles relatives au risque informatique, toutes les dispositions traitant du risque numérique dans le secteur financier seraient pour la première fois réunies de manière cohérente dans un seul et même acte législatif. Cette initiative devrait donc combler les lacunes ou remédier aux incohérences de certains de ces actes juridiques, notamment en ce qui concerne la terminologie qui y est utilisée, et devrait faire explicitement référence aux risques informatiques au travers de règles ciblées sur les capacités de gestion des risques informatiques, la notification et les tests, ainsi que le suivi des risques liés aux tiers.

(13) Les entités financières devraient suivre la même approche et les mêmes règles de principe lorsqu'elles abordent le risque informatique. La cohérence contribue à renforcer la confiance dans le système financier et à préserver sa stabilité, en particulier en période de surexploitation des systèmes, plateformes et infrastructures informatiques, qui accroît le risque numérique.

Le respect d'une hygiène informatique de base devrait également éviter à l'économie d'avoir à supporter des coûts considérables, en réduisant au minimum les incidences et les coûts des perturbations informatiques.

(14) Le recours à un règlement permet de réduire la complexité réglementaire, favorise la convergence en matière de surveillance et accroît la sécurité juridique, tout en contribuant à limiter les coûts de mise en conformité, notamment pour les entités financières exerçant des activités transfrontières, et à réduire les distorsions de concurrence. Le choix d'un règlement pour la mise en place d'un cadre commun en matière de résilience opérationnelle numérique des entités financières apparaît donc comme le moyen le plus approprié de garantir une application homogène et cohérente de toutes les composantes de la gestion du risque informatique par les secteurs financiers de l'Union.

(15) Outre la législation sur les services financiers, la directive (UE) 2016/1148 du Parlement européen et du Conseil[30] constitue le cadre général actuellement en vigueur en matière de cybersécurité au niveau de l'Union. Parmi les sept secteurs critiques visés dans la directive, celle-ci s'applique notamment à trois types d'entités financières, à savoir les établissements de crédit, les plates-formes de négociation et les contreparties centrales. Toutefois, comme la directive (UE) 2016/1148 prévoit un mécanisme d'identification au niveau national des opérateurs de services essentiels, seuls certains établissements de crédit, plates-formes de négociation et contreparties centrales identifiés par les États membres relèvent en pratique de ses dispositions et sont donc tenus de se conformer aux exigences en matière de sécurité informatique et de notification des incidents qui y sont définies.

(16) Étant donné que le présent règlement rehausse le niveau d'harmonisation des composantes de la résilience numérique, en instaurant, en matière de gestion des risques informatiques et de notification des incidents liés à l'informatique, des exigences plus strictes que celles prévues par la législation actuelle de l'Union sur les services financiers, il s'agit d'une harmonisation plus poussée, y compris par rapport aux exigences énoncées dans la directive (UE) 2016/1148. Par conséquent, le présent règlement constitue la lex specialis de la directive (UE) 2016/1148.

Il est indispensable de maintenir un lien étroit entre le secteur financier et le cadre horizontal de l'Union en matière de cybersécurité. Cela garantirait la cohérence avec les stratégies de cybersécurité déjà adoptées par les États membres et permettrait aux autorités de surveillance financière d'être informées des cyberincidents touchant d'autres secteurs couverts par la directive (UE) 2016/1148.

(17) Afin de favoriser un processus d'apprentissage intersectoriel et de tirer efficacement parti des expériences d'autres secteurs en matière de lutte contre les cybermenaces, les entités financières visées dans la directive (UE) 2016/1148 devraient continuer à faire

[30] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

partie de l'«écosystème» de cette directive (par exemple, le groupe de coopération SRI et les CSIRT).

Les AES et les autorités nationales compétentes devraient pouvoir participer respectivement aux discussions stratégiques et aux travaux techniques du groupe de coopération SRI, et échanger des informations et coopérer davantage avec les points de contact uniques désignés en vertu de la directive (UE) 2016/1148. Les autorités compétentes au titre du présent règlement devraient également consulter les CSIRT nationaux désignés conformément à l'article 9 de la directive (UE) 2016/1148 et coopérer avec ceux-ci.

(18) Il est également important de garantir la cohérence avec la directive sur les infrastructures critiques européennes (ICE), qui fait actuellement l'objet d'une révision en vue de renforcer la protection et la résilience des infrastructures critiques contre les menaces non liées à la cybercriminalité, avec d'éventuelles implications pour le secteur financier[31].

(19) Les fournisseurs de services d'informatique en nuage constituent une catégorie de fournisseurs de service numérique couverts par la directive (UE) 2016/1148. En tant que tels, ils sont soumis à une surveillance a posteriori exercée par les autorités nationales désignées conformément à cette directive, qui se limite aux exigences en matière de sécurité informatique et de notification des incidents prévues dans cet acte. Étant donné que le cadre de supervision établi par le présent règlement s'applique à tous les tiers prestataires critiques de services informatiques, y compris les fournisseurs de services d'informatique en nuage, lorsqu'ils fournissent des services informatiques à des entités financières, il devrait être considéré comme complémentaire de la surveillance exercée en vertu de la directive (UE) 2016/1148. En outre, le cadre de supervision établi par le présent règlement devrait couvrir les fournisseurs de services d'informatique en nuage en l'absence d'un cadre horizontal de l'Union non spécifique à un secteur et établissant une autorité de supervision numérique.

(20) Pour garder la maîtrise totale des risques informatiques, les entités financières doivent disposer de capacités globales permettant une gestion solide et efficace des risques informatiques, ainsi que de politiques et de mécanismes spécifiques pour la notification des incidents liés à l'informatique, pour le test des systèmes, contrôles et processus informatiques, ainsi que pour la gestion des risques informatiques liés aux tiers prestataires de services informatiques. Le seuil de résilience opérationnelle numérique du système financier devrait être relevé tout en permettant une application proportionnée des exigences aux entités financières qui sont des microentreprises au sens de la recommandation 2003/361/CE de la Commission[32].

(21) Les seuils et les taxinomies de notification des incidents liés à l'informatique varient considérablement au niveau national. Bien que des bases communes puissent être dégagées grâce aux travaux pertinents menés par l'Agence de l'Union européenne pour la cybersécurité (ENISA)[33] et le groupe de coopération SRI pour les entités

---

31 Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008, p. 75).

32 Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

33 ENISA, «Reference Incident Classification Taxonomy», https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

financières relevant de la directive (UE) 2016/1148, des approches divergentes sur les seuils et les taxinomies existent toujours ou peuvent apparaître pour les autres entités financières. Il en résulte de multiples exigences auxquelles les entités financières doivent se conformer, notamment lorsqu'elles sont actives dans plusieurs pays de l'Union et lorsqu'elles font partie d'un groupe financier. En outre, ces divergences peuvent entraver la création de nouveaux mécanismes uniformes ou centralisés au niveau de l'Union, qui accéléreraient le processus de notification et favoriseraient un échange rapide et sans entrave d'informations entre les autorités compétentes, ce qui est essentiel pour faire face aux risques informatiques en cas d'attaques à grande échelle susceptibles d'avoir des conséquences systémiques.

(22) Afin de permettre aux autorités compétentes de remplir leur rôle de surveillance en disposant d'une vue d'ensemble complète de la nature, de la fréquence, de l'importance et des conséquences des incidents liés à l'informatique, et afin d'améliorer l'échange d'informations entre les autorités publiques compétentes, y compris les autorités répressives et les autorités de résolution, il est nécessaire d'établir des règles qui complètent le régime de notification des incidents liés à l'informatique en y ajoutant les exigences qui font actuellement défaut dans la législation financière sous-sectorielle et de supprimer tout chevauchement et double emploi existant afin d'alléger les coûts. Il est donc essentiel d'harmoniser le régime de notification des incidents liés à l'informatique en imposant à toutes les entités financières de ne les notifier qu'à leurs autorités compétentes. En outre, les AES devraient être habilitées à préciser davantage les éléments nécessaires à la notification des incidents liés à l'informatique, tels que la taxinomie, les délais, les ensembles de données, les modèles et les seuils applicables.

(23) Les exigences en matière de tests de résilience opérationnelle numérique ont évolué dans certains sous-secteurs financiers au sein de plusieurs cadres nationaux non coordonnés traitant les mêmes questions de manière différente. Cette situation entraîne une multiplication des coûts pour les entités financières transfrontières et complique la reconnaissance mutuelle des résultats. L'absence de coordination des tests est donc susceptible de segmenter le marché unique.

(24) En outre, lorsqu'aucun test n'est requis, les vulnérabilités ne sont pas détectées, ce qui expose l'entité financière et, en fin de compte, la stabilité et l'intégrité du secteur financier à un risque plus élevé. Sans une intervention au niveau de l'Union, les tests de résilience opérationnelle numérique demeureraient parcellaires, et il n'y aurait aucune reconnaissance mutuelle des résultats des tests d'un pays à l'autre. En outre, puisqu'il est peu probable que d'autres sous-secteurs financiers adoptent de tels mécanismes à une échelle significative, ils passeraient à côté des avantages qui peuvent en découler, tels que la mise au jour des vulnérabilités et des risques, le test des capacités de défense et de la continuité des activités, et la confiance accrue des clients, des fournisseurs et des partenaires commerciaux. Pour remédier à ces chevauchements, divergences et lacunes, il est nécessaire d'établir des règles visant à coordonner les tests effectués par les entités financières et les autorités compétentes, ce qui facilitera la reconnaissance mutuelle des tests avancés pour les entités financières d'importance significative.

(25) La dépendance des entités financières à l'égard des services informatiques s'explique en partie par le fait qu'elles doivent s'adapter à l'émergence d'une économie mondiale numérique compétitive, accroître leur efficacité commerciale et répondre à la demande des consommateurs. La nature et l'ampleur de cette dépendance n'ont cessé d'évoluer ces dernières années, faisant baisser les coûts de l'intermédiation financière et permettant aux entités financières de s'étendre et de déployer leurs activités à plus grande échelle, tout en disposant d'un large éventail d'outils informatiques pour gérer des processus internes complexes.

(26) Cette utilisation étendue des services informatiques est attestée par des accords contractuels complexes, dans le cadre desquels les entités financières ont souvent du mal à négocier des conditions contractuelles adaptées aux normes prudentielles ou autres exigences réglementaires auxquelles elles sont soumises, ou encore à faire respecter des droits spécifiques, tels que les droits d'accès ou d'audit, lorsque ces derniers sont inscrits dans les accords. En outre, nombre de ces contrats ne prévoient pas de garanties suffisantes pour permettre un véritable suivi des processus de sous-externalisation, privant ainsi l'entité financière de sa capacité à évaluer les risques associés. De plus, comme les tiers prestataires de services informatiques fournissent souvent des services standardisés à différents types de clients, ces contrats ne répondent pas toujours de manière appropriée aux besoins individuels ou particuliers des acteurs du secteur financier.

(27) Malgré l'existence de règles générales sur l'externalisation dans certains actes législatifs de l'Union relatifs aux services financiers, le suivi de la dimension contractuelle n'est pas pleinement consacré dans la législation de l'Union. En l'absence de normes de l'Union claires et adaptées applicables aux accords contractuels conclus avec des tiers prestataires de services informatiques, la source extérieure du risque informatique n'est pas traitée de manière exhaustive. Par conséquent, il est nécessaire de définir certains principes clés pour encadrer la gestion, par les entités financières, du risque lié aux tiers prestataires de services informatiques, en les assortissant d'un ensemble de droits contractuels fondamentaux ayant trait à plusieurs éléments de l'exécution et de la résiliation des contrats, en vue de consacrer certaines garanties minimales renforçant la capacité des entités financières à assurer un suivi efficace de tous les risques qui se posent au niveau des tiers prestataires de services informatiques.

(28) Il existe un manque d'homogénéité et de convergence en ce qui concerne les risques liés aux tiers prestataires de services informatiques et la dépendance à l'égard de ceux-ci. Malgré certains efforts pour couvrir le domaine spécifique de l'externalisation, tels que les recommandations de 2017 sur l'externalisation vers des fournisseurs de services en nuage[34], la question du risque systémique qui peut être déclenché par l'exposition du secteur financier à un nombre limité de tiers prestataires critiques de services informatiques est à peine abordée dans la législation de l'Union. Cette lacune au niveau de l'Union est aggravée par l'absence de mandats et d'outils spécifiques qui permettraient aux autorités de surveillance nationales d'acquérir une solide compréhension des relations de dépendance à l'égard des tiers prestataires de services informatiques et d'assurer un suivi adéquat des risques découlant de la concentration de ces relations de dépendance.

[34] Recommandations sur l'externalisation vers des fournisseurs de services en nuage (EBA/REC/2017/03), désormais abrogées et remplacées par les orientations de l'ABE relatives à l'externalisation (EBA/GL/2019/02).

(29) Compte tenu des risques systémiques potentiels induits par les pratiques accrues d'externalisation et par la concentration des dépendances à l'égard des tiers prestataires de services informatiques, et eu égard à l'insuffisance des mécanismes nationaux permettant aux autorités de surveillance financière de quantifier et de qualifier les risques informatiques liés aux tiers prestataires critiques de services informatiques et de remédier à leurs conséquences, il est nécessaire de mettre en place au niveau de l'Union un cadre de supervision approprié permettant d'assurer un suivi continu des activités des tiers prestataires de services informatiques qui sont des prestataires critiques pour les entités financières.

(30) Face à la complexité et à la sophistication croissantes des menaces informatiques, l'efficacité des mesures de détection et de prévention dépend dans une large mesure de l'échange régulier de renseignements sur les menaces et les vulnérabilités entre les entités financières. Le partage d'informations contribue à accroître la sensibilisation aux cybermenaces, laquelle renforce à son tour la capacité des entités financières à empêcher les menaces de se concrétiser en incidents réels et leur permet de mieux contenir les effets des incidents liés à l'informatique et de se rétablir plus efficacement. En l'absence d'orientations au niveau de l'Union, plusieurs facteurs semblent avoir entravé ce partage de renseignements, notamment l'incertitude quant à la compatibilité avec les règles en matière de protection des données, de pratiques anticoncurrentielles et de responsabilité.

(31) En outre, les incertitudes quant au type d'informations qui peuvent être partagées avec d'autres acteurs du marché ou avec des autorités non chargées de la surveillance (telles que l'ENISA, à des fins d'analyse, ou Europol, à des fins répressives) aboutissent à la rétention d'informations utiles. L'étendue et la qualité du partage d'informations demeurent limitées et fragmentées, puisque les échanges pertinents ont lieu principalement au niveau local (dans le cadre d'initiatives nationales) et qu'il n'existe aucun dispositif cohérent de partage d'informations à l'échelle de l'Union adapté aux besoins d'un secteur financier intégré.

(32) Les entités financières devraient dès lors être encouragées à exploiter ensemble les connaissances et l'expérience pratique de chacune d'entre elles aux niveaux stratégique, tactique et opérationnel en vue de renforcer leur capacité à évaluer et surveiller de manière adéquate les cybermenaces, ainsi qu'à s'en prémunir et à y répondre. Il est donc nécessaire de favoriser l'émergence, au niveau de l'Union, de mécanismes volontaires de partage d'informations qui, employés dans des environnements de confiance, permettraient à la communauté financière de prévenir les menaces et d'y répondre collectivement en limitant rapidement la propagation des risques informatiques et en empêchant une éventuelle contagion à travers les canaux financiers. Ces mécanismes devraient être employés en parfaite conformité avec les règles applicables du droit de la concurrence de l'Union[35] ainsi que d'une manière qui garantisse le plein respect des règles de l'Union en matière de protection des données, principalement le règlement (UE) 2016/679 du Parlement européen et du Conseil[36], en particulier dans le cadre du traitement de données à caractère personnel qui est

[35] Communication de la Commission − Lignes directrices sur l'applicabilité de l'article 101 du traité sur le fonctionnement de l'Union européenne aux accords de coopération horizontale, 2011/C 11/01.

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

nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, tel que visé à l'article 6, paragraphe 1, point f), dudit règlement.

(33) Nonobstant la large couverture prévue par le présent règlement, l'application des règles en matière de résilience opérationnelle numérique devrait tenir compte des différences notables entre les entités financières du point de vue de la taille, des profils d'activité ou de l'exposition au risque numérique. En règle générale, lorsqu'elles allouent des ressources et des capacités à la mise en œuvre du cadre de gestion des risques informatiques, les entités financières devraient assurer un juste équilibre entre leurs besoins liés à l'informatique et leur taille et leur profil d'activité, tandis que les autorités compétentes devraient poursuivre l'évaluation et le réexamen de l'approche suivie pour cette répartition.

(34) Étant donné que les grandes entités financières tendent à disposer de ressources plus importantes et à être en mesure de mobiliser rapidement des fonds pour développer des structures de gouvernance et établir diverses stratégies d'entreprise, seules les entités financières qui ne sont pas des microentreprises au sens du présent règlement devraient être tenues de mettre en place des dispositifs de gouvernance plus complexes. Ces entités sont notamment mieux armées pour mettre en place des fonctions de gestion dédiées à la surveillance des accords avec les tiers prestataires de services informatiques ou à la gestion des crises, pour organiser leur gestion des risques informatiques selon le modèle reposant sur trois lignes de défense, ou pour adopter un document relatif aux ressources humaines exposant de manière exhaustive les politiques en matière de droits d'accès.

De même, seules ces entités financières devraient être tenues d'effectuer des évaluations approfondies après des changements majeurs dans les infrastructures de réseau et de système d'information et les procédures, de procéder régulièrement à des analyses de risque sur les systèmes informatiques patrimoniaux, ou d'étendre les tests des plans de continuité des activités et des plans de réponse et rétablissement pour tenir compte des scénarios de basculement depuis leur infrastructure informatique principale vers les installations redondantes.

(35) En outre, étant donné que seules les entités reconnues comme étant d'importance significative aux fins des tests de résilience numérique avancés devraient être tenues de procéder à des tests de pénétration fondés sur la menace, les processus administratifs et les coûts financiers induits par la réalisation de ces tests devraient être dévolus à un petit pourcentage d'entités financières. Enfin, en vue d'alléger les charges réglementaires, seules les entités financières qui ne sont pas des microentreprises devraient être priées de communiquer régulièrement aux autorités compétentes tous les coûts et pertes causés par des perturbations informatiques, ainsi que les résultats des examens post-incident effectués à la suite de perturbations informatiques importantes.

(36) Pour garantir un alignement complet et une cohérence globale entre les stratégies d'entreprise des entités financières, d'une part, et la mise en œuvre de la gestion des risques informatiques, d'autre part, l'organe de direction devrait être tenu de conserver un rôle actif et déterminant dans la conduite et l'adaptation du cadre de gestion des risques informatiques et de la stratégie globale de résilience numérique. L'approche adoptée par l'organe de direction devrait non seulement être axée sur les moyens de garantir la résilience des systèmes informatiques, mais également couvrir les personnes et les processus au travers d'un ensemble de politiques qui suscitent, à chaque niveau de l'entreprise et auprès de l'ensemble du personnel, une prise de

conscience aiguë des cyberrisques et un engagement à respecter une hygiène informatique rigoureuse à tous les niveaux.

La responsabilité ultime de l'organe de direction dans la gestion des risques informatiques d'une entité financière devrait constituer un principe fondamental de cette approche globale, concrétisé par l'engagement continu de l'organe de direction dans le contrôle du suivi de la gestion des risques informatiques.

(37) De plus, l'entière responsabilité de l'organe de direction va de pair avec la mobilisation d'investissements dans les TIC et d'un budget global suffisants pour permettre à l'entité financière d'atteindre son niveau de référence en matière de résilience opérationnelle numérique.

(38) S'inspirant des normes, lignes directrices, recommandations ou approches internationales, nationales et sectorielles pertinentes en matière de gestion du cyberrisque[37], le présent règlement promeut un ensemble de fonctions destinées à faciliter la structuration globale de la gestion des risques informatiques. Tant que les principales capacités mises en place par les entités financières permettent de répondre aux besoins associés aux objectifs poursuivis par les fonctions (identification, protection et prévention, détection, réponse et rétablissement, apprentissage et évolution et communication) définies dans le présent règlement, les entités financières restent libres d'utiliser des modèles de gestion des risques informatiques qui sont formulés ou classés différemment.

(39) Afin de rester en phase avec l'évolution des cybermenaces, les entités financières devraient maintenir des systèmes informatiques à jour qui soient fiables et dotés d'une capacité suffisante non seulement pour garantir le traitement des données nécessaire à la prestation de leurs services, mais aussi pour assurer une résilience technologique permettant aux entités financières de faire face de manière adéquate aux besoins de traitement supplémentaires qui pourraient résulter d'épisodes de tensions sur les marchés ou d'autres situations défavorables. Bien que le présent règlement ne requière aucune normalisation de systèmes, d'outils ou de technologies informatiques spécifiques, il repose sur le recours approprié, par les entités financières, aux normes techniques (par exemple, ISO) ou aux bonnes pratiques du secteur reconnues à l'échelle européenne et internationale, dans la mesure où ce recours est pleinement conforme aux instructions spécifiques des autorités de surveillance relatives à l'utilisation et à l'incorporation des normes internationales.

(40) Des plans efficaces de continuité des activités et de rétablissement sont nécessaires pour permettre aux entités financières de résoudre immédiatement et rapidement les incidents liés à l'informatique, en particulier les cyberattaques, en limitant les dégâts et en donnant la priorité à la reprise des activités et aux mesures de rétablissement. Toutefois, si les systèmes de sauvegarde doivent entamer le traitement sans retard injustifié, ce démarrage ne doit en aucun cas compromettre l'intégrité et la sécurité des réseaux et des systèmes d'information ni la confidentialité des données.

---

[37] CPIM-OICV, *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf G7, *Fundamental Elements of Cybersecurity for the Financial Sector*, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; Cadre de cybersécurité du NIST, https://www.nist.gov/cyberframework; CSF, *CIRR toolkit*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

(41) Si le présent règlement laisse aux entités financières une certaine latitude pour définir des objectifs en matière de délai de rétablissement et, partant, pour fixer ces objectifs en tenant pleinement compte de la nature et de la criticité de la fonction concernée et de tout besoin opérationnel spécifique, une évaluation des incidences globales potentielles sur l'efficience du marché devrait également être exigée lors de la détermination de ces objectifs.

(42) Les répercussions importantes des cyberattaques sont exacerbées lorsqu'elles se produisent dans le secteur financier, un domaine beaucoup plus à risque d'être la cible de propagateurs malveillants cherchant des gains financiers directement à la source. Pour atténuer ces risques et prévenir toute perte d'intégrité des systèmes informatiques, toute indisponibilité de ceux-ci, toute violation de données confidentielles ou tout dommage à l'infrastructure informatique physique, les entités financières devraient améliorer considérablement la notification des incidents majeurs liés à l'informatique.

La notification des incidents liés à l'informatique devrait être harmonisée pour toutes les entités financières en exigeant de celles-ci qu'elles les notifient seulement à leur autorité compétente. Toutes les entités financières seront soumises à cette obligation de notification, mais elles ne devraient pas toutes être concernées de la même manière, puisque les seuils d'importance significative et les délais pertinents devraient être fixés de manière à ne rendre compte que des incidents majeurs liés à l'informatique. La notification directe permettrait aux autorités de surveillance financière d'avoir accès aux informations sur les incidents liés à l'informatique. Néanmoins, les autorités de surveillance financière devraient transmettre ces informations aux autorités publiques non financières (autorités compétentes en matière de sécurité des réseaux et des systèmes d'information, autorités nationales de protection des données et services répressifs pour les incidents de nature criminelle). Les informations sur les incidents liés à l'informatique devraient être communiquées sur une base mutuelle: les autorités de surveillance financière devraient fournir tous les retours d'information ou orientations nécessaires à l'entité financière, tandis que les AES devraient partager des données anonymisées sur les menaces et les vulnérabilités liées à un événement afin de contribuer à la défense collective au sens large.

(43) Il conviendrait d'étudier la possibilité de centraliser les rapports sur les incidents liés à l'informatique en créant un pôle central de l'UE unique, qui soit recevrait directement les rapports pertinents et en informerait automatiquement les autorités nationales compétentes, soit se contenterait de centraliser les rapports que lui transmettraient les autorités nationales compétentes et assumerait un rôle de coordination. Les AES devraient être chargées d'élaborer, en consultation avec la BCE et l'ENISA, pour une certaine date, un rapport conjoint évaluant la faisabilité de la création d'un tel pôle central de l'UE.

(44) Dans le but de garantir une solide résilience opérationnelle numérique, et conformément aux normes internationales (par exemple, les éléments fondamentaux du G7 concernant les tests de pénétration fondés sur la menace), les entités financières devraient tester régulièrement leurs systèmes informatiques et leur personnel pour évaluer l'efficacité de leurs capacités de prévention, de détection, de réponse et de rétablissement, afin de repérer les vulnérabilités potentielles des TIC et d'y remédier. Afin de tenir compte des différences qui existent entre les sous-secteurs financiers et au sein de ceux-ci en ce qui concerne l'état de préparation des entités financières en matière de cybersécurité, les tests devraient comprendre un large éventail d'outils et d'actions, allant d'une évaluation des exigences de base (par exemple, évaluations et

analyses de la vulnérabilité, analyses des sources ouvertes, évaluations de la sécurité des réseaux, analyses des lacunes, examens de la sécurité physique, questionnaires et solutions logicielles d'analyse, examens du code source lorsque cela est possible, tests fondés sur des scénarios, tests de compatibilité, tests de performance ou tests de bout en bout) à des tests plus avancés (par exemple, tests de pénétration fondés sur la menace pour les entités financières suffisamment matures du point de vue des TIC pour être capables d'effectuer de tels tests). Les tests de résilience opérationnelle numérique devraient donc être plus exigeants pour les entités financières d'importance significative (telles que les grands établissements de crédit, les bourses, les dépositaires centraux de titres, les contreparties centrales, etc.) Dans le même temps, les tests de résilience opérationnelle numérique devraient être plus pertinents pour certains sous-secteurs qui jouent un rôle systémique essentiel (par exemple les paiements, les services bancaires, les services de compensation et de règlement), et moins pertinents pour d'autres sous-secteurs (par exemple, les gestionnaires d'actifs, les agences de notation de crédit, etc.) Les entités financières transfrontières qui exercent leur liberté d'établissement ou de prestation de services dans l'Union devraient se conformer à un ensemble unique d'exigences de tests avancés (tests de pénétration fondé sur la menace) dans leur État membre d'origine, et ces tests devraient englober toutes les infrastructures informatiques que ces groupes transfrontières détiennent dans les différentes juridictions dans lesquelles ils opèrent au sein de l'Union, ce qui leur permettrait de ne supporter les coûts associés aux tests que dans une seule juridiction.

(45) Afin d'assurer un suivi efficace du risque lié aux tiers prestataires de services informatiques, il convient d'établir un ensemble de règles de principe destinées à guider les entités financières dans le suivi des risques engendrés par l'externalisation de fonctions à des tiers prestataires de services informatiques et, plus généralement, par les relations de dépendance à l'égard de tiers prestataires de services informatiques.

(46) Une entité financière devrait à tout moment demeurer pleinement responsable du respect des obligations qui découlent du présent règlement. Un suivi proportionné des risques survenant au niveau du tiers prestataire de services informatiques devrait être assuré en tenant dûment compte de l'ampleur, de la complexité et de l'importance des relations de dépendance liées à l'informatique, de la criticité ou de l'importance des services, processus ou fonctions faisant l'objet des accords contractuels et, enfin, en procédant à une évaluation minutieuse de toute incidence potentielle sur la continuité et la qualité des services financiers au niveau individuel et au niveau du groupe, selon le cas.

(47) La réalisation de ce suivi devrait se fonder sur une approche stratégique du risque lié aux tiers prestataires de services informatiques, laquelle serait formalisée par l'adoption, par l'organe de direction de l'entité financière, d'une stratégie dédiée reposant sur une analyse continue de toutes les relations de dépendance à l'égard des tiers prestataires de services informatiques. Afin que les autorités de surveillance cernent mieux les relations de dépendance à l'égard de tiers prestataires de services informatiques, et en vue de consolider le cadre de supervision établi par le présent règlement, les autorités de surveillance financière devraient recevoir régulièrement des informations essentielles provenant des registres et devraient pouvoir en demander des extraits de manière ponctuelle.

(48) Une analyse précontractuelle approfondie devrait étayer et précéder la conclusion formelle des accords contractuels, tandis qu'un ensemble minimal de circonstances

révélant des insuffisances chez le tiers prestataire de services informatiques devrait déclencher la résiliation des contrats.

(49) Afin de remédier à l'effet systémique du risque de concentration des tiers prestataires de services informatiques, il convient de privilégier une solution équilibrée reposant sur une approche souple et progressive, car des plafonds rigides ou des limitations strictes seraient susceptibles d'entraver la conduite des affaires et la liberté contractuelle. Les entités financières devraient procéder à une évaluation rigoureuse des accords contractuels afin de déterminer la probabilité qu'un tel risque apparaisse, y compris au moyen d'analyses approfondies des accords de sous-externalisation, notamment lorsqu'ils sont conclus avec des tiers prestataires de services informatiques établis dans un pays tiers. À ce stade, et en vue de trouver un juste équilibre entre la nécessité de préserver la liberté contractuelle et celle de garantir la stabilité financière, il n'est pas jugé approprié de définir des plafonds et des limites stricts pour les expositions aux tiers prestataires de services informatiques. Il convient plutôt que l'AES désignée pour assurer la supervision de chaque tiers prestataire critique de services informatiques (le «superviseur principal») veille tout particulièrement, dans l'exercice de ses fonctions de supervision, à saisir pleinement l'ampleur des interdépendances et à détecter les cas spécifiques dans lesquels un degré élevé de concentration de tiers prestataires critiques de services informatiques dans l'Union est susceptible de mettre à mal la stabilité et l'intégrité du système financier de l'Union, et qu'elle prévoie un dialogue avec les tiers prestataires critiques de services informatiques lorsque ce risque est avéré[38].

(50) Afin de pouvoir évaluer et contrôler régulièrement la capacité du tiers prestataire de services informatiques à fournir en toute sécurité des services à l'entité financière sans effets préjudiciables sur la résilience de cette dernière, il convient d'harmoniser des éléments contractuels clés tout au long de l'exécution des contrats avec les tiers prestataires de services informatiques. Ces éléments couvrent uniquement les aspects contractuels minimaux considérés comme fondamentaux pour permettre à l'entité financière d'assurer un suivi complet dans le but de garantir sa résilience numérique, qui dépend de la stabilité et de la sécurité du service informatique.

(51) Les accords contractuels devraient notamment comporter une description complète des fonctions et des services, des lieux où ces fonctions sont assurées et où les données sont traitées, ainsi qu'une description complète des niveaux de service, accompagnée d'objectifs de performance quantitatifs et qualitatifs correspondant aux niveaux de service convenus, afin de permettre à l'entité financière de procéder à un suivi efficace. Dans le même ordre d'idées, les dispositions relatives à l'accessibilité, la disponibilité, l'intégrité, la sécurité et la protection des données à caractère personnel, ainsi que les garanties d'accès, de récupération et de restitution en cas d'insolvabilité, de résolution ou d'interruption des activités commerciales du tiers prestataire de services informatiques doivent également être considérées comme des éléments fondamentaux pour permettre à une entité financière d'assurer le suivi du risque lié aux tiers.

[38] En outre, si le risque d'abus par un tiers prestataire de services informatiques considéré comme dominant devait se matérialiser, les entités financières devraient également avoir la possibilité de déposer une plainte formelle ou informelle auprès de la Commission européenne ou des autorités nationales chargées du droit de la concurrence.

(52) Afin que les entités financières conservent la pleine maîtrise de toutes les évolutions susceptibles de nuire à leur sécurité informatique, il convient que soient définis les délais de préavis et les obligations de notification incombant au tiers prestataire de services informatiques en cas d'évolutions susceptibles d'avoir une incidence significative sur la capacité de ce dernier à remplir efficacement des fonctions critiques ou importantes, y compris la fourniture, sans frais supplémentaires ou à un coût déterminé ex ante, d'une assistance en cas d'incident lié à l'informatique.

(53) Les droits d'accès, d'inspection et d'audit accordés à l'entité financière ou à une tierce partie désignée constituent des outils essentiels pour permettre aux entités financières d'assurer un suivi permanent des performances du tiers prestataire de services informatiques, parallèlement à la coopération totale de ce dernier lors des inspections. Dans le même ordre d'idées, l'autorité compétente de l'entité financière devrait être habilitée, moyennant préavis, à inspecter et à auditer le tiers prestataire de services informatiques, dans le respect de la confidentialité.

(54) Les accords contractuels devraient établir des droits de résiliation clairs et des préavis minimaux correspondants, ainsi que des stratégies de sortie spécifiques prévoyant, en particulier, des périodes de transition obligatoires pendant lesquelles les tiers prestataires de services informatiques seraient tenus de continuer à assumer les fonctions concernées en vue de réduire le risque de perturbations au niveau de l'entité financière ou de permettre à celle-ci de changer de tiers prestataire de services informatiques, ou encore de recourir à des solutions sur site, en fonction de la complexité du service fourni.

(55) En outre, le recours volontaire aux clauses contractuelles types élaborées par la Commission pour les services d'informatique en nuage pourrait procurer un degré accru de confiance aux entités financières et à leurs tiers prestataires de services informatiques, en améliorant le niveau de sécurité juridique relatif à l'utilisation des services d'informatique en nuage par le secteur financier, dans le respect total des exigences et des attentes définies par la réglementation sur les services financiers. Ce travail s'appuie sur les mesures déjà envisagées dans le plan d'action 2018 pour les technologies financières, dans lequel la Commission a annoncé son intention d'encourager et de faciliter l'élaboration de clauses contractuelles types pour l'externalisation des activités d'informatique en nuage par les entités financières, en s'appuyant sur les efforts des parties prenantes de l'informatique en nuage au niveau transsectoriel, que la Commission a facilités grâce à la participation du secteur financier.

(56) Afin de promouvoir la convergence et l'efficacité des approches des autorités de surveillance en matière de risques liés aux tiers prestataires de services informatiques dans le secteur financier, de renforcer la résilience opérationnelle numérique des entités financières qui dépendent de tiers prestataires critiques de services informatiques pour l'exécution de fonctions opérationnelles, et de contribuer ainsi à préserver la stabilité du système financier de l'Union et l'intégrité du marché unique des services financiers, les tiers prestataires critiques de services informatiques devraient être soumis à un cadre de supervision de l'Union.

(57) Étant donné que seuls les tiers prestataires critiques de services nécessitent un traitement particulier, un mécanisme de désignation aux fins de l'application du cadre de supervision de l'Union devrait être mis en place pour tenir compte de la dimension et de la nature de la dépendance du secteur financier à l'égard de ces tiers prestataires de services informatiques. Ce mécanisme consisterait en un ensemble de critères

quantitatifs et qualitatifs qui définiraient les paramètres de criticité servant de référence aux fins de l'inclusion dans le cadre de supervision. Les tiers prestataires critiques de services informatiques qui ne sont pas automatiquement désignés par suite de l'application des critères susmentionnés devraient avoir la possibilité d'adhérer volontairement au cadre de supervision, tandis que les tiers prestataires de services informatiques qui sont déjà soumis à des cadres de supervision établis au niveau de l'Eurosystème à l'appui des missions énoncées à l'article 127, paragraphe 2, du traité sur le fonctionnement de l'Union européenne devraient par conséquent en être exemptés.

(58) L'exigence que les tiers prestataires de services informatiques qui ont été désignés comme critiques soient constitués dans l'Union n'équivaut pas à une localisation des données puisque le présent règlement ne comporte aucune autre exigence concernant le stockage ou le traitement des données à effectuer dans l'Union.

(59) Ce cadre devrait être sans préjudice de la compétence des États membres à mener leurs propres missions de supervision des tiers prestataires de services informatiques qui ne sont pas critiques au titre du présent règlement, mais qui pourraient être jugés importants au niveau national.

(60) Afin de tirer parti de l'architecture institutionnelle à plusieurs niveaux actuellement en place dans le domaine des services financiers, le comité mixte des AES devrait continuer à assurer la coordination intersectorielle globale pour toutes les questions relatives aux risques informatiques, conformément aux tâches qui lui incombent en matière de cybersécurité, avec le soutien d'un nouveau sous-comité (le forum de supervision) chargé de préparer aussi bien les décisions individuelles à l'adresse des tiers prestataires critiques de services informatiques que les recommandations collectives, en ce qui concerne notamment l'analyse comparative des programmes de supervision des tiers prestataires critiques de services informatiques et l'identification des bonnes pratiques pour parer aux risques de concentration informatique.

(61) Afin que les tiers prestataires de services informatiques qui jouent un rôle critique dans le fonctionnement du secteur financier fassent l'objet d'une supervision appropriée à l'échelle de l'Union, l'une des AES devrait être désignée comme superviseur principal pour chaque tiers prestataire critique de services informatiques.

(62) Les superviseurs principaux devraient être investis des pouvoirs nécessaires pour mener des enquêtes, des inspections sur place et hors site auprès des tiers prestataires critiques de services informatiques, accéder à tous les locaux et sites pertinents et obtenir des informations complètes et actualisées afin de leur permettre de se faire une idée précise du type, de la dimension et des incidences du risque que les tiers prestataires de services informatiques représentent pour les entités financières et, en définitive, pour le système financier de l'Union.

Il est indispensable de placer les AES à la tête de la supervision afin de cerner et de prendre en compte la dimension systémique du risque informatique dans le secteur financier. L'envergure dans l'Union des tiers prestataires critiques de services informatiques et les problèmes éventuels liés au risque de concentration informatique qui en découlent nécessitent l'adoption d'une approche collective au niveau de l'Union. Une multiplicité d'audits et de droits d'accès, exercés séparément par de nombreuses autorités compétentes avec une coordination limitée, voire inexistante, ne permettrait pas de disposer d'une vue d'ensemble exhaustive du risque lié aux tiers prestataires de services informatiques, tandis qu'elle engendrerait une redondance, des

charges et une complexité inutiles pour les tiers prestataires critiques de services informatiques confrontés à cette multiplicité des requêtes.

(63) En outre, les superviseurs principaux devraient avoir la possibilité de soumettre des recommandations sur les risques informatiques et les mesures correctives appropriées, y compris en s'opposant à certains accords contractuels susceptibles d'affecter à terme la stabilité de l'entité financière ou du système financier. Le respect de ces recommandations de fond formulées par les superviseurs principaux devrait être dûment pris en considération par les autorités nationales compétentes dans le cadre de leur fonction de surveillance prudentielle des entités financières.

(64) Le cadre de supervision ne remplace pas, ni ne se substitue en aucune façon, même partiellement, à la gestion, par les entités financières, du risque que comporte le recours à des tiers prestataires de services informatiques, y compris l'obligation d'assurer un suivi permanent de leurs accords contractuels conclus avec des tiers prestataires critiques de services informatiques, et ne change en rien l'entière responsabilité qui incombe aux entités financières de se conformer à toutes les exigences imposées par le présent règlement et par la législation applicable aux services financiers et de s'en acquitter. Afin d'éviter les doubles emplois et les chevauchements, les autorités compétentes devraient s'abstenir de prendre à titre individuel des mesures destinées à assurer le suivi des risques liés aux tiers prestataires critiques de services informatiques. Toute mesure de ce type devrait faire l'objet d'une coordination et d'un accord préalables dans le contexte du cadre de supervision.

(65) Dans le but de promouvoir la convergence au niveau international en ce qui concerne les bonnes pratiques à utiliser dans le cadre de l'examen de la gestion des risques numériques des tiers prestataires de services informatiques, les AES devraient être encouragées à conclure des accords de coopération avec les autorités compétentes de pays tiers en matière de surveillance et de réglementation afin de faciliter l'élaboration de bonnes pratiques pour parer aux risques liés aux tiers prestataires de services informatiques.

(66) Pour tirer parti de l'expertise technique des experts des autorités compétentes en matière de gestion des risques opérationnels et informatiques, les superviseurs principaux devraient s'appuyer sur l'expérience acquise au niveau national dans le domaine de la surveillance et mettre en place des équipes d'examen dédiées pour chaque tiers prestataire critique de services informatiques, en constituant des équipes multidisciplinaires pour contribuer à la préparation et à l'exécution effective des activités de supervision, y compris les inspections sur place auprès des tiers prestataires critiques de services informatiques, ainsi que les suites à leur donner.

(67) Les autorités compétentes devraient disposer de tous les pouvoirs de surveillance, d'enquête et de sanction nécessaires pour garantir l'application du présent règlement. Les sanctions administratives devraient, en principe, être rendues publiques. Étant donné que les entités financières et les tiers prestataires de services informatiques peuvent être établis dans des États membres différents et être soumis à la surveillance d'autorités compétentes sectorielles différentes, il convient d'assurer une coopération étroite entre les autorités compétentes concernées, y compris la BCE pour ce qui est des missions spécifiques qui lui sont conférées par le règlement (UE) nº 1024/2013 du

Conseil[39], ainsi qu'en consultation avec les AES, par l'échange réciproque d'informations et la fourniture d'une assistance mutuelle dans l'exercice des activités de surveillance.

(68) Afin de mieux quantifier et qualifier les critères de désignation des tiers prestataires critiques de services informatiques et d'harmoniser les redevances de supervision, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission afin de préciser: l'effet systémique qu'une défaillance d'un tiers prestataire de services informatiques pourrait avoir sur les entités financières auxquelles il fournit des services, le nombre d'établissements d'importance systémique mondiale (EISm) ou d'autres établissements d'importance systémique (autres EIS) qui dépendent du tiers prestataire de services informatiques concerné, le nombre de tiers prestataires de services informatiques actifs sur un marché spécifique, les coûts de la migration vers un autre tiers prestataire de services informatiques, le nombre d'États membres dans lesquels le tiers prestataire de services informatiques concerné fournit des services et dans lesquels les entités financières ayant recours au tiers prestataire de services informatiques concerné opèrent, ainsi que le montant des redevances de supervision et les modalités de leur paiement.

Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer»[40]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(69) Étant donné que le présent règlement, conjointement avec la directive (UE) 20xx/xx du Parlement européen et du Conseil[41], consiste en une consolidation des dispositions relatives à la gestion des risques informatiques énoncées dans de multiples règlements et directives de l'acquis de l'Union dans le domaine des services financiers, notamment les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014, il convient, afin de garantir une cohérence totale, de modifier lesdits règlements pour y préciser que les dispositions pertinentes applicables aux risques informatiques sont énoncées dans le présent règlement.

Des normes techniques devraient garantir l'harmonisation cohérente des exigences prévues par le présent règlement. Il convient de charger les AES, en tant qu'organismes dotés de compétences très spécialisées, d'élaborer des projets de normes techniques de réglementation n'impliquant pas de choix politiques, en vue de les soumettre à la Commission. Des normes techniques de réglementation devraient être élaborées dans les domaines de la gestion des risques informatiques, de la notification, des tests et des exigences clés pour garantir un suivi solide des risques liés aux tiers prestataires de services informatiques.

---

39 Règlement (UE) nº 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit (JO L 287 du 29.10.2013, p. 63).

40 JO L 123 du 12.5.2016, p. 1.

41 [*Veuillez insérer la référence complète*]

(70) Il est particulièrement important que la Commission procède aux consultations appropriées au cours de ses travaux préparatoires, y compris au niveau des experts. La Commission et les AES devraient veiller à ce que toutes les entités financières puissent appliquer ces normes et exigences d'une manière proportionnée à la nature, à l'échelle et de la complexité de ces entités et de leurs activités.

(71) Afin de faciliter la comparabilité des rapports sur les incidents majeurs liés à l'informatique et de garantir la transparence des accords contractuels relatifs à l'utilisation de services informatiques fournis par des tiers prestataires de services informatiques, les AES devraient être chargées d'élaborer des projets de normes techniques d'exécution établissant des modèles, des formulaires et des procédures normalisés permettant aux entités financières de signaler un incident majeur lié à l'informatique, ainsi que des modèles normalisés pour le registre d'informations. Lors de l'élaboration de ces normes, les AES devraient prendre en considération la taille et la complexité des entités financières, ainsi que la nature et le niveau de risque de leurs activités. La Commission devrait être habilitée à adopter ces normes techniques d'exécution au moyen d'actes d'exécution en vertu de l'article 291 du traité sur le fonctionnement de l'Union européenne et conformément à l'article 15 des règlements (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010. Étant donné que des exigences supplémentaires ont déjà été définies au moyen d'actes délégués et d'actes d'exécution fondés sur des normes techniques de réglementation ou des normes techniques d'exécution dans les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014, il convient de charger les AES, soit individuellement, soit conjointement par l'intermédiaire du comité mixte, de soumettre des normes techniques de réglementation et des normes techniques d'exécution à la Commission en vue de l'adoption d'actes délégués et d'actes d'exécution reprenant et actualisant les règles existantes en matière de gestion des risques informatiques.

(72) Cette démarche impliquera la modification ultérieure d'actes délégués et d'actes d'exécution existants adoptés dans différents domaines de la législation sur les services financiers. Le champ d'application des articles relatifs au risque opérationnel pour lesquels des délégations de pouvoirs dans ces actes prévoyaient l'adoption d'actes délégués et d'actes d'exécution devrait être modifié en vue de transférer dans le présent règlement toutes les dispositions relatives à la résilience opérationnelle numérique qui font actuellement partie de ces règlements.

(73) Étant donné que les objectifs du présent règlement, à savoir atteindre un niveau élevé de résilience opérationnelle numérique applicable à toutes les entités financières, ne peuvent pas être atteints de manière suffisante par les États membres, puisqu'ils supposent d'harmoniser une multitude de règles différentes qui figurent actuellement soit dans certains actes de l'Union, soit dans les systèmes juridiques des différents États membres, mais qu'ils peuvent, en raison de leurs dimensions et de leurs effets, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GENERALES

Article premier

Objet

1. Le présent règlement établit les exigences uniformes suivantes relatives à la sécurité des réseaux et des systèmes d'information sous-tendant les processus opérationnels des entités financières, nécessaires pour atteindre un niveau commun élevé de résilience opérationnelle numérique, comme suit:

   (a) les exigences applicables aux entités financières en ce qui concerne:

   – la gestion des risques liés aux technologies de l'information et de la communication (TIC);

   – la notification, aux autorités compétentes, des incidents majeurs liés à l'informatique;

   – les tests de résilience opérationnelle numérique;

   – le partage d'informations et de renseignements en rapport avec les cybermenaces et les cybervulnérabilités;

   – les mesures destinées à garantir une gestion solide, par les entités financières, du risque lié aux tiers prestataires de services informatiques;

   (b) les exigences relatives aux accords contractuels conclus entre des tiers prestataires de services informatiques et des entités financières;

   (c) le cadre de supervision applicable aux tiers prestataires critiques de services informatiques lorsqu'ils fournissent des services à des entités financières;

   (d) les règles relatives à la coopération entre les autorités compétentes et les règles relatives à la surveillance et à l'exécution par les autorités compétentes en ce qui concerne toutes les questions couvertes par le présent règlement.

2. S'agissant des entités financières identifiées en tant qu'opérateurs de services essentiels conformément aux dispositions nationales transposant l'article 5 de la directive (UE) 2016/1148, le présent règlement est considéré comme un acte juridique sectoriel de l'Union aux fins de l'article 1er, paragraphe 7, de ladite directive.

Article 2

Champ d'application personnel

1. Le présent règlement s'applique aux entités suivantes:

   (a) les établissements de crédit,

   (b) les établissements de paiement,

   (c) les établissements de monnaie électronique,

   (d) les entreprises d'investissement,

(e) les prestataires de services sur crypto-actifs, les émetteurs de crypto-actifs, les émetteurs de jetons se référant à un ou des actifs et les émetteurs de jetons se référant à un ou des actifs et revêtant une importance significative,

(f) les dépositaires centraux de titres,

(g) les contreparties centrales,

(h) les plates-formes de négociation,

(i) les référentiels centraux,

(j) les gestionnaires de fonds d'investissement alternatifs,

(k) les sociétés de gestion,

(l) les prestataires de services de communication de données,

(m) les entreprises d'assurance et de réassurance,

(n) les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire,

(o) les institutions de retraite professionnelle,

(p) les agences de notation de crédit,

(q) les contrôleurs légaux des comptes et les cabinets d'audit,

(r) les administrateurs d'indices de référence d'importance critique,

(s) les prestataires de services de financement participatif,

(t) les référentiels des titrisations,

(u) les tiers prestataires de services informatiques.

2. Aux fins du présent règlement, les entités visées au paragraphe 1, points a) à t), sont collectivement dénommées «entités financières».

Article 3

Définitions

Aux fins du présent règlement, on entend par:

(1) «résilience opérationnelle numérique»: la capacité d'une entité financière à développer, garantir et réévaluer son intégrité opérationnelle d'un point de vue technologique en assurant directement, ou indirectement par le recours aux services de tiers prestataires de services informatiques, l'intégralité des capacités liées à l'informatique nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité;

(2) «réseau et système d'information»: un réseau et système d'information au sens de l'article 4, point 1), de la directive (UE) 2016/1148;

(3) «sécurité des réseaux et des systèmes d'information»: la sécurité des réseaux et des systèmes d'information au sens de l'article 4, point 2), de la directive (UE) 2016/1148;

(4) «risque informatique»: toute circonstance raisonnablement identifiable liée à l'utilisation des réseaux et des systèmes d'information, – y compris un dysfonctionnement, un dépassement de capacité, une défaillance, une perturbation,

une altération, une mauvaise utilisation, une perte ou tout autre type d'événement, malveillant ou non – qui, si elle se concrétise, peut compromettre la sécurité des réseaux et des systèmes d'information, de tout outil ou processus dépendant de la technologie, du fonctionnement et de l'exécution des processus ou de la fourniture de services, compromettant ainsi l'intégrité ou la disponibilité des données, des logiciels ou de tout autre composante des services et infrastructures informatiques, ou entraînant une violation de la confidentialité, un dommage à l'infrastructure informatique physique ou d'autres effets préjudiciables;

(5) «actif d'information»: un ensemble d'informations, matérielles ou immatérielles, qui justifie une protection;

(6) «incident lié à l'informatique»: un événement imprévu détecté dans les réseaux et les systèmes d'information, qu'il résulte ou non d'une activité malveillante, qui compromet la sécurité des réseaux et des systèmes d'information, des informations que ces systèmes traitent, stockent ou transmettent, ou qui a des effets préjudiciables sur la disponibilité, la confidentialité, la continuité ou l'authenticité des services financiers fournis par l'entité financière;

(7) «incident majeur lié à l'informatique»: un incident lié à l'informatique ayant une incidence négative potentiellement élevée sur les réseaux et les systèmes d'information qui sous-tendent les fonctions critiques de l'entité financière;

(8) «cybermenace»: une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881 du Parlement européen et du Conseil[42];

(9) «cyberattaque»: un incident lié à l'informatique malveillant résultant d'une tentative de destruction, d'exposition, de modification, de désactivation, de vol, d'utilisation non autorisée d'un actif ou d'accès non autorisé à celui-ci, perpétrée par un acteur de la menace;

(10) «renseignements sur les menaces»: les informations qui ont été rassemblées, transformées, analysées, interprétées ou enrichies pour fournir le contexte nécessaire à la prise de décisions et qui apportent une compréhension pertinente et suffisante en vue d'atténuer les effets d'un incident lié à l'informatique ou d'une cybermenace, y compris les détails techniques d'une cyberattaque, les responsables de l'attaque, ainsi que leur mode opératoire et leurs motivations;

(11) «défense en profondeur»: une stratégie liée à l'informatique intégrant des personnes, des processus et des technologies afin d'établir des barrières diverses à travers les multiples couches et dimensions de l'entité;

(12) «vulnérabilité»: une faiblesse, une susceptibilité ou un défaut d'un actif, d'un système, d'un processus ou d'un contrôle qui peuvent être exploités par une menace;

(13) «tests de pénétration fondés sur la menace»: un cadre simulant les tactiques, les techniques et les procédures d'acteurs de la menace réels perçus comme représentant une véritable cybermenace, qui permet de tester de manière contrôlée, sur mesure et en fonction des renseignements (red team) les systèmes de production en direct critiques de l'entité;

[42] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

(14) «risque lié aux tiers prestataires de services informatiques»: risque informatique auquel une entité financière peut être exposée du fait de son recours à des services informatiques fournis par des tiers prestataires de services informatiques ou par des sous-traitants de ces derniers;

(15) «tiers prestataire de services informatiques»: une entreprise qui fournit des services numériques et de données, y compris les fournisseurs de services d'informatique en nuage, de logiciels, de services d'analyse de données, de centres de données, mais à l'exclusion des fournisseurs de composants matériels et des entreprises agréées en vertu du droit de l'Union qui fournissent des services de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972 du Parlement européen et du Conseil[43];

(16) «services informatiques»: les services numériques et de données fournis par l'intermédiaire des systèmes informatiques à un ou plusieurs utilisateurs internes ou externes, dont la fourniture de données, la saisie de données, le stockage de données, le traitement des données et les services de notification, le suivi des données ainsi que les services de soutien opérationnel et décisionnel fondés sur les données;

(17) «fonction critique ou importante»: une fonction dont une interruption, une anomalie ou une défaillance de l'exécution est susceptible de nuire sérieusement à la capacité d'une entité financière de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables de la législation sur les services financiers, ou à sa performance financière ou à la solidité ou la continuité de ses services et activités;

(18) «tiers prestataire critique de services informatiques»: un tiers prestataire de services informatiques désigné conformément à l'article 29 et soumis au cadre de supervision visé aux articles 30 à 37;

(19) «tiers prestataire de services informatiques établi dans un pays tiers»: un tiers prestataire de services informatiques qui est une personne morale établie dans un pays tiers, qui n'a pas établi d'activité ou de présence dans l'Union et qui a conclu un accord contractuel avec une entité financière pour la fourniture de services informatiques;

(20) «sous-traitant informatique établi dans un pays tiers»: un sous-traitant informatique qui est une personne morale établie dans un pays tiers, qui n'a pas établi d'activité ou de présence dans l'Union et qui a conclu un accord contractuel soit avec un tiers prestataire de services informatiques, soit avec un tiers prestataire de services informatiques établi dans un pays tiers;

(21) «risque de concentration informatique»: une exposition à des tiers prestataires critiques de services informatiques individuels ou multiples et liés, créant un degré de dépendance à l'égard de ces prestataires, de sorte que l'indisponibilité, la défaillance ou tout autre type d'insuffisance de ces derniers peut potentiellement mettre en péril la capacité d'une entité financière, et en fin de compte du système financier de l'Union dans son ensemble, à assurer des fonctions critiques, ou à faire face à d'autres types d'effets préjudiciables, y compris des pertes importantes;

[43] Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

(22) «organe de direction»: un organe de direction au sens de l'article 4, paragraphe 1, point 36), de la directive 2014/65/UE, de l'article 3, paragraphe 1, point 7), de la directive 2013/36/UE, de l'article 2, paragraphe 1, point s), de la directive 2009/65/CE, de l'article 2, paragraphe 1, point 45), du règlement (UE) nº 909/2014, de l'article 3, paragraphe 1, point 20), du règlement (UE) 2016/1011 du Parlement européen et du Conseil[44], de l'article 3, paragraphe 1, point u), du règlement (UE) 20xx/xx du Parlement européen et du Conseil[45] [MICA] ou les personnes assimilées qui dirigent effectivement l'entité ou qui exercent des fonctions clés conformément à la législation de l'Union ou nationale applicable;

(23) «établissement de crédit»: un établissement de crédit au sens de l'article 4, paragraphe 1, point 1), du règlement (UE) nº 575/2013 du Parlement européen et du Conseil[46];

(24) «entreprise d'investissement»: une entreprise d'investissement au sens de l'article 4, paragraphe 1, point 1), de la directive 2014/65/UE;

(25) «établissement de paiement»: un établissement de paiement au sens de l'article 1er, paragraphe 1, point d), de la directive (UE) 2015/2366;

(26) «établissement de monnaie électronique»: un établissement de monnaie électronique au sens de l'article 2, point 1), de la directive 2009/110/CE du Parlement européen et du Conseil[47];

(27) «contrepartie centrale»: une contrepartie centrale au sens de l'article 2, point 1) du règlement (UE) nº 648/2012;

(28) «référentiel central»: un référentiel central au sens de l'article 2, point 2), du règlement (UE) nº 648/2012;

(29) «dépositaire central de titres»: un dépositaire central de titres au sens de l'article 2, paragraphe 1, point 1), du règlement (UE) nº 909/2014;

(30) «plate-forme de négociation»: une plate-forme de négociation au sens de l'article 4, paragraphe 1, point 24), de la directive 2014/65/UE;

(31) «gestionnaire de fonds d'investissement alternatifs»: un gestionnaire de fonds d'investissement alternatifs au sens de l'article 4, paragraphe 1, point b), de la directive 2011/61/UE;

(32) «société de gestion»: une société de gestion au sens de l'article 2, paragraphe 1, point b), de la directive 2009/65/CE;

---

44 Règlement (UE) 2016/1011 du Parlement européen et du Conseil du 8 juin 2016 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement et modifiant les directives 2008/48/CE et 2014/17/UE et le règlement (UE) nº 596/2014 (JO L 171 du 29.6.2016, p. 1).

45 [*veuillez insérer le titre complet et la référence du JO*]

46 Règlement (UE) nº 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) nº 648/2012 (JO L 176 du 27.6.2013, p. 1).

47 Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE (JO L 267 du 10.10.2009, p. 7).

(33) «prestataire de services de communication de données»: un prestataire de services de communication de données au sens de l'article 4, paragraphe 1, point 63), de la directive 2014/65/UE;

(34) «entreprise d'assurance»: une entreprise d'assurance au sens de l'article 13, point 1), de la directive 2009/138/CE;

(35) «entreprise de réassurance»: une entreprise de réassurance au sens de l'article 13, point 4), de la directive 2009/138/CE;

(36) «intermédiaire d'assurance»: un intermédiaire d'assurance au sens de l'article 2, point 3), de la directive (UE) 2016/97;

(37) «intermédiaire d'assurance à titre accessoire»: un intermédiaire d'assurance à titre accessoire au sens de l'article 2, point 4), de la directive (UE) 2016/97;

(38) «intermédiaire de réassurance»: un intermédiaire de réassurance au sens de l'article 2, point 5), de la directive (UE) 2016/97;

(39) «institution de retraite professionnelle»: une institution de retraite professionnelle au sens de l'article 6, point 1), de la directive (UE) 2016/2341;

(40) «agence de notation de crédit»: une agence de notation de crédit au sens de l'article 3, paragraphe 1, point a), du règlement (CE) nº 1060/2009;

(41) «contrôleur légal des comptes»: un contrôleur légal des comptes au sens de l'article 2, point 2), de la directive 2006/43/CE;

(42) «cabinet d'audit»: un cabinet d'audit au sens de l'article 2, point 3), de la directive 2006/43/CE;

(43) «prestataire de services sur crypto-actifs»: un prestataire de services sur crypto-actifs au sens de l'article 3, paragraphe 1, point n), du règlement (UE) 202x/xx [*OP: insérer la référence du règlement MICA*];

(44) «émetteur de crypto-actifs»: un émetteur de crypto-actifs au sens de l'article 3, paragraphe 1, point h), du [*JO: insérer la référence du règlement MICA*];

(45) «émetteur de jetons se référant à un ou des actifs»: un émetteur de jetons se référant à un ou des actifs au sens de l'article 3, paragraphe 1, point i), du [*JO: insérer la référence du règlement MICA*];

(46) «émetteur de jetons se référant à un ou des actifs et revêtant une importance significative»: un émetteur de jetons se référant à un ou des actifs et revêtant une importance significative au sens de l'article 3, paragraphe 1, point j), du [*JO: insérer la référence du règlement MICA*];

(47) «administrateur d'indices de référence d'importance critique»: un administrateur d'indices de référence d'importance critique au sens de l'article x, point x), du règlement xx/202x [*JO: insérer la référence du règlement sur les indices de référence*];

(48) «prestataire de services de financement participatif»: un prestataire de services de financement participatif au sens de l'article x, point x), du règlement (UE) 202x/xx [*OP: insérer la référence du règlement sur le financement participatif*];

(49) «référentiel des titrisations»: un référentiel des titrisations au sens de l'article 2, point 23), du règlement (UE) 2017/2402;

(50) «microentreprise»: une entité financière au sens de l'article 2, paragraphe 3, de l'annexe de la recommandation 2003/361/CE.

CHAPITRE II

GESTION DES RISQUES INFORMATIQUES

SECTION 1

Article 4

Gouvernance et organisation

1. Les entités financières disposent de cadres de gouvernance et de contrôle internes qui garantissent une gestion efficace et prudente de tous les risques informatiques.

2. L'organe de direction de l'entité financière définit, approuve, supervise et est responsable de la mise en œuvre de toutes les dispositions relatives au cadre de gestion des risques informatiques visé à l'article 5, paragraphe 1.

   Aux fins du premier alinéa, l'organe de direction:

   (a) assume la responsabilité finale de la gestion des risques informatiques de l'entité financière;

   (b) définit clairement les rôles et les responsabilités pour toutes les fonctions liées à l'informatique;

   (c) détermine le niveau approprié de tolérance au risque informatique de l'entité financière, tel que visé à l'article 5, paragraphe 9, point b);

   (d) approuve, supervise et examine périodiquement la mise en œuvre de la politique de continuité des activités informatiques de l'entité financière et du plan de rétablissement après sinistre informatique, visés à l'article 10, respectivement au paragraphe 1 et au paragraphe 3;

   (e) approuve et examine périodiquement les plans d'audit informatique, les audits informatiques et les modifications significatives qui y sont apportées;

   (f) alloue et réexamine périodiquement le budget approprié pour satisfaire les besoins de l'entité financière en matière de résilience opérationnelle numérique pour tous les types de ressources, y compris la formation sur les risques informatiques et les compétences en la matière pour l'ensemble du personnel concerné;

   (g) approuve et examine périodiquement la politique de l'entité financière concernant les modalités d'utilisation des services informatiques fournis par des tiers prestataires de services informatiques;

   (h) est dûment informé des accords conclus avec des tiers prestataires de services informatiques sur l'utilisation des services informatiques, de tout changement significatif pertinent prévu concernant les tiers prestataires de services informatiques, et des incidences potentielles de ces changements sur les fonctions critiques ou importantes faisant l'objet de ces accords, et reçoit notamment un résumé de l'analyse des risques visant à évaluer les incidences de ces changements;

(i) est dûment informé des incidents liés à l'informatique et de leur incidence, ainsi que des mesures de réponse, de rétablissement et de correction.

3. Les entités financières autres que les microentreprises instituent un rôle de suivi des accords conclus avec des tiers prestataires de services informatiques sur l'utilisation des services informatiques, ou désignent un membre de la direction générale chargé de superviser l'exposition aux risques connexe et la documentation pertinente.

4. Les membres de l'organe de direction suivent régulièrement une formation spécifique afin d'acquérir et de maintenir à jour des connaissances et des compétences suffisantes pour comprendre et évaluer les risques informatiques et leur incidence sur les opérations de l'entité financière.

SECTION II

Article 5

Cadre de gestion des risques informatiques

1. Les entités financières disposent d'un cadre de gestion des risques informatiques solide, complet et bien documenté, qui leur permet de parer aux risques informatiques de manière rapide, efficiente et exhaustive et de garantir un niveau élevé de résilience opérationnelle numérique conforme aux besoins, à la taille et à la complexité de leurs activités.

2. Le cadre de gestion des risques informatiques visé au paragraphe 1 englobe les stratégies, les politiques, les procédures, les protocoles et les outils informatiques qui sont nécessaires pour protéger dûment et efficacement toutes les composantes et infrastructures physiques pertinentes, y compris le matériel informatique, les serveurs, ainsi que tous les locaux, centres de données et zones sensibles désignées pertinents, afin de garantir que tous ces éléments physiques sont correctement protégés contre les risques, y compris les dommages et les accès ou utilisations non autorisés.

3. Les entités financières réduisent au minimum l'incidence des risques informatiques en déployant des stratégies, des politiques, des procédures, des protocoles et des outils adéquats, tels que définis dans le cadre de gestion des risques informatiques. Elles fournissent des informations complètes et actualisées sur les risques informatiques, conformément aux exigences des autorités compétentes.

4. Aux fins du cadre de gestion des risques informatiques visé au paragraphe 1, les entités financières autres que les microentreprises mettent en œuvre un système de gestion de la sécurité de l'information fondé sur des normes internationales reconnues et conforme aux orientations des autorités de surveillance, et le réexaminent régulièrement.

5. Les entités financières autres que les microentreprises garantissent une séparation adéquate des fonctions de gestion informatique, des fonctions de contrôle et des fonctions d'audit interne, selon le modèle reposant sur trois lignes de défense, ou un modèle de gestion des risques et de contrôle internes.

6. Le cadre de gestion des risques informatiques visé au paragraphe 1 est documenté et réexaminé au moins une fois par an, ainsi qu'en cas de survenance d'incidents majeurs liés à l'informatique, et conformément aux instructions des autorités de surveillance ou aux conclusions tirées des tests de résilience opérationnelle

numérique ou des processus d'audit pertinents. Il est amélioré en permanence sur la base des enseignements tirés de la mise en œuvre et du suivi.

7. Le cadre de gestion des risques informatiques visé au paragraphe 1 fait l'objet d'audits réguliers réalisés par des auditeurs informatiques qui possèdent des connaissances, des compétences et une expertise suffisantes en matière de risques informatiques. La fréquence et le point de mire des audits informatiques sont proportionnés aux risques informatiques de l'entité financière.

8. Un processus de suivi formel, comprenant des règles pour la vérification et la correction rapides des constatations d'importance critique de l'audit informatique, est établi, en tenant compte des conclusions de l'audit et en prenant dûment en considération la nature, l'ampleur et la complexité des services et des activités des entités financières.

9. Le cadre de gestion des risques informatiques visé au paragraphe 1 comprend une stratégie de résilience numérique qui définit les modalités de mise en œuvre du cadre. À cet effet, il précise les méthodes pour parer aux risques informatiques et atteindre des objectifs informatiques spécifiques, en:

   (a) expliquant la manière dont le cadre de gestion des risques informatiques appuie la stratégie d'entreprise et les objectifs opérationnels de l'entité financière;

   (b) déterminant le niveau de tolérance au risque informatique, en fonction de l'appétit pour le risque de l'entité financière, et en analysant la tolérance à l'incidence des perturbations informatiques;

   (c) définissant des objectifs clairs en matière de sécurité de l'information;

   (d) décrivant l'architecture informatique de référence et les changements nécessaires pour atteindre des objectifs opérationnels spécifiques;

   (e) présentant les différents mécanismes mis en place pour détecter et prévenir les incidents liés à l'informatique, ainsi que pour se protéger contre leurs effets;

   (f) déterminant le nombre d'incidents majeurs liés à l'informatique et l'efficacité des mesures de prévention;

   (g) définissant une stratégie globale multi-fournisseurs en matière de technologies de l'information et de la communication au niveau de l'entité, qui met en évidence les principales relations de dépendance à l'égard des tiers prestataires de services informatiques et expose les raisons qui sous-tendent la combinaison de tiers prestataires de services choisis;

   (h) mettant en œuvre des tests de résilience opérationnelle numérique;

   (i) définissant une stratégie de communication en cas d'incidents liés à l'informatique.

10. Sur approbation des autorités compétentes, les entités financières peuvent déléguer les tâches de vérification du respect des exigences en matière de gestion des risques informatiques à des entreprises intra-groupe ou externes.

Article 6

Systèmes, protocoles et outils informatiques

1. Les entités financières utilisent et tiennent à jour des systèmes, protocoles et outils informatiques qui satisfont aux conditions suivantes:

   (a) les systèmes et les outils sont adaptés à la nature, à la variété, à la complexité et à l'ampleur des opérations qui sous-tendent l'exercice de leurs activités;

   (b) ils sont fiables;

   (c) ils disposent d'une capacité suffisante pour traiter avec exactitude les données nécessaires à l'exécution des activités et à la fourniture des services en temps voulu, et pour faire face aux pics de volume d'ordres, de messages ou de transactions, selon les besoins, y compris en cas de mise en place de nouvelles technologies;

   (d) ils sont suffisamment résilients sur le plan technologique pour répondre de manière adéquate aux besoins supplémentaires de traitement de l'information qui apparaissent en situation de tensions sur les marchés ou dans d'autres situations défavorables.

2. Lorsque les entités financières ont recours à des normes techniques reconnues au niveau international et des bonnes pratiques du secteur en matière de sécurité de l'information et de contrôles internes informatiques, elles utilisent ces normes et pratiques conformément aux recommandations pertinentes des autorités de surveillance relatives à leur incorporation.

Article 7

Identification

1. Aux fins du cadre de gestion des risques informatiques visé à l'article 5, paragraphe 1, les entités financières identifient, classent et documentent de manière adéquate toutes les fonctions opérationnelles liées à l'informatique, les actifs d'information qui appuient ces fonctions, ainsi que les configurations des systèmes informatiques et les interconnexions avec les systèmes informatiques internes et externes. Les entités financières examinent si nécessaire, et au moins une fois par an, le caractère adéquat de la classification des actifs d'information et de toute documentation pertinente.

2. Les entités financières identifient de manière continue toutes les sources de risque informatique, en particulier l'exposition au risque vis-à-vis d'autres entités financières et émanant de celles-ci, et évaluent les cybermenaces et les vulnérabilités informatiques qui concernent leurs fonctions opérationnelles et leurs actifs d'information liés à l'informatique. Les entités financières examinent régulièrement, et au moins une fois par an, les scénarios de risque qui ont des incidences sur elles.

3. Les entités financières autres que les microentreprises procèdent à une évaluation des risques à chaque modification importante de l'infrastructure du réseau et du système d'information, des processus ou des procédures, qui affecte leurs fonctions, leurs processus de soutien ou leurs actifs d'information.

4. Les entités financières identifient tous les comptes des systèmes informatiques, y compris ceux situés sur des sites extérieurs, les ressources du réseau et les équipements matériels, et répertorient les équipements physiques considérés comme

critiques. Elles répertorient la configuration des actifs informatiques et les liens et interdépendances entre les différents actifs informatiques.

5. Les entités financières identifient et documentent tous les processus qui dépendent de tiers prestataires de services informatiques, et identifient les interconnexions avec des tiers prestataires de services informatiques.

6. Aux fins des paragraphes 1, 4 et 5, les entités financières tiennent des inventaires pertinents et les mettent régulièrement à jour.

7. Les entités financières autres que les microentreprises procèdent régulièrement, et au moins une fois par an, à une évaluation spécifique des risques informatiques sur tous les systèmes informatiques patrimoniaux, en particulier avant et après la connexion d'anciens et de nouveaux systèmes, applications ou technologies.

Article 8

Protection et prévention

1. Aux fins de la protection adéquate des systèmes informatiques et en vue d'organiser les mesures de réponse, les entités financières assurent un suivi et un contrôle permanents du fonctionnement des systèmes et outils informatiques et réduisent au minimum l'incidence de ces risques par le déploiement d'outils, de stratégies et de procédures appropriés en matière de sécurité informatique.

2. Les entités financières conçoivent, acquièrent et mettent en œuvre des stratégies, des politiques, des procédures, des protocoles et des outils de sécurité informatique qui visent, en particulier, à garantir la résilience, la continuité et la disponibilité des systèmes informatiques, et à maintenir des normes élevées en matière de sécurité, de confidentialité et d'intégrité des données, que ce soit au repos, en cours d'utilisation ou en transit.

3. Pour atteindre les objectifs visés au paragraphe 2, les entités financières utilisent des technologies et des processus informatiques de pointe qui:

   (a) garantissent la sécurité des moyens de transfert d'informations;

   (b) réduisent au minimum le risque de corruption ou de perte de données, d'accès non autorisé et de défauts techniques susceptibles d'entraver les activités;

   (c) empêchent les fuites d'informations;

   (d) garantissent que les données sont protégées contre les risques liés à une mauvaise administration ou à un mauvais traitement, y compris une tenue de registre inadéquate.

4. Aux fins du cadre de gestion des risques informatiques visé à l'article 5, paragraphe 1, les entités financières:

   (a) élaborent et documentent une politique de sécurité de l'information qui définit des règles visant à protéger la confidentialité, l'intégrité et la disponibilité de leurs ressources, de leurs données et de leurs actifs d'information liés à l'informatique, ainsi que de ceux de leurs clients;

   (b) instaurent, selon une approche fondée sur les risques, une gestion solide des réseaux et des infrastructures en recourant aux techniques, aux méthodes et aux protocoles appropriés, notamment en mettant en œuvre des mécanismes

automatisés pour isoler les actifs d'information affectés en cas de cyberattaques;

(c) mettent en œuvre des politiques qui limitent l'accès physique et virtuel aux ressources et aux données des systèmes informatiques à ce qui est nécessaire uniquement pour les fonctions et les activités légitimes et approuvées, et définissent à cet effet un ensemble de politiques, de procédures et de contrôles qui portent sur les privilèges d'accès et leur bonne administration;

(d) mettent en œuvre des politiques et des protocoles pour des mécanismes d'authentification forte, fondés sur des normes pertinentes et des systèmes de contrôle dédiés pour empêcher l'accès aux clés cryptographiques par lesquelles les données sont chiffrées sur la base des résultats des processus approuvés de classification des données et d'évaluation des risques;

(e) mettent en œuvre des politiques, des procédures et des contrôles pour la gestion des changements informatiques, y compris les changements apportés aux logiciels, au matériel, aux composants de micrologiciels, aux systèmes ou à la sécurité, qui sont fondés sur une approche d'évaluation des risques et font partie intégrante du processus global de gestion des changements de l'entité financière, afin de garantir que tous les changements apportés aux systèmes informatiques sont consignés, testés, évalués, approuvés, mis en œuvre et vérifiés de manière contrôlée;

(f) disposent de stratégies appropriées et globales en matière de correctifs et de mises à jour.

Aux fins du point b), les entités financières conçoivent l'infrastructure de connexion au réseau de manière à permettre une déconnexion instantanée et assurent sa compartimentation et sa segmentation, afin de réduire au minimum la contagion et de la prévenir, en particulier pour les processus financiers interconnectés.

Aux fins du point e), le processus de gestion des changements informatiques est approuvé par la structure hiérarchique appropriée et comporte des protocoles spécifiques activés pour les changements en urgence.

Article 9

Détection

1. Les entités financières mettent en place des mécanismes permettant de détecter rapidement les activités anormales, conformément à l'article 15, y compris les problèmes de performance des réseaux informatiques et les incidents liés à l'informatique, ainsi que de repérer tous les points uniques de défaillance potentiellement significatifs.

   Tous les mécanismes de détection visés au premier alinéa sont régulièrement testés conformément à l'article 22.

2. Les mécanismes de détection visés au paragraphe 1 permettent la mise en place de plusieurs niveaux de contrôle, définissent des seuils d'alerte et des critères de déclenchement des processus de détection des incidents liés à l'informatique et de réponse en cas d'incident lié à l'informatique, et comprennent des mécanismes d'alerte automatique destinés au personnel compétent chargé de la réponse aux incidents liés à l'informatique.

3. Les entités financières consacrent des ressources et des capacités suffisantes, en tenant dûment compte de leur taille, de leur activité et de leur profil de risque, pour surveiller l'activité des utilisateurs, l'apparition d'anomalies informatiques et d'incidents liés à l'informatique, en particulier les cyberattaques.

4. Les entités financières visées à l'article 2, paragraphe 1, point l), disposent en outre de systèmes capables de vérifier efficacement l'exhaustivité des déclarations de transactions, de repérer les omissions et les erreurs manifestes et de demander une nouvelle transmission des déclarations erronées le cas échéant.

Article 10

Réponse et rétablissement

1. Aux fins du cadre de gestion des risques informatiques visé à l'article 5, paragraphe 1, et sur la base des exigences en matière d'identification énoncées à l'article 7, les entités financières se dotent d'une politique de continuité des activités informatiques dédiée et complète, qui fait partie intégrante de leur politique de continuité des activités opérationnelles.

2. Les entités financières mettent en œuvre la politique de continuité des activités informatiques visée au paragraphe 1 au moyen de dispositifs, de plans, de procédures et de mécanismes dédiés, appropriés et documentés visant à:

   (a) consigner tous les incidents liés à l'informatique;

   (b) garantir la continuité des fonctions critiques de l'entité financière;

   (c) répondre aux incidents liés à l'informatique et les résoudre rapidement, dûment et efficacement, en particulier, mais pas uniquement, en cas de cyberattaques, de manière à limiter les dommages et à donner la priorité à la reprise des activités et aux mesures de rétablissement;

   (d) activer sans délai des plans dédiés permettant de déployer des mesures, des processus et des technologies d'endiguement adaptés à chaque type d'incident lié à l'informatique et de prévenir tout dommage supplémentaire, ainsi que des procédures sur mesure de réponse et rétablissement, définies conformément à l'article 11;

   (e) estimer les incidences, les dommages et les pertes préliminaires;

   (f) définir des mesures de communication et de gestion des crises qui garantissent la transmission d'informations actualisées à tous les membres du personnel interne et les parties prenantes externes concernés, conformément à l'article 13, et leur communication aux autorités compétentes, conformément à l'article 17.

3. Aux fins du cadre de gestion des risques informatiques visé à l'article 5, paragraphe 1, les entités financières mettent en œuvre un plan de rétablissement après sinistre informatique, qui, dans le cas des entités financières autres que les microentreprises, fait l'objet d'un audit indépendant.

4. Les entités financières mettent en place, maintiennent et testent périodiquement des plans de continuité des activités informatiques appropriés, notamment en ce qui concerne les fonctions critiques ou importantes externalisées ou sous-traitées dans le cadre d'accords avec des tiers prestataires de services informatiques.

5. Dans le cadre de leur gestion globale des risques informatiques, les entités financières:

(a) testent la politique de continuité des activités informatiques et le plan de rétablissement après sinistre informatique au moins une fois par an et après l'apport de modifications substantielles aux systèmes informatiques;

(b) testent les plans de communication en situation de crise établis conformément à l'article 13.

Aux fins du point a), les entités financières autres que les microentreprises incluent dans les plans de test des scénarios de cyberattaques et de basculement entre l'infrastructure informatique principale et la capacité redondante, les sauvegardes et les installations redondantes nécessaires pour satisfaire aux obligations énoncées à l'article 11.

Les entités financières réexaminent régulièrement leur politique de continuité des activités informatiques et leur plan de rétablissement après sinistre informatique en tenant compte des résultats des tests effectués conformément au premier alinéa et des recommandations découlant des contrôles d'audit ou des examens des autorités de surveillance.

6. Les entités financières autres que les microentreprises disposent d'une fonction de gestion de crise qui, en cas d'activation de leur politique de continuité des activités informatiques ou de leur plan de rétablissement après sinistre informatique, définit des procédures claires pour gérer les communications internes et externes en situation de crise, conformément à l'article 13.

7. Les entités financières tiennent un registre des activités avant et pendant les perturbations lorsque leur politique de continuité des activités informatiques ou leur plan de rétablissement après sinistre informatique est activé. Ces registres sont facilement accessibles.

8. Les entités financières visées à l'article 2, paragraphe 1, point f), fournissent aux autorités compétentes des copies des résultats des tests de continuité des activités informatiques ou d'exercices similaires réalisés au cours de la période considérée.

9. Les entités financières autres que les microentreprises communiquent aux autorités compétentes tous les coûts et pertes occasionnés par des perturbations informatiques et des incidents liés à l'informatique.

Article 11

Politiques de sauvegarde et méthodes de rétablissement

1. Dans le but de veiller à la restauration des systèmes informatiques en limitant au maximum la durée d'indisponibilité et les perturbations, aux fins de leur cadre de gestion des risques informatiques, les entités financières définissent:

(a) une politique de sauvegarde qui précise la portée des données concernées par la sauvegarde et la fréquence minimale de celle-ci, en fonction de la criticité des informations ou du caractère sensible des données;

(b) des méthodes de rétablissement.

2. Les systèmes de sauvegarde commencent le traitement sans retard excessif, à moins que ce démarrage ne compromette la sécurité du réseau et des systèmes d'information, ou l'intégrité ou la confidentialité des données.

3. Lorsqu'elles restaurent des données de sauvegarde à l'aide de leurs propres systèmes, les entités financières utilisent des systèmes informatiques qui fonctionnent dans un

environnement d'exploitation différent du système principal, qui n'est pas directement connecté à ce dernier et qui est protégé de manière sécurisée contre tout accès non autorisé ou toute corruption informatique.

Dans le cas des entités financières visées à l'article 2, paragraphe 1, point g), les plans de rétablissement favorisent la reprise de toutes les transactions qui étaient en cours au moment de la perturbation, pour permettre aux contreparties centrales de continuer à fonctionner avec précision et d'achever le règlement à la date programmée.

4. Les entités financières maintiennent des capacités informatiques redondantes dotées de ressources et de fonctionnalités suffisantes et adéquates pour répondre aux besoins opérationnels.

5. Les entités financières visées à l'article 2, paragraphe 1, point f), maintiennent ou veillent à ce que leurs tiers prestataires de services informatiques maintiennent au moins un site de traitement secondaire doté de ressources, de capacités, de fonctionnalités et d'effectifs suffisants et appropriés pour répondre aux besoins opérationnels.

Le site de traitement secondaire:

(a) est situé à une certaine distance géographique du site de traitement primaire afin de veiller à ce qu'il présente un profil de risque distinct et d'éviter qu'il ne soit affecté par l'événement qui a touché le site primaire;

(b) est capable d'assurer la continuité des services critiques de la même manière que le site primaire, ou de fournir le niveau de services dont l'entité financière a besoin pour effectuer ses opérations critiques dans le cadre des objectifs de rétablissement;

(c) est immédiatement accessible au personnel de l'entité financière afin d'assurer la continuité des services critiques en cas d'indisponibilité du site de traitement primaire.

6. Lorsqu'elles déterminent les objectifs en matière de délai et de point de rétablissement pour chaque fonction, les entités financières tiennent compte des effets globaux potentiels sur l'efficience du marché. Ces objectifs temporels permettent d'assurer, dans des scénarios extrêmes, le respect des niveaux de service convenus.

7. Lorsqu'elles opèrent un rétablissement à la suite d'un incident lié à l'informatique, les entités financières effectuent de multiples contrôles, y compris des rapprochements, afin de garantir le niveau d'intégrité des données le plus haut possible. Ces contrôles sont également effectués lors de la reconstitution des données provenant de parties prenantes externes, afin que toutes les données soient cohérentes entre les systèmes.

Article 12

Apprentissage et évolution

1. Les entités financières disposent de capacités et d'effectifs, adaptés à leur taille, à leur activité et à leur profil de risque, pour recueillir des informations sur les vulnérabilités et les cybermenaces, et sur les incidents liés à l'informatique, en

particulier les cyberattaques, et analyser leurs incidences probables sur leur résilience opérationnelle numérique.

2. Les entités financières réalisent des examens post-incident lié à l'informatique après toute perturbation informatique importante de leurs activités principales, afin d'analyser les causes de cette perturbation et de déterminer les améliorations à apporter aux opérations informatiques ou dans le cadre de la politique de continuité des activités informatiques visée à l'article 10.

   Lorsqu'elles procèdent à des changements, les entités financières autres que les microentreprises communiquent ces changements aux autorités compétentes.

   Les examens post-incident lié à informatique visés au premier alinéa consistent à déterminer si les procédures établies ont été suivies et si les mesures prises ont été efficaces, notamment en ce qui concerne:

   (a) la célérité de la réponse aux alertes de sécurité et de l'évaluation des effets associés aux incidents liés à l'informatique et de leur gravité;

   (b) la qualité et la rapidité de l'analyse technico-légale;

   (c) l'efficacité de la remontée des incidents au sein de l'entité financière;

   (d) l'efficacité de la communication interne et externe.

3. Les enseignements tirés des tests de résilience opérationnelle numérique effectués conformément aux articles 23 et 24 et des incidents liés à l'informatique en situation réelle, en particulier les cyberattaques, ainsi que les difficultés rencontrées lors de l'activation des plans de continuité des activités ou de rétablissement, de même que les informations pertinentes échangées avec les contreparties et évaluées lors des contrôles prudentiels, sont dûment intégrés, de manière continue, dans le processus d'évaluation des risques informatiques. Ces constatations donnent lieu à un examen approprié des composantes pertinentes du cadre de gestion des risques informatiques visé à l'article 5, paragraphe 1.

4. Les entités financières contrôlent l'efficacité de la mise en œuvre de leur stratégie de résilience numérique définie à l'article 5, paragraphe 9. Elles retracent l'évolution des risques informatiques dans le temps, analysent la fréquence, les types, l'ampleur et l'évolution des incidents liés à l'informatique, en particulier les cyberattaques et leurs caractéristiques, afin de cerner le niveau d'exposition aux risques informatiques et de renforcer la maturité et la préparation informatiques de l'entité financière.

5. Les membres de l'encadrement supérieur responsables des TIC rendent compte au moins une fois par an, à l'organe de direction, des constatations visées au paragraphe 3 et formulent des recommandations.

6. Les entités financières élaborent des programmes de sensibilisation à la sécurité informatique et des formations à la résilience opérationnelle numérique qu'elles intègrent à leurs programmes de formation du personnel sous forme de modules obligatoires. Ceux-ci sont destinés à tous les employés et aux membres de la direction.

   Les entités financières assurent un suivi continu des évolutions technologiques pertinentes, notamment en vue de déterminer les incidences que le déploiement de ces nouvelles technologies pourrait avoir sur les exigences en matière de sécurité informatique et la résilience opérationnelle numérique. Elles se tiennent informées

des processus de gestion des risques informatiques les plus récents, afin de lutter efficacement contre les formes actuelles ou émergentes de cyberattaques.

Article 13
Communication

1. Aux fins du cadre de gestion des risques informatiques visé à l'article 5, paragraphe 1, les entités financières mettent en place des plans de communication qui favorisent une divulgation responsable des incidents liés à l'informatique ou des vulnérabilités majeures aux clients et aux contreparties ainsi qu'au public, le cas échéant.

2. Aux fins du cadre de gestion des risques informatiques visé à l'article 5, paragraphe 1, les entités financières mettent en œuvre des politiques de communication à l'intention du personnel et des parties prenantes externes. Les politiques de communication à l'intention du personnel tiennent compte de la nécessité d'établir une distinction entre le personnel participant à la gestion des risques informatiques, en particulier la réponse et le rétablissement, et le personnel qui doit être informé.

3. Au moins une personne au sein de l'entité est chargée de mettre en œuvre la stratégie de communication concernant les incidents liés à l'informatique et remplit le rôle de porte-parole auprès du public et des médias à cette fin.

Article 14
Harmonisation accrue des outils, méthodes, processus et politiques de gestion des risques informatiques

L'Autorité bancaire européenne (ABE), l'Autorité européenne des marchés financiers (AEMF) et l'Autorité européenne des assurances et des pensions professionnelles (AEAPP) élaborent, en concertation avec l'Agence de l'Union européenne pour la cybersécurité (ENISA), des projets de normes techniques de réglementation aux fins suivantes:

(a) préciser davantage les éléments à inclure dans les politiques, procédures, protocoles et outils de sécurité informatique visés à l'article 8, paragraphe 2, en vue de garantir la sécurité des réseaux, de favoriser la mise en place de garanties adéquates contre les intrusions et les utilisations abusives des données, de préserver l'authenticité et l'intégrité des données, y compris en recourant à des techniques cryptographiques, et de garantir une transmission précise et rapide des données sans perturbation majeure;

(b) préciser la manière dont les politiques, procédures et outils de sécurité informatique visés à l'article 8, paragraphe 2, intègrent les contrôles de sécurité dans les systèmes dès leur conception (sécurité dès le stade de la conception), permettent de procéder à des ajustements en fonction de l'évolution du paysage des menaces et prévoient l'utilisation de technologies de défense en profondeur;

(c) préciser davantage les techniques, méthodes et protocoles appropriés visés à l'article 8, paragraphe 4, point b);

(d) approfondir les composantes relatives au contrôle des droits de gestion des accès visés à l'article 8, paragraphe 4, point c), et de la politique connexe en matière de ressources humaines, en précisant les droits d'accès, les procédures

d’octroi et de révocation des droits, le suivi des comportements anormaux par rapport aux risques informatiques au moyen d’indicateurs adéquats, notamment pour les modes et les heures d’utilisation du réseau, l’activité informatique et les dispositifs inconnus;

(e) approfondir les éléments spécifiés à l’article 9, paragraphe 1, qui permettent une détection rapide des activités anormales, ainsi que les critères visés à l’article 9, paragraphe 2, qui entraînent le déclenchement des processus de détection des incidents liés à l'informatique et de réponse à ces incidents;

(f) détailler davantage les composantes de la politique de continuité des activités informatiques visée à l’article 10, paragraphe 1;

(g) détailler davantage les tests des plans de continuité des activités informatiques visés à l’article 10, paragraphe 5, afin de veiller à ce qu’ils tiennent dûment compte des scénarios dans lesquels la qualité de l’exécution d’une fonction critique se détériore à un niveau inacceptable ou dans lesquels l'exécution d'une fonction critique échoue, et à ce qu’ils prennent dûment en considération les incidences potentielles de l’insolvabilité ou d’autres défaillances de tout tiers prestataire de services informatiques concerné et, le cas échéant, les risques politiques dans les juridictions des prestataires en question;

(h) détailler davantage les composantes du plan de rétablissement après sinistre informatique visé à l’article 10, paragraphe 3.

L’ABE, l’AEMF et l’AEAPP soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le [*JO: insérer la date correspondant à une année après la date d’entrée en vigueur*].

La Commission est habilitée à adopter les normes techniques de réglementation visées au premier alinéa conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010, du règlement (UE) nº 1094/2010 et du règlement (UE) nº 1095/2010, respectivement.

CHAPITRE III

GESTION, CLASSIFICATION ET NOTIFICATION DES INCIDENTS LIÉS À L'INFORMATIQUE

Article 15

Processus de gestion des incidents liés à l'informatique

1. Les entités financières définissent et mettent en œuvre un processus de gestion des incidents liés à l'informatique afin de détecter, de gérer et de notifier les incidents liés à l'informatique, et elles mettent en place des indicateurs d’alerte précoce sous forme d’alertes.

2. Les entités financières mettent en place des processus adéquats pour assurer une surveillance, un traitement et un suivi cohérents et intégrés des incidents liés à l'informatique, afin de déterminer et de supprimer les causes profondes pour éviter que de tels incidents ne se produisent.

3. Le processus de gestion des incidents liés à l'informatique visé au paragraphe 1:

(a) instaure des procédures destinées à identifier, suivre, consigner, catégoriser et classer les incidents liés à l'informatique en fonction de leur priorité ainsi que de la gravité et de la criticité des services touchés, conformément aux critères visés à l'article 16, paragraphe 1;

(b) attribue les rôles et les responsabilités qui doivent être activés pour différents types et scénarios d'incidents liés à l'informatique;

(c) établit des plans pour la communication à l'intention du personnel, des parties prenantes externes et des médias, conformément à l'article 13, et pour la notification aux clients, les procédures internes de remontée des incidents, y compris les plaintes des clients liées aux TIC, ainsi que pour la fourniture d'informations aux entités financières qui agissent en tant que contreparties, le cas échéant;

(d) permet de notifier les incidents majeurs liés à l'informatique aux membres de la direction concernés et de communiquer à l'organe de direction des informations sur les incidents majeurs liés à l'informatique, expliquant leurs incidences, la réponse à leur apporter et les contrôles supplémentaires à mettre en place à la suite d'incidents liés à l'informatique;

(e) définit des procédures de réponse en cas d'incident lié à l'informatique, afin d'en atténuer les effets et de garantir que les services redeviennent opérationnels et sécurisés en temps utile.

Article 16

Classification des incidents liés à l'informatique

1. Les entités financières classent les incidents liés à l'informatique et déterminent leur incidence sur la base des critères suivants:

(a) le nombre d'utilisateurs ou de contreparties financières touchés par les perturbations provoquées par l'incident lié à l'informatique, et si cet incident a porté atteinte à la réputation;

(b) la durée de l'incident lié à l'informatique, y compris les interruptions de service;

(c) la répartition géographique en ce qui concerne les zones touchées par l'incident lié à l'informatique, en particulier si celui-ci touche plus de deux États membres;

(d) les pertes de données occasionnées par l'incident lié à l'informatique, telles que la perte d'intégrité, la perte de confidentialité ou la perte de disponibilité;

(e) la gravité des effets de l'incident lié à l'informatique sur les systèmes informatiques de l'entité financière;

(f) la criticité des services touchés, y compris les transactions et les opérations de l'entité financière;

(g) les conséquences économiques, en termes absolus et relatifs, de l'incident lié à l'informatique.

2. Les AES élaborent, par l'intermédiaire du comité mixte des AES (ci-après le «comité mixte») et après consultation de la Banque centrale européenne (BCE) et de

l'ENISA, des projets communs de normes techniques de réglementation qui précisent les éléments suivants:

(a) les critères énoncés au paragraphe 1, y compris les seuils d'importance significative pour déterminer les incidents majeurs liés à l'informatique qui sont soumis à l'obligation de déclaration prévue à l'article 17, paragraphe 1;

(b) les critères que les autorités compétentes doivent appliquer pour évaluer si un incident majeur lié à l'informatique est pertinent pour les juridictions des autres États membres, et les détails des rapports d'incidents liés à l'informatique à partager avec les autres autorités compétentes conformément à l'article 17, paragraphes 5 et 6.

3. Lors de l'élaboration des projets communs de normes techniques de réglementation visés au paragraphe 2, les AES tiennent compte des normes internationales, ainsi que des spécifications élaborées et publiées par l'ENISA, y compris, le cas échéant, des spécifications relatives à d'autres secteurs économiques.

Les AES soumettent ces projets communs de normes techniques de réglementation à la Commission, au plus tard le [*OP: insérer la date correspondant à une année après la date d'entrée en vigueur*].

Le pouvoir de compléter le présent règlement par l'adoption des normes techniques de réglementation visées au paragraphe 2 est délégué à la Commission conformément aux articles 10 à 14 des règlements (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010, respectivement.

Article 17

Notification des incidents majeurs liés à l'informatique

1. Les entités financières notifient à l'autorité compétente pertinente visée à l'article 41 les incidents majeurs liés à l'informatique, dans les délais prévus au paragraphe 3.

Aux fins du premier alinéa, les entités financières établissent, après avoir recueilli et analysé toutes les informations pertinentes, un rapport d'incident en utilisant le modèle visé à l'article 18, et le soumettent à l'autorité compétente.

Le rapport comprend toutes les informations nécessaires pour permettre à l'autorité compétente de déterminer l'importance de l'incident majeur lié à l'informatique et d'évaluer les éventuelles incidences transfrontières.

2. Lorsqu'un incident majeur lié à l'informatique a ou est susceptible d'avoir des répercussions sur les intérêts financiers des utilisateurs de services et des clients, les entités financières informent leurs utilisateurs de services et leurs clients de cet incident majeur lié à l'informatique dans les meilleurs délais et leur communiquent dès que possible toutes les mesures qui ont été prises pour atténuer les effets préjudiciables de cet incident.

3. Les entités financières soumettent à l'autorité compétente visée à l'article 41:

(a) une notification initiale, sans délai, et au plus tard à la fin du jour ouvrable, ou, si l'incident majeur lié à l'informatique qui a eu lieu moins de deux heures avant la fin du jour ouvrable, au plus tard quatre heures après le début du jour ouvrable suivant, ou, en cas d'indisponibilité des canaux de notification, aussitôt que ces derniers redeviennent accessibles;

(b) un rapport intermédiaire, au plus tard une semaine après la notification initiale visée au point a), suivi, le cas échéant, de notifications actualisées chaque fois qu'une mise à jour pertinente de la situation est disponible, ainsi que sur demande spécifique de l'autorité compétente;

(c) un rapport final, lorsque l'analyse des causes profondes est terminée, que des mesures d'atténuation aient déjà été mises en œuvre ou non, et lorsque les chiffres relatifs aux incidences réelles sont disponibles en lieu et place des estimations, mais au plus tard un mois après l'envoi du rapport initial.

4. Les entités financières ne peuvent déléguer à un tiers prestataire de services les obligations de notification prévues par le présent article qu'après approbation de la délégation par l'autorité compétente concernée visée à l'article 41.

5. Dès réception du rapport visé au paragraphe 1, l'autorité compétente fournit, dans les meilleurs délais, des précisions sur l'incident:

(a) à l'ABE, à l'AEMF ou à l'AEAPP, le cas échéant;

(b) à la BCE, le cas échéant, pour ce qui est des entités financières visées à l'article 2, paragraphe 1, points a), b) et c); et

(c) au point de contact unique désigné en vertu de l'article 8 de la directive (UE) 2016/1148.

6. L'ABE, l'AEMF ou l'AEAPP et la BCE évaluent la pertinence de l'incident majeur lié à l'informatique pour les autres autorités publiques concernées et les notifient en conséquence dès que possible. La BCE informe les membres du Système européen de banques centrales des questions pertinentes pour le système de paiement. Sur la base de cette notification, les autorités compétentes prennent, le cas échéant, toutes les mesures nécessaires afin de protéger la stabilité immédiate du système financier.

Article 18

Harmonisation du contenu et des modèles des rapports de notification

1. Les AES, agissant par l'intermédiaire du comité mixte et après consultation de l'ENISA et de la BCE, élaborent:

(a) des projets communs de normes techniques de réglementation dans le but:

(1) de définir le contenu des rapports de notification relatifs aux incidents majeurs liés à l'informatique;

(2) de préciser les conditions dans lesquelles les entités financières peuvent déléguer à un tiers prestataire de services, après approbation préalable de l'autorité compétente, les obligations de notification énoncées dans le présent chapitre;

(b) des projets communs de normes techniques d'exécution afin de définir les formulaires, les modèles et les procédures types permettant aux entités financières de notifier un incident majeur lié à l'informatique.

Les AES soumettent à la Commission les projets communs de normes techniques de réglementation visés au paragraphe 1, point a), et les projets communs de normes techniques d'exécution visés au paragraphe 1, point b), au plus tard le xx 202x [*OP: insérer la date correspondant à une année après la date d'entrée en vigueur*].

Le pouvoir de compléter le présent règlement par l'adoption des normes techniques de réglementation communes visées au paragraphe 1, point a), est délégué à la Commission conformément aux articles 10 à 14 des règlements (UE) nº 1093/2010, (UE) nº 1095/2010 et (UE) nº 1094/2010, respectivement.

Le pouvoir d'adopter les normes techniques d'exécution communes visées au paragraphe 1, point b), est conféré à la Commission conformément à l'article 15 des règlements (UE) nº 1093/2010, (UE) nº 1095/2010 et (UE) nº 1094/2010, respectivement.

Article 19

Centralisation des notifications d'incidents majeurs liés à l'informatique

1. Les AES, agissant par l'intermédiaire du comité mixte et en concertation avec la BCE et l'ENISA, élaborent un rapport conjoint qui évalue la possibilité de renforcer la centralisation des notifications d'incidents par la création d'un pôle de l'UE unique pour la notification des incidents majeurs liés à l'informatique par les entités financières. Le rapport étudie les moyens de faciliter le flux des notifications d'incidents liés à l'informatique, de réduire les coûts connexes et d'étayer les analyses thématiques en vue de renforcer la convergence en matière de surveillance.

2. Le rapport visé au paragraphe 1 comprend au moins les éléments suivants:

   (a) les conditions préalables à la création de ce pôle de l'UE;

   (b) les avantages, les limites et les risques éventuels;

   (c) les aspects de la gestion opérationnelle;

   (d) les conditions de participation;

   (e) les modalités d'accès des entités financières et des autorités nationales compétentes au pôle de l'UE;

   (f) une évaluation préliminaire des coûts financiers engendrés par la mise en place de la plateforme opérationnelle qui soutiendra le pôle de l'UE, y compris l'expertise requise.

3. Les AES remettent le rapport visé au paragraphe 1 à la Commission, au Parlement européen et au Conseil au plus tard le xx 202x [*JO: insérer la date correspondant à trois années après la date d'entrée en vigueur*].

Article 20

Retour d'information en matière de surveillance

1. Dès qu'elle reçoit un rapport au titre de l'article 17, paragraphe 1, l'autorité compétente en accuse réception et fournit le plus rapidement possible à l'entité financière tout retour d'information ou toute orientation nécessaire, notamment pour examiner les mesures correctives au niveau de l'entité ou les moyens de réduire au maximum les effets préjudiciables dans les différents secteurs.

2. Les AES, agissant par l'intermédiaire du comité mixte, présentent chaque année un rapport anonymisé et agrégé sur les notifications d'incidents liés à l'informatique reçues des autorités compétentes, en indiquant au minimum le nombre d'incidents majeurs liés à l'informatique, leur nature, leurs répercussions sur les opérations des

entités financières ou des clients, leurs coûts et les mesures correctives mises en œuvre.

Les AES émettent des avertissements et produisent des statistiques de haut niveau à l'appui des évaluations relatives aux menaces et à la vulnérabilité informatiques.

CHAPITRE IV

TESTS DE RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE

Article 21

Exigences générales applicables à la réalisation de tests de résilience opérationnelle numérique

1. Afin d'évaluer l'état de préparation en cas d'incidents liés à l'informatique, de recenser les faiblesses, les défaillances ou les lacunes en matière de résilience opérationnelle numérique et de mettre rapidement en œuvre des mesures correctives, les entités financières établissent, maintiennent et réexaminent, en tenant dûment compte de leur taille, de leur activité et de leur profil de risque, un programme solide et complet de tests de résilience opérationnelle numérique, qui fait partie intégrante du cadre de gestion des risques informatiques visé à l'article 5.

2. Le programme de tests de résilience opérationnelle numérique comprend une série d'évaluations, de tests, de méthodologies, de pratiques et d'outils à appliquer conformément aux dispositions des articles 22 et 23.

3. Les entités financières adoptent une approche fondée sur le risque lorsqu'elles exécutent le programme de tests de résilience opérationnelle numérique visé au paragraphe 1, en tenant compte de l'évolution du paysage des risques informatiques, de tout risque spécifique auquel l'entité financière est ou pourrait être exposée, de la criticité des actifs d'information et des services fournis, ainsi que de tout autre facteur que l'entité financière juge approprié.

4. Les entités financières veillent à ce que les tests soient effectués par des parties indépendantes internes ou externes.

5. Les entités financières définissent des procédures et des stratégies destinées à hiérarchiser, classer et résoudre tous les problèmes relevés au cours des tests et élaborent des méthodes de validation interne pour veiller à ce que toutes les faiblesses, défaillances ou lacunes recensées soient entièrement corrigées.

6. Les entités financières soumettent tous les systèmes et applications informatiques essentiels à des tests au moins une fois par an.

Article 22

Test des outils et systèmes informatiques

1. Le programme de tests de résilience opérationnelle numérique visé à l'article 21 prévoit l'exécution d'un éventail complet de tests appropriés, y compris des évaluations et des analyses de vulnérabilité, des analyses des logiciels libres, des évaluations de la sécurité des réseaux, des analyses des lacunes, des examens de la sécurité physique, des questionnaires et des solutions logicielles de numérisation, des examens du code source lorsque cela est possible, des tests fondés sur des scénarios,

des tests de compatibilité, des tests de performance, des tests de bout en bout ou des tests de pénétration.

2. Les entités financières visées à l'article 2, paragraphe 1, points f) et g), procèdent à des évaluations de la vulnérabilité avant tout déploiement ou redéploiement de services nouveaux ou existants à l'appui des fonctions, applications et composantes d'infrastructure critiques de l'entité financière.

Article 23

Tests avancés d'outils, de systèmes et de processus informatiques sur la base de tests de pénétration fondés sur la menace

1. Les entités financières identifiées conformément au paragraphe 4 effectuent au moins tous les trois ans des tests avancés au moyen d'un test de pénétration fondé sur la menace.

2. Les tests de pénétration fondés sur la menace couvrent au minimum les fonctions et les services critiques d'une entité financière et sont effectués sur des systèmes de production en direct qui appuient ces fonctions. La portée précise des tests de pénétration fondés sur la menace, reposant sur l'évaluation des fonctions et services critiques, est déterminée par les entités financières et validée par les autorités compétentes.

   Aux fins du premier alinéa, les entités financières recensent tous les processus, systèmes et technologies informatiques sous-jacents pertinents qui appuient les fonctions et services critiques, y compris les fonctions et les services externalisés ou sous-traités à des tiers prestataires de services informatiques.

   Lorsque des tiers prestataires de services informatiques sont inclus dans le champ d'application du test de pénétration fondé sur la menace, l'entité financière prend les mesures nécessaires pour garantir la participation de ces prestataires.

   Les entités financières procèdent à des contrôles efficaces de la gestion des risques afin de réduire les risques d'incidence potentielle sur les données, de dommages aux actifs et de perturbation des services ou opérations critiques au sein de l'entité financière elle-même, de ses contreparties ou du secteur financier.

   À l'issue du test, une fois que les rapports et les plans de mesures correctives ont été approuvés, l'entité financière et les testeurs externes fournissent à l'autorité compétente la documentation confirmant que le test de pénétration fondé sur la menace a été effectué conformément aux exigences. Les autorités compétentes valident la documentation et délivrent une attestation.

3. Pour réaliser les tests de pénétration fondés sur la menace, les entités financières font appel à des testeurs qui répondent aux critères définis par l'article 24 .

   Les autorités compétentes désignent les entités financières qui doivent se soumettre à un test de pénétration fondé sur la menace d'une manière qui soit proportionnée à la taille, à l'échelle, à l'activité et au profil de risque global de l'entité financière, sur la base de l'appréciation des éléments suivants:

   (a) les facteurs d'incidence, en particulier la criticité des services fournis et des activités entreprises par l'entité financière;

(b) les éventuels problèmes de stabilité financière, y compris le caractère systémique de l'entité financière au niveau national ou au niveau de l'Union, le cas échéant;

(c) le profil de risque informatique spécifique, le niveau de maturité informatique de l'entité financière ou les caractéristiques technologiques qui sont concernées.

4. L'ABE, l'AEMF et l'AEAPP élaborent, après avoir consulté la BCE et en tenant compte des cadres pertinents en vigueur dans l'Union qui s'appliquent aux tests de pénétration fondés sur le renseignement, des projets de normes techniques de réglementation visant à préciser:

(a) les critères utilisés aux fins de l'application du paragraphe 6 du présent article;

(b) les exigences concernant:

(a) la portée du test de pénétration fondé sur la menace visé au paragraphe 2 du présent article;

(b) la méthodologie des tests et l'approche à suivre pour chaque phase spécifique du processus de test;

(c) les stades de résultats, de clôture et de correction des tests;

(c) le type de coopération nécessaire, en matière de surveillance, pour l'exécution des tests de pénétration fondés sur la menace dans le contexte des entités financières qui opèrent dans plus d'un État membre, afin de garantir un niveau approprié de participation des autorités de surveillance et une mise en œuvre souple tenant compte des spécificités des sous-secteurs financiers ou des marchés financiers locaux.

Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le [*JO: insérer la date correspondant à deux mois avant la date d'entrée en vigueur*].

Le pouvoir de compléter le présent règlement par l'adoption des normes techniques de réglementation visées au deuxième alinéa est délégué à la Commission conformément aux articles 10 à 14 des règlements (UE) nº 1093/2010, (UE) nº 1095/2010 et (UE) nº 1094/2010, respectivement.

Article 24

Exigences applicables aux testeurs

1. Aux fins du déploiement de tests de pénétration fondés sur la menace, les entités financières ont uniquement recours à des testeurs qui:

(a) possèdent le degré de compétence et d'intégrité le plus élevé;

(b) possèdent des capacités techniques et organisationnelles et justifient d'une expertise spécifique en matière de renseignement sur les menaces, de tests de pénétration ou de tests de la red team;

(c) sont certifiés par un organisme d'accréditation dans un État membre ou adhèrent à des codes de conduite ou des cadres éthiques formels;

(d) dans le cas de testeurs externes, fournissent une assurance indépendante ou un rapport d'audit ayant trait à la bonne gestion des risques associés à l'exécution

de tests de pénétration fondés sur la menace, y compris la protection adéquate des informations confidentielles de l'entité financière et la couverture des risques opérationnels de l'entité financière;

(e) dans le cas de testeurs externes, sont dûment et entièrement couverts par les assurances de responsabilité civile professionnelle pertinentes, y compris contre les risques de mauvaise conduite et de négligence.

2. Les entités financières veillent à ce que les accords conclus avec des testeurs externes requièrent une gestion efficace des résultats des tests de pénétration fondés sur la menace et à ce que leur traitement, y compris la génération, l'élaboration, le stockage, l'agrégation, le rapport, la communication ou la destruction, ne fasse pas courir de risques à l'entité financière.

CHAPITRE V

GESTION DES RISQUES LIÉS AUX TIERS PRESTATAIRES DE SERVICES INFORMATIQUES

SECTION 1

PRINCIPES CLES POUR UNE BONNE GESTION DES RISQUES LIES AUX TIERS PRESTATAIRES DE SERVICES INFORMATIQUES

Article 25

Principes généraux

Les entités financières gèrent les risques liés aux tiers prestataires de services informatiques en tant que partie intégrante des risques informatiques dans leur cadre de gestion des risques informatiques et conformément aux principes ci-dessous.

1. Les entités financières qui ont conclu des accords contractuels pour l'utilisation de services informatiques dans le cadre de leurs activités commerciales restent à tout moment pleinement responsables du respect et de l'exécution de toutes les obligations découlant du présent règlement et de la législation applicable aux services financiers.

2. Les entités financières gèrent les risques liés aux tiers prestataires de services informatiques dans le respect du principe de proportionnalité, en tenant compte:

   (a) de l'ampleur, de la complexité et de l'importance des relations de dépendance en matière de TIC,

   (b) des risques découlant des accords contractuels portant sur l'utilisation de services informatiques conclus avec des tiers prestataires de services informatiques, compte tenu de la criticité ou de l'importance du service, du processus ou de la fonction en question, ainsi que des incidences potentielles de ces risques sur la continuité et la qualité des services et activités financiers, au niveau individuel et au niveau du groupe.

3. Aux fins de leur cadre de gestion des risques informatiques, les entités financières adoptent une stratégie en matière de risques liés aux tiers prestataires de services

informatiques, et la réexaminent régulièrement, en tenant compte de la stratégie multi-fournisseurs visée à l'article 5, paragraphe 9, point g). Cette stratégie inclut une politique relative à l'utilisation des services informatiques fournis par des tiers prestataires de services informatiques et s'applique sur une base individuelle et, le cas échéant, sur une base sous-consolidée et consolidée. L'organe de direction examine régulièrement les risques identifiés pour ce qui est de l'externalisation de fonctions critiques.

4. Aux fins de leur cadre de gestion des risques informatiques, les entités financières tiennent et mettent à jour, au niveau de l'entité et aux niveaux sous-consolidé et consolidé, un registre d'informations en rapport avec tous les accords contractuels portant sur l'utilisation de services informatiques fournis par des tiers prestataires de services informatiques.

   Les accords contractuels visés au premier alinéa sont dûment documentés, en opérant une distinction entre ceux qui couvrent des fonctions critiques et ceux qui ne le font pas.

   Les entités financières communiquent au moins une fois par an aux autorités compétentes des informations sur le nombre de nouveaux accords relatifs à l'utilisation de services informatiques, les catégories de tiers prestataires de services informatiques, le type d'accords contractuels et les services et fonctions qui sont fournis.

   Les entités financières mettent à la disposition de l'autorité compétente, si elle en fait la demande, le registre d'informations complet ou, le cas échéant, des sections spécifiques de celui-ci, ainsi que toute information jugée nécessaire pour garantir une surveillance efficace de l'entité financière.

   Les entités financières informent en temps utile l'autorité compétente des projets de contrats portant sur des fonctions critiques et des cas dans lesquels une fonction est devenue critique.

5. Avant de conclure un accord contractuel sur l'utilisation de services informatiques, les entités financières:

   (a) déterminent si l'accord contractuel couvre une fonction critique;

   (b) évaluent si les conditions fixées par les autorités de surveillance en matière de conclusion de contrats sont remplies;

   (c) identifient et évaluent tous les risques pertinents ayant trait à l'accord contractuel, y compris la possibilité que cet accord contractuel contribue à accroître le risque de concentration informatique;

   (d) font preuve de toute la diligence requise à l'égard des tiers prestataires de services informatiques potentiels et s'assurent, tout au long des processus de sélection et d'évaluation, que les tiers prestataires de services informatiques présentent les qualités requises;

   (e) identifient et évaluent les conflits d'intérêts susceptibles de découler de l'accord contractuel.

6. Les entités financières ne peuvent conclure des accords contractuels qu'avec des tiers prestataires de services informatiques qui respectent des normes élevées, adéquates et actualisées en matière de sécurité de l'information.

7. Lorsqu'elles exercent leurs droits d'accès, d'inspection et d'audit à l'égard d'un tiers prestataire de services informatiques, les entités financières déterminent au préalable, selon une approche fondée sur les risques, la fréquence des audits et des inspections, ainsi que les domaines qui doivent faire l'objet d'un audit, dans le respect des normes d'audit communément admises et conformément à toute instruction de surveillance relative à l'utilisation et à l'incorporation de ces normes d'audit.

Pour les accords contractuels qui supposent un niveau élevé de complexité technologique, l'entité financière vérifie que les auditeurs, qu'il s'agisse d'auditeurs internes ou externes ou de groupes d'auditeurs, possèdent les compétences et les connaissances requises pour réaliser efficacement les évaluations et les audits pertinents.

8. Les entités financières veillent à ce que les accords contractuels relatifs à l'utilisation de services informatiques soient résiliés au moins dans les circonstances suivantes:

(a) le tiers prestataire de services informatiques a enfreint les dispositions législatives, réglementaires ou contractuelles applicables;

(b) le suivi des risques liés aux tiers prestataires de services informatiques a révélé l'existence de circonstances susceptibles d'altérer l'exécution des fonctions prévues par l'accord contractuel, y compris des changements significatifs qui affectent l'accord ou la situation du tiers prestataire de services informatiques;

(c) le tiers prestataire de services informatiques présente des faiblesses avérées dans sa gestion globale des risques informatiques et, en particulier, dans la manière dont il assure la sécurité et l'intégrité des données confidentielles, personnelles ou autrement sensibles ou des informations non personnelles;

(d) il existe des circonstances dans lesquelles l'autorité compétente ne peut plus surveiller efficacement l'entité financière en raison de l'accord contractuel en question.

9. Les entités financières mettent en place des stratégies de sortie afin de tenir compte des risques susceptibles d'apparaître au niveau du tiers prestataire de services informatiques, en particulier une éventuelle défaillance de ce dernier, une détérioration de la qualité des fonctions fournies, toute perturbation de l'activité due à une fourniture inappropriée ou défaillante de services ou un risque significatif découlant du déploiement approprié et continu de la fonction.

Les entités financières veillent à ce qu'elles puissent se retirer des accords contractuels sans:

(a) perturber leurs activités commerciales,

(b) restreindre le respect des exigences réglementaires,

(c) porter atteinte à la continuité et à la qualité de leur prestation de services aux clients.

Les plans de sortie sont complets, documentés et, le cas échéant, soumis à des tests suffisants.

Les entités financières définissent des solutions de substitution et élaborent des plans de transition leur permettant de supprimer les fonctions visées par le contrat et les données pertinentes détenues par le tiers prestataire de services informatiques, et de les transférer en toute sécurité et intégralement à d'autres prestataires ou de les réorganiser en interne.

Les entités financières prennent les mesures d'urgence qui s'imposent pour maintenir la continuité des activités dans toutes les circonstances visées au premier alinéa.

10. Les AES élaborent, par l'intermédiaire du comité mixte, des projets de normes techniques d'exécution visant à mettre en place les modèles types aux fins du registre d'informations visé au paragraphe 4.

Les AES soumettent ces projets de normes techniques d'exécution à la Commission au plus tard le [*JO: insérer la date correspondant à une année après la date d'entrée en vigueur du présent règlement*].

Le pouvoir d'adopter les normes techniques d'exécution visées au premier alinéa est conféré à la Commission conformément à l'article 15 des règlements (UE) nº 1093/2010, (UE) nº 1095/2010 et (UE) nº 1094/2010, respectivement.

11. Les AES élaborent, par l'intermédiaire du comité mixte, des projets de normes de réglementation:

(a) pour préciser le contenu détaillé de la stratégie visée au paragraphe 3 en ce qui concerne les accords contractuels relatifs à l'utilisation de services informatiques fournis par des tiers prestataires de services informatiques, en se référant aux principales phases du cycle de vie des accords respectifs relatifs à l'utilisation de services informatiques;

(b) pour préciser les types d'informations à inclure dans le registre d'informations visé au paragraphe 4.

Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le [*JO: insérer la date correspondant à une année après la date d'entrée en vigueur*].

Le pouvoir de compléter le présent règlement par l'adoption des normes techniques de réglementation visées au deuxième alinéa est délégué à la Commission conformément aux articles 10 à 14 des règlements (UE) nº 1093/2010, (UE) nº 1095/2010 et (UE) nº 1094/2010, respectivement.

Article 26

Évaluation préliminaire du risque de concentration informatique et autres accords de sous-traitance

1. Lorsqu'elles procèdent à l'identification et à l'évaluation du risque de concentration informatique visé à l'article 25, paragraphe 5, point c), les entités financières déterminent si la conclusion d'un accord contractuel portant sur les services informatiques déboucherait sur l'une des situations suivantes:

(a) la conclusion d'un contrat avec un tiers prestataire de services informatiques dont les services ne sont pas facilement substituables; ou

(b) la mise en place de plusieurs accords contractuels relatifs à la fourniture de services informatiques avec le même tiers prestataire de services informatiques ou avec des tiers prestataires de services informatiques étroitement liés.

Les entités financières évaluent les avantages et les coûts des solutions de substitution, telles que le recours à différents tiers prestataires de services informatiques, en tenant compte de la compatibilité éventuelle des solutions

envisagées avec les besoins et les objectifs opérationnels définis dans leur stratégie de résilience numérique, et de la manière de garantir cette compatibilité.

2. Lorsque l'accord contractuel relatif à l'utilisation de services informatiques prévoit la possibilité qu'un tiers prestataire de services informatiques sous-traite une fonction critique à d'autres tiers prestataires de services informatiques, les entités financières évaluent les avantages et les risques qui peuvent découler de cette éventuelle sous-traitance, en particulier dans le cas d'un sous-traitant de services informatiques établi dans un pays tiers.

Lorsque des accords contractuels relatifs à l'utilisation de services informatiques sont conclus avec un tiers prestataire de services informatiques établi dans un pays tiers, les entités financières tiennent compte, au minimum, des facteurs suivants:

(a) le respect de la protection des données;

(b) l'application effective de la législation;

(c) les dispositions de la législation en matière d'insolvabilité qui s'appliqueraient en cas de faillite du tiers prestataire de services informatiques;

(d) toute contrainte qui pourrait survenir relativement à la récupération urgente des données de l'entité financière.

Les entités financières évaluent si et comment des chaînes de sous-traitance potentiellement longues ou complexes sont susceptibles de compromettre leur capacité à assurer un suivi rigoureux des fonctions visées par le contrat et la capacité de l'autorité compétente à surveiller efficacement l'entité financière à cet égard.

Article 27

Principales dispositions contractuelles

1. Les droits et obligations de l'entité financière et du tiers prestataire de services informatiques sont définis clairement et consignés par écrit. L'intégralité du contrat, qui comprend les accords de niveau de service, est consignée dans un document écrit unique mis à la disposition des parties sur papier ou dans un format téléchargeable et accessible.

2. Les accords contractuels relatifs à l'utilisation de services informatiques comportent au moins les éléments suivants:

(a) une description claire et exhaustive de tous les services et fonctions qui seront fournis par le tiers prestataire de services informatiques, indiquant si la sous-traitance d'une fonction critique, ou de parties significatives de celle-ci, est autorisée et, le cas échéant, les conditions applicables à cette sous-traitance;

(b) les lieux où les services et fonctions visés par le contrat ou la sous-traitance seront fournis et où les données seront traitées, y compris le lieu de stockage, et l'obligation pour le tiers prestataire de services informatiques d'informer l'entité financière si celui-ci envisage de déplacer ces lieux;

(c) des dispositions sur l'accessibilité, la disponibilité, l'intégrité, la sécurité et la protection des données à caractère personnel et sur la garantie de l'accès, de la récupération et de la restitution, dans un format facilement accessible, des données à caractère personnel et autres traitées par l'entité financière en cas d'insolvabilité, de résolution ou de cessation des activités commerciales du tiers prestataire de services informatiques;

(d) des descriptions complètes des niveaux de service, y compris leurs mises à jour et révisions, et des objectifs de performance quantitatifs et qualitatifs précis dans le cadre des niveaux de service convenus, afin de permettre un suivi efficace par l'entité financière et de prendre dans les meilleurs délais des mesures correctives appropriées lorsque les niveaux de service convenus ne sont pas atteints;

(e) les délais de préavis et les obligations de notification du tiers prestataire de services informatiques à l'entité financière, y compris la notification de tout développement susceptible d'avoir une incidence significative sur la capacité du tiers prestataire de services informatiques à remplir efficacement des fonctions critiques conformément aux niveaux de service convenus;

(f) l'obligation pour le tiers prestataire de services informatiques de fournir, sans frais supplémentaires ou à un coût déterminé ex ante, une assistance en cas d'incident lié à l'informatique;

(g) l'obligation pour le tiers prestataire de services informatiques de mettre en œuvre et de tester des plans d'urgence et de mettre en place des mesures, des outils et des politiques de sécurité en matière de TIC qui garantissent de manière adéquate une prestation de services sûre par l'entité financière, conformément à son cadre réglementaire;

(h) le droit d'assurer un suivi permanent des performances du tiers prestataire de services informatiques, qui comprend:

i) les droits d'accès, d'inspection et d'audit par l'entité financière ou par un tiers désigné, et le droit de prendre copie des documents pertinents, dont l'exercice effectif n'est pas entravé ou limité par d'autres dispositions contractuelles ou politiques d'exécution contractuelle;

ii) le droit de convenir d'autres niveaux d'assurance si les droits d'autres clients sont affectés;

iii) l'engagement de coopérer pleinement lors des inspections sur place effectuées par l'entité financière et des précisions sur la portée, les modalités et la fréquence des audits à distance;

(i) l'obligation pour le tiers prestataire de services informatiques de coopérer pleinement avec les autorités compétentes et les autorités de résolution de l'entité financière, y compris les personnes désignées par celles-ci;

(j) les droits de résiliation et le délai de préavis minimal correspondant pour la résiliation du contrat, conformément aux attentes des autorités compétentes;

(k) les stratégies de sortie, en particulier la fixation d'une période de transition adéquate obligatoire:

(a) au cours de laquelle le tiers prestataire de services informatiques continuera à fournir les fonctions ou services concernés en vue de réduire le risque de perturbation au niveau de l'entité financière;

(b) qui permet à l'entité financière de basculer vers un autre tiers prestataire de services informatiques ou de recourir à des solutions sur site adaptées à la complexité du service fourni.

3. Lors de la négociation d'accords contractuels, les entités financières et les tiers prestataires de services informatiques envisagent l'utilisation de clauses contractuelles types élaborées pour des services particuliers.

4. Les AES élaborent, par l'intermédiaire du comité mixte, des projets de normes techniques de réglementation visant à préciser les éléments qu'une entité financière doit déterminer et évaluer lorsqu'elle sous-traite des fonctions critiques pour donner correctement effet aux dispositions du paragraphe 2, point a).

Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le [*JO: insérer la date correspondant à une année après la date d'entrée en vigueur*].

Le pouvoir de compléter le présent règlement par l'adoption des normes techniques de réglementation visées au premier alinéa est délégué à la Commission conformément aux articles 10 à 14 des règlements (UE) nº 1093/2010, (UE) nº 1095/2010 et (UE) nº 1094/2010, respectivement.

SECTION II

CADRE DE SUPERVISION DES TIERS PRESTATAIRES CRITIQUES DE SERVICES INFORMATIQUES

Article 28

Désignation de tiers prestataires critiques de services informatiques

1. Les AES, agissant par l'intermédiaire du comité mixte et sur recommandation du forum de supervision établi conformément à l'article 29, paragraphe 1:

   (a) désignent les tiers prestataires de services informatiques qui sont critiques pour les entités financières, en tenant compte des critères précisés au paragraphe 2;

   (b) désignent l'ABE, l'AEMF ou l'AEAPP comme superviseur principal pour chaque tiers prestataire critique de services informatiques, selon que la valeur totale des actifs des entités financières qui utilisent les services de ce tiers prestataire critique de services informatiques et qui relèvent de l'un des règlements (UE) nº 1093/2010, (UE) nº 1094/2010 ou (UE) nº 1095/2010 respectivement, représente plus de la moitié de la valeur du total des actifs de toutes les entités financières qui utilisent les services du tiers prestataire critique de services informatiques, sur la base des bilans consolidés de ces entités financières, ou de leurs bilans individuels lorsque les bilans ne sont pas consolidés.

2. La désignation visée au paragraphe 1, point a), repose sur l'ensemble des critères suivants:

   (a) l'effet systémique sur la stabilité, la continuité ou la qualité de la fourniture de services financiers dans les cas où le tiers prestataire de services informatiques concerné serait confronté à une défaillance opérationnelle à grande échelle dans la prestation de ses services, compte tenu du nombre d'entités financières auxquelles le tiers prestataire de services informatiques concerné fournit des services;

(b) le caractère ou l'importance systémique des entités financières qui dépendent du tiers prestataire de services informatiques concerné, appréciés selon les paramètres suivants:

i) le nombre d'établissements d'importance systémique mondiale (EISm) ou d'autres établissements d'importance systémique (autres EIS) qui dépendent du tiers prestataire de services informatiques concerné;

ii) l'interdépendance entre les EISm ou les autres EIS visés au point i) et d'autres entités financières, y compris les situations dans lesquelles les EISm ou les autres EIS fournissent des services d'infrastructure financière à d'autres entités financières;

(c) la dépendance des entités financières à l'égard des services fournis par le tiers prestataire de services informatiques concerné en ce qui concerne les fonctions critiques des entités financières qui font en fin de compte intervenir le même tiers prestataire de services informatiques, que les entités financières dépendent de ces services directement ou indirectement, par des moyens ou par des accords de sous-traitance;

(d) le degré de substituabilité du tiers prestataire de services informatiques, en tenant compte des paramètres suivants:

i) l'absence de réelles solutions de substitution, même partielles, en raison du nombre limité de tiers prestataires de services informatiques actifs sur un marché donné, ou de la part de marché du tiers prestataire de services informatiques concerné, ou de la complexité ou du degré de sophistication technique en jeu, y compris en ce qui concerne toute technologie propriétaire, ou des caractéristiques spécifiques de l'organisation ou de l'activité du tiers prestataire de services informatiques;

ii) des difficultés à migrer partiellement ou entièrement les données et les charges de travail pertinentes du tiers prestataire de services informatiques concerné vers un autre, en raison soit de coûts financiers importants, de contraintes de temps ou d'autres types de ressources que le processus de migration peut imposer, soit de risques informatiques accrus ou d'autres risques opérationnels auxquels l'entité financière est susceptible d'être exposée du fait de cette migration;

(e) le nombre d'États membres dans lesquels le tiers prestataire de services informatiques concerné fournit des services;

(f) le nombre d'États membres dans lesquels opèrent des entités financières faisant appel au tiers prestataire de services informatiques concerné.

3. La Commission est habilitée à adopter des actes délégués, en conformité avec l'article 50, pour compléter les critères mentionnés au paragraphe 2.

4. Le mécanisme de désignation visé au paragraphe 1, point a), n'est pas activé tant que la Commission n'a pas adopté un acte délégué conformément au paragraphe 3.

5. Le mécanisme de désignation visé au paragraphe 1, point a), ne s'applique pas aux tiers prestataires de services informatiques qui sont soumis à des cadres de supervision établis en vue de soutenir les missions visées à l'article 127, paragraphe 2, du traité sur le fonctionnement de l'Union européenne.

6. Les AES, agissant par l'intermédiaire du comité mixte, établissent, publient et mettent à jour chaque année la liste des tiers prestataires critiques de services informatiques au niveau de l'Union.

7. Aux fins du paragraphe 1, point a), les autorités compétentes transmettent, sur une base annuelle et agrégée, les rapports visés à l'article 25, paragraphe 4, au forum de supervision institué en vertu de l'article 29. Le forum de supervision évalue les relations de dépendance des entités financières à l'égard de tiers prestataires de services informatiques sur la base des informations reçues des autorités compétentes.

8. Les tiers prestataires de services informatiques qui ne figurent pas sur la liste visée au paragraphe 6 peuvent demander à y figurer.

   Aux fins du premier alinéa, le tiers prestataire de services informatiques présente une demande motivée à l'ABE, à l'AEMF ou à l'AEAPP, lesquelles, par l'intermédiaire du comité mixte, décident d'inscrire ou non ce tiers prestataire de services informatiques sur cette liste conformément au paragraphe 1, point a).

   La décision visée au deuxième alinéa est adoptée et notifiée au tiers prestataire de services informatiques dans un délai de six mois à compter de la réception de la demande.

9. Les entités financières ne font pas appel à un tiers prestataire de services informatiques établi dans un pays tiers qui serait désigné comme critique en vertu du paragraphe 1, point a), s'il était établi dans l'Union.

Article 29

Structure du cadre de supervision

1. Le comité mixte institue, conformément à l'article 57 du règlement (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010, le forum de supervision en tant que sous-comité dans le but de soutenir les travaux du comité mixte et du superviseur principal visé à l'article 28, paragraphe 1, point b), dans le domaine des risques liés aux tiers prestataires de services informatiques dans les différents secteurs financiers. Le forum de supervision prépare les projets de positions communes et d'actes communs du comité mixte dans ce domaine.

   Le forum de supervision examine régulièrement les évolutions pertinentes en matière de risques et de vulnérabilités informatiques et promeut une approche cohérente dans le suivi des risques liés aux tiers prestataires de services informatiques à l'échelle de l'Union.

2. Le forum de supervision procède chaque année à une évaluation collective des résultats et des conclusions des activités de supervision menées pour l'ensemble des tiers prestataires critiques de services informatiques et promeut des mesures de coordination visant à accroître la résilience opérationnelle numérique des entités financières, à encourager les bonnes pratiques en matière de gestion du risque de concentration informatique et à envisager des mesures d'atténuation des transferts de risques intersectoriels.

3. Le forum de supervision soumet des indices de référence exhaustifs concernant les tiers prestataires critiques de services informatiques, qui seront adoptés par le comité mixte en tant que positions communes des AES, conformément à l'article 56, paragraphe 1, des règlements (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010.

4. Le forum de supervision se compose des présidents des AES et d'un représentant à haut niveau du personnel en poste de l'autorité compétente concernée de chaque État membre. Les directeurs exécutifs de chaque AES et un représentant de la Commission européenne, du CERS, de la BCE et de l'ENISA participent au forum de supervision en qualité d'observateurs.

5. Conformément à l'article 16 du règlement (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010, les AES publient des orientations sur la coopération entre les AES et les autorités compétentes, aux fins de la présente section, détaillant les procédures et conditions relatives à l'exécution des tâches entre les autorités compétentes et les AES, ainsi que les modalités des échanges d'informations nécessaires aux autorités compétentes pour assurer le suivi des recommandations adressées par les superviseurs principaux, conformément à l'article 31, paragraphe 1, point d), aux tiers prestataires critiques de services informatiques.

6. Les exigences énoncées dans la présente section sont sans préjudice de l'application de la directive (UE) 2016/1148 et des autres dispositions de l'Union en matière de supervision applicables aux fournisseurs de services d'informatique en nuage.

7. Les AES, agissant par l'intermédiaire du comité mixte et sur la base des travaux préparatoires menés par le forum de supervision, présentent chaque année au Parlement européen, au Conseil et à la Commission un rapport sur l'application de la présente section.

Article 30

Tâches du superviseur principal

1. Le superviseur principal détermine si chaque tiers prestataire critique de services informatiques a mis en place des règles, des procédures, des mécanismes et des dispositifs complets, solides et efficaces pour gérer les risques informatiques qu'il est susceptible de faire peser sur les entités financières.

2. L'évaluation visée au paragraphe 1 comprend:

   (a) des exigences en matière de TIC pour garantir, en particulier, la sécurité, la disponibilité, la continuité, l'extensibilité et la qualité des services que le tiers prestataire critique de services informatiques fournit aux entités financières, ainsi que la capacité à maintenir à tout moment des normes élevées de sécurité, de confidentialité et d'intégrité des données;

   (b) la sécurité physique qui contribue à assurer la sécurité informatique, y compris la sécurité des locaux, des installations et des centres de données;

   (c) les processus de gestion des risques, y compris les politiques de gestion des risques informatiques, la continuité des activités informatiques et les plans de rétablissement après sinistre dans le domaine informatique;

   (d) les modalités de gouvernance, notamment une structure organisationnelle comportant des lignes de responsabilité et des règles de reddition de comptes claires, transparentes et cohérentes permettant une gestion efficace des risques informatiques;

   (e) le recensement et le suivi des incidents liés à l'informatique, ainsi que leur notification rapide aux entités financières, la gestion et la résolution de ces incidents, en particulier les cyberattaques;

(f) les mécanismes relatifs à la portabilité des données, à la portabilité des applications et à l'interopérabilité, qui garantissent un exercice effectif des droits de résiliation par les entités financières;

(g) les tests des systèmes, des infrastructures et des contrôles informatiques;

(h) les audits informatiques;

(i) l'utilisation des normes nationales et internationales pertinentes applicables à la fourniture de ses services informatiques aux entités financières.

3. Sur la base de l'évaluation visée au paragraphe 1, le superviseur principal adopte un plan de supervision individuel clair, détaillé et motivé pour chaque tiers prestataire critique de services informatiques. Ce plan est communiqué chaque année au tiers prestataire critique de services informatiques.

4. Une fois que les plans annuels de supervision visés au paragraphe 3 ont été approuvés et notifiés aux tiers prestataires critiques de services informatiques, les autorités compétentes ne peuvent prendre des mesures concernant les tiers prestataires critiques de services informatiques qu'en accord avec le superviseur principal.

Article 31

Pouvoirs du superviseur principal

1. Aux fins de l'exécution des tâches prévues par la présente section, le superviseur principal dispose des pouvoirs suivants:

(a) demander l'ensemble des informations et des documents pertinents conformément à l'article 32;

(b) mener des enquêtes et des inspections générales conformément aux articles 33 et 34;

(c) demander, au terme des activités de supervision, des rapports dans lesquels sont précisées les mesures qui ont été prises ou les solutions qui ont été mises en œuvre par les tiers prestataires critiques de services informatiques en ce qui concerne les recommandations visées au point d) du présent paragraphe;

(d) formuler des recommandations dans les domaines visés à l'article 30, paragraphe 2, notamment en ce qui concerne:

i) le recours à des exigences ou à des processus spécifiques de sécurité et de qualité en matière de TIC, notamment en ce qui concerne le déploiement de correctifs, de mises à jour, de mesures de chiffrement et d'autres mesures de sécurité que le superviseur principal juge pertinentes pour garantir la sécurité informatique des services fournis aux entités financières;

ii) le recours à des conditions et des modalités, y compris leur mise en œuvre technique, en vertu desquelles les tiers prestataires critiques de services informatiques fournissent des services aux entités financières, que le superviseur principal juge pertinentes pour prévenir l'émergence de points uniques de défaillance ou leur amplification, ou pour réduire au maximum l'effet systémique éventuel dans l'ensemble du secteur financier de l'Union en cas de risque de concentration informatique;

iii) lors de l'examen, entrepris conformément aux articles 32 et 33, des accords de sous-traitance, y compris les accords d'externalisation que les tiers prestataires critiques de services informatiques prévoient de conclure avec d'autres tiers prestataires de services informatiques ou avec des sous-traitants informatiques établis dans un pays tiers, toute sous-traitance envisagée, y compris l'externalisation, lorsque le superviseur principal estime que la poursuite de la sous-traitance peut entraîner des risques pour la fourniture de services par l'entité financière ou des risques pour la stabilité financière;

iv) l'abstention de conclure un nouvel accord de sous-traitance, lorsque les conditions cumulatives suivantes sont remplies:

– le sous-traitant envisagé est un tiers prestataire de services informatiques ou un sous-traitant informatique établi dans un pays tiers;

– la sous-traitance concerne une fonction critique de l'entité financière.

2. Le superviseur principal consulte le forum de supervision avant d'exercer les pouvoirs visés au paragraphe 1.

3. Les tiers prestataires critiques de services informatiques coopèrent de bonne foi avec le superviseur principal et l'assistent dans l'accomplissement de ses tâches.

4. Le superviseur principal peut imposer une astreinte pour obliger le tiers prestataire critique de services informatiques à se conformer aux points a), b) et c) du paragraphe 1.

5. L'astreinte visée au paragraphe 4 est imposée sur une base journalière jusqu'à ce que la conformité soit atteinte et pendant une période maximale de six mois à compter de la notification au tiers prestataire critique de services informatiques.

6. Le montant de l'astreinte, calculé à partir de la date indiquée dans la décision d'astreinte, est égal à 1 % du chiffre d'affaires quotidien moyen réalisé au niveau mondial par le tiers prestataire critique de services informatiques au cours de l'exercice précédent.

7. Les astreintes sont de nature administrative et sont exécutoires. L'exécution forcée est régie par les règles de la procédure civile en vigueur dans l'État membre sur le territoire duquel les inspections sont effectuées et l'accès accordé. Les juridictions de l'État membre concerné sont compétentes pour statuer sur les plaintes relatives à un comportement abusif en matière d'exécution. Les montants des astreintes sont affectés au budget général de l'Union européenne.

8. Les AES rendent publique toute astreinte infligée, sauf dans les cas où cette publication perturberait gravement les marchés financiers ou causerait un préjudice disproportionné aux parties en cause.

9. Avant d'imposer une astreinte en vertu du paragraphe 4, le superviseur principal donne aux représentants du tiers prestataire critique de services informatiques faisant l'objet de la procédure la possibilité d'être entendus sur les conclusions et ne fonde ses décisions que sur les conclusions sur lesquelles le tiers prestataire critique de services informatiques faisant l'objet de la procédure a eu la possibilité de formuler des observations. Les droits de la défense des personnes faisant l'objet de la procédure sont pleinement assurés au cours de la procédure. Elles disposent d'un

droit d'accès au dossier, sous réserve de l'intérêt légitime d'autres personnes à ce que leurs secrets d'affaires ne soient pas divulgués. Le droit d'accès au dossier ne s'étend pas aux informations confidentielles ni aux documents préparatoires internes du superviseur principal.

Article 32
Demande d'informations

1. Le superviseur principal peut, sur simple demande ou par voie de décision, exiger des tiers prestataires critiques de services informatiques qu'ils fournissent toutes les informations nécessaires à l'exécution des tâches qui lui incombent en vertu du présent règlement, notamment tous les documents commerciaux ou opérationnels, contrats, documents stratégiques, rapports d'audit de sécurité informatique, rapports d'incidents liés à l'informatique, ainsi que toute information relative aux parties auxquelles le tiers prestataire critique de services informatiques a externalisé des fonctions ou activités opérationnelles.

2. Lorsqu'il sollicite des renseignements par simple demande en vertu du paragraphe 1, le superviseur principal:

   (a) se réfère au présent article en tant que base juridique de la demande;

   (b) indique le but de la demande;

   (c) précise la nature des informations demandées;

   (d) fixe un délai dans lequel ces informations doivent être communiquées;

   (e) informe le représentant du tiers prestataire critique de services informatiques auquel les informations sont demandées qu'il n'est pas tenu de les communiquer, mais que toute réponse donnée volontairement à la demande de renseignements ne doit pas être inexacte ni trompeuse;

3. Lorsqu'il demande des informations par voie de décision en vertu du paragraphe 1, le superviseur principal:

   (a) se réfère au présent article en tant que base juridique de la demande;

   (b) indique le but de la demande;

   (c) précise la nature des informations demandées;

   (d) fixe un délai dans lequel ces informations doivent être communiquées;

   (e) indique les astreintes prévues par l'article 31, paragraphe 4, pour le cas où les informations communiquées seraient incomplètes;

   (f) informe du droit de former un recours contre la décision devant la commission de recours de l'AES et d'en demander le réexamen par la Cour de justice de l'Union européenne (ci-après la «Cour de justice») conformément aux articles 60 et 61 des règlements (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010, respectivement.

4. Les représentants des tiers prestataires critiques de services informatiques fournissent les informations demandées. Les avocats dûment mandatés peuvent fournir les renseignements demandés au nom de leurs mandants. Le tiers prestataire critique de services informatiques reste pleinement responsable du caractère complet, exact et non trompeur des renseignements fournis.

5. Le superviseur principal envoie sans retard une copie de la décision portant sur la communication d'informations aux autorités compétentes des entités financières qui ont recours aux services des tiers prestataires critiques de services informatiques.

Article 33
Enquêtes générales

1. Afin d'exercer les fonctions qui lui incombent en vertu du présent règlement, le superviseur principal, assisté de l'équipe d'examen visée à l'article 34, paragraphe 1, peut mener les enquêtes nécessaires auprès des tiers prestataires de services informatiques.

2. Le superviseur principal est habilité à:

   (a) examiner les dossiers, données, procédures et tout autre document pertinent pour l'exécution de ses tâches, quel qu'en soit le support;

   (b) prendre ou obtenir des copies certifiées conformes ou prélever des extraits de ces dossiers, données, procédures et autres documents;

   (c) convoquer les représentants du tiers prestataire de services informatiques et leur demander de fournir oralement ou par écrit des explications sur des faits ou des documents en rapport avec l'objet et le but de l'enquête, et enregistrer leurs réponses;

   (d) interroger toute autre personne physique ou morale qui accepte de l'être aux fins de recueillir des informations concernant l'objet d'une enquête;

   (e) demander les enregistrements des échanges téléphoniques et de données.

3. Les agents et autres personnes mandatés par le superviseur principal pour mener les enquêtes visées au paragraphe 1 exercent leurs pouvoirs sur présentation d'un mandat écrit qui indique l'objet et le but de l'enquête.

   Ce mandat indique également les astreintes prévues à l'article 31, paragraphe 4, lorsque les dossiers, données, procédures ou autres documents requis, ou les réponses aux questions posées aux représentants du tiers prestataire de services informatiques ne sont pas fournis ou sont incomplets.

4. Les représentants des tiers prestataires de services informatiques sont tenus de se soumettre aux enquêtes sur la base d'une décision du superviseur principal. La décision indique l'objet et le but de l'enquête, les astreintes prévues à l'article 31, paragraphe 4, les voies de recours existantes en vertu des règlements (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010, ainsi que le droit de recours qui peut être ouvert devant la Cour de justice contre la décision.

5. En temps utile avant l'enquête, les superviseurs principaux informent les autorités compétentes des entités financières utilisant ce tiers prestataire de services informatiques de l'enquête prévue et de l'identité des personnes mandatées.

Article 34
Inspections sur place

1. Afin d'exercer les fonctions qui lui incombent en vertu du présent règlement, le superviseur principal, assisté des équipes d'examen visées à l'article 35, paragraphe 1, peut pénétrer dans tout local commercial, sur tout terrain ou sur toute propriété des tiers prestataires de services informatiques, tels que les sièges sociaux,

les centres d'exploitation et les locaux secondaires, et y effectuer toutes les inspections sur place nécessaires, ainsi que procéder à des inspections hors site.

2. Les agents et autres personnes mandatés par le superviseur principal pour effectuer une inspection sur place peuvent pénétrer dans ces locaux commerciaux, sur ces terrains ou sur ces propriétés et disposent de tous les pouvoirs nécessaires pour sceller les locaux commerciaux et les livres ou registres pendant la durée de l'inspection et dans la mesure nécessaire à celle-ci.

   Ils exercent leurs pouvoirs sur présentation d'un mandat écrit précisant l'objet et le but de l'inspection et les astreintes prévues à l'article 31, paragraphe 4, lorsque les représentants des tiers prestataires de services informatiques concernés ne se soumettent pas à l'inspection.

3. En temps utile avant l'inspection, les superviseurs principaux informent les autorités compétentes des entités financières utilisant ce tiers prestataire de services informatiques.

4. Les inspections couvrent l'ensemble des systèmes, réseaux, dispositifs, informations et données informatiques pertinents utilisés pour la fourniture de services aux entités financières ou contribuant à cette fourniture.

5. Avant toute visite sur place prévue, les superviseurs principaux adressent un préavis raisonnable aux tiers prestataires critiques de services informatiques, à moins que ce préavis ne soit pas possible en raison d'une situation d'urgence ou de crise, ou qu'il n'aboutisse à une situation dans laquelle l'inspection ou l'audit ne serait plus efficace.

6. Le tiers prestataire critique de services informatiques se soumet aux inspections sur place ordonnées par décision du superviseur principal. La décision indique l'objet et le but de l'inspection, précise la date à laquelle celle-ci commencera et indique les astreintes prévues à l'article 31, paragraphe 4, les voies de recours existantes en vertu des règlements (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010, ainsi que le droit de recours qui peut être ouvert devant la Cour de justice contre la décision.

7. Lorsque les agents et les autres personnes mandatés par le superviseur principal constatent qu'un tiers prestataire critique de services informatiques s'oppose à une inspection ordonnée en vertu du présent article, le superviseur principal informe le tiers prestataire critique de services informatiques des conséquences de cette opposition, et notamment de la possibilité qu'ont les autorités compétentes des entités financières concernées de résilier les accords contractuels conclus avec ce tiers prestataire critique de services informatiques.

Article 35

Supervision continue

1. Lorsqu'ils procèdent à des enquêtes générales ou à des inspections sur place, les superviseurs principaux sont assistés par une équipe d'examen conjoint, constituée pour chaque tiers prestataire critique de services informatiques.

2. L'équipe d'examen conjoint visée au paragraphe 1 se compose de membres du personnel du superviseur principal et des autorités compétentes concernées qui assurent la surveillance des entités financières auxquelles le tiers prestataire critique de services informatiques fournit des services, qui participent à la préparation et à l'exécution des activités de supervision, avec un maximum de dix membres. Tous les membres de l'équipe d'examen conjoint possèdent une expertise en matière de TIC

et de risque opérationnel. L'équipe d'examen conjoint travaille sous la coordination d'un membre désigné du personnel de l'AES (le «coordonnateur du superviseur principal»).

3. Les AES, par l'intermédiaire du comité mixte, élaborent des projets communs de normes techniques de réglementation afin de préciser les modalités de désignation des membres de l'équipe d'examen conjoint issus des autorités compétentes concernées, ainsi que les tâches et les modalités de travail de l'équipe d'examen. Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le [*JO: insérer la date correspondant à une année après la date d'entrée en vigueur*].

   La Commission est habilitée à adopter les normes techniques de réglementation visées au premier alinéa conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010, du règlement (UE) nº 1094/2010 et du règlement (UE) nº 1095/2010, respectivement.

4. Dans les trois mois suivant la fin d'une enquête ou d'une inspection sur place, le superviseur principal, après consultation du forum de supervision, adopte des recommandations qu'il adresse au tiers prestataire critique de services informatiques en vertu des pouvoirs prévus par l'article 31.

5. Les recommandations visées au paragraphe 4 sont immédiatement communiquées au tiers prestataire critique de services informatiques et aux autorités compétentes des entités financières auxquelles il fournit des services.

   Aux fins de la réalisation des activités de supervision, les superviseurs principaux peuvent prendre en considération toute certification pertinente d'un tiers et tout rapport d'audit interne ou externe d'un tiers prestataire de services informatiques mis à disposition par le tiers prestataire critique de services informatiques.

Article 36

Harmonisation des conditions permettant l'exercice de la supervision

1. Les AES élaborent, par l'intermédiaire du comité mixte, des projets de normes techniques de réglementation destinées à préciser:

   (a) les informations que doit fournir un tiers prestataire critique de services informatiques dans la demande d'adhésion volontaire visée à l'article 28, paragraphe 8;

   (b) le contenu et le format des rapports qui peuvent être demandés aux fins de l'article 31, paragraphe 1, point c);

   (c) la présentation des informations, y compris la structure, les formats et les méthodes, qu'un tiers prestataire critique de services informatiques est tenu de soumettre, de publier ou de fournir dans un rapport conformément à l'article 31, paragraphe 1;

   (d) les détails de l'évaluation, par les autorités compétentes, des mesures prises par des tiers prestataires critiques de services informatiques sur la base des recommandations formulées par les superviseurs principaux conformément à l'article 37, paragraphe 2.

2. Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le 1er janvier 20xx [*JO: insérer la date correspondant à une année après la date d'entrée en vigueur*].

Le pouvoir de compléter le présent règlement en adoptant les normes techniques de réglementation prévues au premier alinéa est délégué à la Commission conformément à la procédure prévue aux articles 10 à 14 des règlements (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010, respectivement.

Article 37

Suivi par les autorités compétentes

1. Dans les trente jours civils suivant la réception des recommandations formulées par les superviseurs principaux conformément à l'article 31, paragraphe 1, point d), les tiers prestataires critiques de services informatiques notifient au superviseur principal s'ils ont l'intention ou non de suivre ces recommandations. Les superviseurs principaux transmettent immédiatement ces informations aux autorités compétentes.

2. Les autorités compétentes vérifient si les entités financières tiennent compte des risques identifiés dans les recommandations adressées aux tiers prestataires critiques de services informatiques par le superviseur principal conformément à l'article 31, paragraphe 1, point d).

3. Les autorités compétentes peuvent, conformément à l'article 44, exiger des entités financières qu'elles suspendent temporairement, en partie ou en totalité, l'utilisation ou le déploiement d'un service fourni par le tiers prestataire critique de services informatiques, jusqu'à ce que les risques identifiés dans les recommandations adressées aux tiers prestataires critiques de services informatiques aient été écartés. Le cas échéant, elles peuvent exiger des entités financières qu'elles résilient, en partie ou en totalité, les accords contractuels concernés conclus avec les tiers prestataires critiques de services informatiques.

4. Lorsqu'elles prennent les décisions prévues au paragraphe 3, les autorités compétentes tiennent compte du type et de l'ampleur des risques qui n'ont pas été écartés par le tiers prestataire critique de services informatiques, ainsi que de la gravité de la non-conformité, au regard des critères suivants, en examinant:

   (a) la gravité et la durée de la non-conformité;

   (b) si la non-conformité a révélé de graves faiblesses dans les procédures, les systèmes de gestion, la gestion des risques et les contrôles internes du tiers prestataire critique de services informatiques;

   (c) si un délit financier a été facilité ou occasionné par la non-conformité ou est imputable, d'une quelconque manière, à cette non-conformité;

   (d) si la non-conformité est délibérée ou résulte d'une négligence.

5. Les autorités compétentes informent régulièrement les superviseurs principaux des approches suivies et des mesures prises dans le cadre de leurs tâches de surveillance des entités financières, ainsi que des mesures contractuelles prises par ces dernières lorsque des tiers prestataires critiques de services informatiques n'ont pas suivi, en partie ou en totalité, les recommandations adressées par les superviseurs principaux.

Article 38

Redevances de supervision

1. Les AES perçoivent auprès des tiers prestataires critiques de services informatiques des redevances qui couvrent intégralement les dépenses qu'elles doivent engager pour exercer les tâches de supervision que leur assigne le présent règlement, y compris le remboursement de tous les coûts pouvant résulter des travaux effectués par les autorités compétentes qui participent aux activités de supervision conformément à l'article 35.

   Le montant de la redevance perçue auprès d'un tiers prestataire critique de services informatiques couvre tous les frais administratifs et est proportionnel à son chiffre d'affaires.

2. La Commission est habilitée à adopter un acte délégué conformément à l'article 50 pour compléter le présent règlement en déterminant le montant des redevances et leurs modalités de paiement.

Article 39

Coopération internationale

1. L'ABE, l'AEMF et l'AEAPP peuvent, conformément à l'article 33 des règlements (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010, respectivement, conclure des accords administratifs avec les autorités de réglementation et de surveillance de pays tiers afin de faciliter la coopération internationale en ce qui concerne les risques liés aux tiers prestataires de services informatiques dans différents secteurs financiers, notamment en élaborant des bonnes pratiques pour l'examen des pratiques et des contrôles en matière de gestion des risques informatiques, des mesures d'atténuation et des réponses apportées en cas d'incident.

2. Les AES remettent tous les cinq ans au Parlement européen, au Conseil et à la Commission, par l'intermédiaire du comité mixte, un rapport conjoint confidentiel qui résume les conclusions de leurs discussions en la matière avec les autorités de pays tiers visées au paragraphe 1 et qui met l'accent sur l'évolution du risque lié aux tiers prestataires de services informatiques et sur ses implications pour la stabilité financière, l'intégrité du marché, la protection des investisseurs ou le fonctionnement du marché unique.

CHAPITRE VI

DISPOSITIFS DE PARTAGE D'INFORMATIONS

Article 40

Dispositifs de partage d'informations et de renseignements sur les cybermenaces

1. Les entités financières peuvent échanger entre elles des informations et des renseignements sur les cybermenaces, notamment des indicateurs de compromis, des tactiques, des techniques et des procédures, des alertes de cybersécurité et des outils de configuration, dans la mesure où ce partage d'informations et de renseignements:

   (a) vise à améliorer la résilience opérationnelle numérique des entités financières, notamment en les sensibilisant aux cybermenaces, en limitant ou en bloquant la

capacité de propagation des cybermenaces, et en soutenant l'éventail de capacités défensives, de techniques de détection des menaces et de stratégies d'atténuation des entités financières, ou leurs phases de réponse et de rétablissement;

(b) se déroule au sein de communautés d'entités financières de confiance;

(c) repose sur des dispositifs de partage des informations qui protègent la nature potentiellement sensible des informations partagées et qui sont régis par des règles de conduite dans le plein respect de la confidentialité des affaires, de la protection des données à caractère personnel[48] et des lignes directrices sur la politique de concurrence[49].

2. Aux fins du paragraphe 1, point c), les dispositifs de partage d'informations définissent les conditions à respecter pour y participer et, le cas échéant, précisent les modalités de participation des autorités publiques, et en quelle qualité elles peuvent être associées à ces dispositifs, ainsi que les aspects opérationnels de ce partage, y compris de l'utilisation de plateformes informatiques spécialisées.

3. Les entités financières notifient aux autorités compétentes leur participation aux dispositifs de partage d'informations visés au paragraphe 1 lors de la validation de leur adhésion ou, le cas échéant, la cessation de leur adhésion, lorsque celle-ci prend effet.

CHAPITRE VII

AUTORITÉS COMPÉTENTES

Article 41

Autorités compétentes

Sans préjudice des dispositions relatives au cadre de supervision des tiers prestataires critiques de services informatiques visés au chapitre V, section II, du présent règlement, le respect des obligations énoncées dans le présent règlement est assuré par les autorités compétentes suivantes, conformément aux pouvoirs conférés par les actes juridiques correspondants:

(a) pour les établissements de crédit, l'autorité compétente désignée conformément à l'article 4 de la directive 2013/36/UE, sans préjudice des missions spécifiques confiées à la BCE par le règlement (UE) nº 1024/2013;

(b) pour les prestataires de services de paiement, l'autorité compétente désignée conformément à l'article 22 de la directive (UE) 2015/2366;

(c) pour les établissements de paiement électronique, l'autorité compétente désignée conformément à l'article 37 de la directive 2009/110/CE;

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

[49] Communication de la Commission − Lignes directrices sur l'applicabilité de l'article 101 du traité sur le fonctionnement de l'Union européenne aux accords de coopération horizontale, 2011/C 11/01.

(d) pour les entreprises d'investissement, l'autorité compétente désignée conformément à l'article 4 de la directive (UE) 2019/2034;

(e) pour les prestataires de services sur crypto-actifs, les émetteurs de crypto-actifs, les émetteurs de jetons se référant à un ou des actifs et les émetteurs de jetons se référant à un ou des actifs et revêtant une importance significative, l'autorité compétente désignée conformément à l'article 3, paragraphe 1, point e *sexies*), premier tiret, du [*règlement (UE) 20xx (règlement MICA)*];

(f) pour les dépositaires centraux de titres, l'autorité compétente désignée conformément à l'article 11 du règlement (UE) nº 909/2014;

(g) pour les contreparties centrales, l'autorité compétente désignée conformément à l'article 22 du règlement (UE) nº 648/2012;

(h) pour les plates-formes de négociation et les prestataires de services de communication de données, l'autorité compétente désignée conformément à l'article 67 de la directive 2014/65/UE;

(i) pour les référentiels centraux, l'autorité compétente désignée conformément à l'article 55 du règlement (UE) nº 648/2012;

(j) pour les gestionnaires de fonds d'investissement alternatifs, l'autorité compétente désignée conformément à l'article 44 de la directive 2011/61/UE;

(k) pour les sociétés de gestion, l'autorité compétente désignée conformément à l'article 97 de la directive 2009/65/CE;

(l) pour les entreprises d'assurance et de réassurance, l'autorité compétente désignée conformément à l'article 30 de la directive 2009/138/CE;

(m) pour les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire, l'autorité compétente désignée conformément à l'article 12 de la directive (UE) 2016/97;

(n) pour les institutions de retraite professionnelle, l'autorité compétente désignée conformément à l'article 47 de la directive (UE) 2016/2341;

(o) pour les agences de notation de crédit, l'autorité compétente désignée conformément à l'article 21 du règlement (UE) nº 1060/2009;

(p) pour les contrôleurs légaux des comptes et les cabinets d'audit, l'autorité compétente désignée conformément à l'article 3, paragraphe 2, et à l'article 32 de la directive 2006/43/CE;

(q) pour les administrateurs d'indices de référence d'importance critique, l'autorité compétente désignée conformément aux articles 40 et 41 du *règlement xx/202x*;

(r) pour les prestataires de services de financement participatif, l'autorité compétente désignée conformément à *l'article x du règlement xx/202x*;

(s) pour les référentiels des titrisations, l'autorité compétente désignée conformément à l'article 10 et à l'article 14, paragraphe 1, du règlement (UE) nº 2017/2402.

Article 42

Coopération avec les structures et autorités établies par la directive (UE) 2016/1148

1. Afin de favoriser la coopération et de permettre des échanges en matière de surveillance entre les autorités compétentes désignées conformément au présent règlement et le groupe de coopération institué par l'article 11 de la directive (UE) 2016/1148, les AES et les autorités compétentes peuvent demander à être invitées à participer aux travaux du groupe de coopération.

2. Les autorités compétentes peuvent, le cas échéant, consulter le point de contact unique et les centres de réponse aux incidents de sécurité informatique visés respectivement aux articles 8 et 9 de la directive (UE) 2016/1148.

Article 43

Exercices, communication et coopération entre secteurs financiers

1. Les AES, par l'intermédiaire du comité mixte et en collaboration avec les autorités compétentes, la BCE et le CERS, peuvent mettre en place des mécanismes qui permettent le partage de pratiques efficaces entre les secteurs financiers afin d'améliorer la perception de chaque situation et de détecter les cybervulnérabilités et les cyberrisques communs aux différents secteurs.

   Elles peuvent mettre au point des exercices de gestion de crise et d'urgence reposant sur des scénarios de cyberattaques, en vue de développer les canaux de communication et de favoriser la mise en place progressive d'une réponse efficace et coordonnée au niveau de l'Union, en cas d'incident transfrontière majeur lié à l'informatique ou de menace connexe ayant une incidence systémique sur l'ensemble du secteur financier de l'Union.

   Ces exercices peuvent aussi éventuellement tester les relations de dépendance du secteur financier vis-à-vis d'autres secteurs économiques.

2. Les autorités compétentes, l'ABE, l'AEMF ou l'AEAPP, et la BCE coopèrent étroitement entre elles et échangent des informations afin de s'acquitter de leurs missions conformément aux articles 42 à 48. Elles coordonnent étroitement leurs activités de surveillance afin d'identifier les infractions au présent règlement et d'y remédier, de mettre au point et de promouvoir des bonnes pratiques, de faciliter la coopération, de renforcer la cohérence des interprétations et de fournir des avis interjuridictionnels en cas de désaccord.

Article 44

Sanctions administratives et mesures correctives

1. Les autorités compétentes disposent de tous les pouvoirs de surveillance, d'enquête et de sanction nécessaires pour s'acquitter des tâches qui leur incombent en vertu du présent règlement.

2. Les pouvoirs visés au paragraphe 1 incluent au minimum les pouvoirs suivants:

   (a) accéder à tout document ou toute donnée, quelle qu'en soit la forme, que les autorités compétentes jugent pertinent(e) pour l'accomplissement de leur mission de surveillance, et en recevoir ou en réaliser une copie;

   (b) procéder à des inspections sur place ou à des enquêtes;

(c) imposer des mesures correctives en cas de manquement aux exigences du présent règlement.

3. Sans préjudice du droit des États membres d'imposer des sanctions pénales conformément à l'article 46, les États membres arrêtent des règles prévoyant des sanctions administratives et des mesures correctives appropriées en cas de violation du présent règlement et veillent à leur mise en œuvre effective.

Ces sanctions et ces mesures sont efficaces, proportionnées et dissuasives.

4. Les États membres confèrent aux autorités compétentes le pouvoir d'appliquer au moins les sanctions administratives ou les mesures correctives suivantes en cas de violation du présent règlement:

(a) émettre une injonction ordonnant à la personne physique ou morale de mettre un terme au comportement en cause et lui interdisant de le réitérer;

(b) exiger la cessation temporaire ou définitive de toute pratique ou conduite que l'autorité compétente juge contraire aux dispositions du présent règlement et en prévenir la répétition;

(c) adopter tout type de mesure, y compris de nature pécuniaire, propre à garantir que les entités financières continueront à respecter leurs obligations légales;

(d) exiger, dans la mesure où le droit national le permet, les enregistrements d'échanges de données existants détenus par un opérateur de télécommunications, lorsqu'il est raisonnablement permis de suspecter une violation du présent règlement et que ces enregistrements peuvent être importants pour une enquête portant sur une violation du présent règlement; et

(e) émettre des communications au public, y compris des déclarations publiques, indiquant l'identité de la personne physique ou morale et la nature de la violation.

5. Lorsque les dispositions du paragraphe 2, point c), et du paragraphe 4 s'appliquent à des personnes morales, les États membres confèrent aux autorités compétentes le pouvoir d'appliquer les sanctions administratives et les mesures correctives prévues, sous réserve des conditions prévues dans le droit national, aux membres de l'organe de direction, ainsi qu'aux autres personnes responsables de la violation au sens du droit national.

6. Les États membres veillent à ce que toute décision d'imposer des sanctions administratives ou des mesures correctives mentionnées au paragraphe 2, point c), soit dûment motivée et puisse faire l'objet d'un recours.

Article 45

Exercice du pouvoir d'imposer des sanctions administratives et des mesures correctives

1. Les autorités compétentes exercent le pouvoir d'imposer les sanctions administratives et les mesures correctives prévues par l'article 44 conformément à leurs cadres juridiques nationaux, et, selon le cas:

(a) directement;

(b) en collaboration avec d'autres autorités;

(c) par délégation à d'autres autorités agissant sous leur responsabilité;

(d) par la saisine des autorités judiciaires compétentes.

2. Les autorités compétentes, lorsqu'elles déterminent le type et le niveau des sanctions administratives ou des mesures correctives à imposer en vertu de l'article 44, examinent dans quelle mesure la violation est intentionnelle ou résulte d'une négligence ainsi que de toutes les autres circonstances pertinentes, et notamment, le cas échéant:

(a) de la matérialité, de la gravité et de la durée de la violation;

(b) du degré de responsabilité de la personne physique ou morale responsable de la violation;

(c) de l'assise financière de la personne physique ou morale responsable;

(d) de l'importance des gains obtenus ou des pertes évitées par la personne physique ou morale en cause, dans la mesure où ils peuvent être déterminés;

(e) des préjudices subis par des tiers du fait de la violation, dans la mesure où ils peuvent être déterminés;

(f) du degré de coopération de la personne physique ou morale en cause avec l'autorité compétente, sans préjudice de la nécessité de veiller à la restitution des gains obtenus ou des pertes évitées par cette personne;

(g) des violations antérieures commises par la personne physique ou morale en cause.

Article 46

Sanctions pénales

1. Les États membres peuvent décider de ne pas prévoir de régime de sanctions administratives ou de mesures correctives pour les violations qui font l'objet de sanctions pénales dans le cadre de leur droit pénal national.

2. Les États membres qui choisissent d'instituer des sanctions pénales pour les violations du présent règlement veillent à ce que des mesures appropriées soient prises pour que les autorités compétentes disposent de tous les pouvoirs nécessaires pour se mettre en rapport avec les autorités judiciaires, les autorités chargées des poursuites ou les autorités judiciaires pénales de leur ressort territorial en vue de recevoir des informations spécifiques liées aux enquêtes ou procédures pénales engagées pour violation du présent règlement, et de fournir ces mêmes informations aux autres autorités compétentes, ainsi qu'à l'ABE, l'AEMF ou l'AEAPP, afin de s'acquitter de leurs obligations de coopération aux fins du présent règlement.

Article 47

Obligations de notification

Les États membres notifient à la Commission, à l'AEMF, à l'ABE et à l'AEAPP les dispositions législatives, réglementaires et administratives qui mettent en œuvre le présent chapitre, y compris toute disposition de droit pénal pertinente, au plus tard le [*JO: insérer la date correspondant à une année après la date d'entrée en vigueur*]. Les États membres notifient à la Commission, à l'AEMF, à l'ABE et à l'AEAPP, dans les meilleurs délais, toute modification ultérieure desdites dispositions.

Article 48

Publication des sanctions administratives

1. Les autorités compétentes publient sur leur site web officiel, dans les meilleurs délais, toute décision d'imposer une sanction administrative contre laquelle il n'y a pas de recours, une fois que cette décision a été notifiée au destinataire de la sanction.

2. La publication prévue au paragraphe 1 contient des informations sur le type et la nature de la violation ainsi que sur l'identité des personnes responsables et les sanctions imposées.

3. Si l'autorité compétente, après une évaluation au cas par cas, estime que la publication de l'identité de personnes morales, ou de l'identité et des données à caractère personnel de personnes physiques, serait disproportionnée, compromettrait la stabilité des marchés financiers ou la poursuite d'une enquête pénale en cours, ou causerait, dans la mesure où ils peuvent être déterminés, des dommages disproportionnés à la personne concernée, elle adopte l'une des solutions suivantes en ce qui concerne la décision d'imposer une sanction administrative:

   (a) reporter sa publication jusqu'à ce qu'il n'existe plus aucune raison de ne pas la publier;

   (b) la publier en préservant l'anonymat des intéressés, conformément au droit national; ou

   (c) s'abstenir de la publier, si les options a) et b) sont jugées insuffisantes pour garantir l'absence totale de risque pour la stabilité des marchés financiers, ou si cette publication ne serait pas proportionnée, eu égard à la clémence de la sanction imposée.

4. S'il est décidé de publier une sanction administrative en préservant l'anonymat des intéressés, conformément au paragraphe 3, point b), la publication des données concernées peut être différée.

5. Si une autorité compétente publie une décision de sanction administrative pouvant faire l'objet d'un recours devant les autorités judiciaires concernées, les autorités compétentes publient immédiatement cette information sur leur site web officiel et y publient ensuite toute information connexe sur l'issue de ce recours. Toute décision judiciaire annulant une décision de sanction administrative est elle aussi publiée.

6. Les autorités compétentes veillent à ce que toute publication visée aux paragraphes 1 à 4 demeure sur leur site web officiel pendant une période d'au moins cinq ans après sa publication. Les données à caractère personnel figurant dans une telle publication ne sont maintenues sur le site web officiel de l'autorité compétente que pour la durée nécessaire au sens des règles applicables en matière de protection des données.

Article 49

Secret professionnel

1. Toute information confidentielle reçue, échangée ou transmise en vertu du présent règlement est soumise aux conditions relatives à l'obligation de secret professionnel énoncées au paragraphe 2.

2. L'obligation de secret professionnel s'applique à toutes les personnes qui travaillent ou ont travaillé pour les autorités compétentes en vertu du présent règlement, ou pour toute autorité, entreprise de marché ou personne physique ou morale à laquelle ces autorités compétentes ont délégué leurs pouvoirs, y compris les auditeurs et les experts qu'elles ont mandatés.

3. Les informations couvertes par le secret professionnel ne peuvent être divulguées à quelque autre personne ou autorité que ce soit, sauf en vertu de dispositions du droit de l'Union ou du droit national.

4. Toutes les informations que s'échangent les autorités compétentes au titre du présent règlement au sujet des conditions commerciales ou opérationnelles et d'autres questions économiques ou personnelles sont considérées comme confidentielles et sont soumises aux exigences du secret professionnel, sauf si l'autorité compétente précise, au moment où elle les communique, qu'elles peuvent être divulguées, ou si cette divulgation est nécessaire aux fins d'une procédure judiciaire.

CHAPITRE VIII

ACTES DÉLÉGUÉS

Article 50

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées par le présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 28, paragraphe 3, et à l'article 38, paragraphe 2, est conféré à la Commission pour une période de cinq ans à compter du *[OP:*insérer la date correspondant à cinq années après la date d'entrée en vigueur du présent règlement].

3. La délégation de pouvoir visée à l'article 28, paragraphe 3, et à l'article 38, paragraphe 2, peut être révoquée à tout moment par le Parlement européen ou le Conseil. Une décision de révocation met fin à la délégation de pouvoir spécifiée dans la décision. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure précisée dans cette décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.

6. Un acte délégué adopté en vertu de l'article 28, paragraphe 3, et de l'article 38, paragraphe 2, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet

acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

CHAPITRE IX

DISPOSITIONS TRANSITOIRES ET FINALES

SECTION 1

Article 51

Clause de réexamen

Au plus tard le *insérer la date correspondant à cinq années après la date d'entrée en vigueur du présent règlement*], la Commission, après avoir consulté l'ABE, l'AEMF, l'AEAPP et le CERS, selon le cas, procède à un réexamen et remet au Parlement européen et au Conseil un rapport, accompagné, le cas échéant, d'une proposition législative, concernant les critères de désignation des tiers prestataires critiques de services informatiques visés à l'article 28, paragraphe 2.

SECTION II

MODIFICATIONS

Article 52

Modifications du règlement (CE) nº 1060/2009

À l'annexe I du règlement (CE) nº 1060/2009, dans la section A, au point 4, le premier alinéa est remplacé par le texte suivant:

«Toute agence de notation de crédit dispose de procédures comptables et administratives saines, de mécanismes de contrôle interne, de procédures efficaces d'évaluation des risques et de dispositifs efficaces de contrôle et de sauvegarde pour une gestion des systèmes informatiques conforme au règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA].

* Règlement (UE) 2021/xx du Parlement européen et du Conseil […] (JO L XX, JJ.MM.AAAA, p. X).».

Article 53

Modifications du règlement (UE) nº 648/2012

Le règlement (UE) nº 648/2012 est modifié comme suit:

(1) L'article 26 est modifié comme suit:

(a) le paragraphe 3 est remplacé par le texte suivant:

«3. Les contreparties centrales maintiennent et exploitent une structure organisationnelle qui assure la continuité et le bon fonctionnement de la fourniture de leurs services et de l'exercice de leurs activités. Ils utilisent des systèmes, des ressources et des procédures appropriés et proportionnés, dont des systèmes informatiques gérés conformément au règlement (UE) 2021/xx du Parlement européen et du Conseil* [DORA].

Règlement (UE) 2021/xx du Parlement européen et du Conseil […] (JO L XX, JJ.MM.AAAA, p. X).»;

(b) le paragraphe 6 est supprimé.

(2) L'article 34 est modifié comme suit:

(a) le paragraphe 1 est remplacé par le texte suivant:

«1. Les contreparties centrales établissent, mettent en œuvre et tiennent à jour une politique adéquate de continuité des activités et un plan de rétablissement après sinistre, qui incluent des plans de continuité des activités informatiques et de rétablissement après sinistre informatique établis conformément au règlement (UE) 2021/xx [DORA], visant à assurer la préservation de leurs fonctions, la reprise rapide de leurs activités et le respect de leurs obligations.»;

(b) au paragraphe 3, le premier alinéa est remplacé par le texte suivant:

«Afin d'assurer une application cohérente du présent article, l'AEMF élabore, après avoir consulté les membres du SEBC, des projets de normes techniques de réglementation précisant le contenu minimal et les exigences minimales de la politique de continuité des activités et du plan de rétablissement après sinistre, à l'exclusion des plans de continuité des activités informatiques et de rétablissement après sinistre informatique.».

(3) À l'article 56, paragraphe 3, le premier alinéa est remplacé par le texte suivant:

«3. Afin d'assurer une application cohérente du présent article, l'AEMF élabore des projets de normes techniques de réglementation précisant les détails de la demande d'enregistrement prévue au paragraphe 1, autres que ceux concernant les exigences liées à la gestion des risques informatiques.».

(4) À l'article 79, les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Les référentiels centraux détectent les sources de risques opérationnels et les réduisent au minimum en mettant en place des systèmes, des moyens de contrôle et des procédures appropriés, y compris des systèmes informatiques gérés conformément au règlement (UE) 2021/xx *[DORA*].

2. Les référentiels centraux établissent, mettent en œuvre et tiennent à jour une politique adéquate de continuité des activités et un plan de rétablissement après sinistre, y compris des plans de continuité des activités informatiques et de rétablissement après sinistre informatique établis conformément au règlement (UE) 2021/xx *[DORA]*, visant à assurer la poursuite de leurs fonctions, la reprise rapide de leurs activités et le respect de leurs obligations.».

(5) À l'article 80, le paragraphe 1 est supprimé.

Article 54

Modifications du règlement (UE) nº 909/2014

L'article 45 du règlement (UE) nº 909/2014 est modifié comme suit:

(1) Le paragraphe 1 est remplacé par le texte suivant:

«1. Le DCT identifie les sources de risque opérationnel, tant internes qu'externes, et réduit au minimum leur incidence potentielle par le déploiement d'outils, de processus et de politiques informatiques appropriés, mis en place et gérés conformément au règlement (UE) 2021/xx du Parlement européen et du Conseil* *[DORA]*, ainsi que de tous autres outils, contrôles et procédures adaptés à d'autres types de risque opérationnel, notamment à tous les systèmes de règlement de titres qu'il exploite.

Règlement (UE) 2021/xx du Parlement européen et du Conseil […] (JO L XX, JJ.MM.AAAA, p. X).».

(2) Le paragraphe 2 est supprimé.

(3) Les paragraphes 3 et 4 sont remplacés par le texte suivant:

«3. Pour les services qu'il fournit ainsi que pour chaque système de règlement de titres qu'il exploite, le DCT établit, met en œuvre et tient à jour une politique de continuité de l'activité et un plan de rétablissement après sinistre appropriés, y compris des plans de continuité des activités informatiques et de rétablissement après sinistre informatique établis conformément au règlement (UE) 2021/xx [DORA], pour garantir le maintien de ses services, la reprise rapide de ses activités et le respect de ses obligations en cas d'événement risquant sérieusement de perturber ses activités.

4. Le plan visé au paragraphe 3 prévoit le rétablissement de toutes les transactions et positions des participants en cours au moment où s'est produit le dysfonctionnement, de manière à permettre aux participants du DCT de continuer à fonctionner de manière sûre et de finaliser le règlement à la date programmée, notamment en veillant à ce que les systèmes informatiques critiques puissent reprendre les opérations à partir du moment où s'est produit le dysfonctionnement, comme prévu à l'article 11, paragraphes 5 et 7, du règlement (UE) 2021/xx [DORA].».

(4) Au paragraphe 6, le premier alinéa est remplacé par le texte suivant:

«Le DCT identifie, suit et gère les risques que sont susceptibles de représenter pour ses activités les participants clés aux systèmes de règlement de titres qu'il exploite, les prestataires de services et les fournisseurs de services de réseau, ainsi que les autres DCT et les autres infrastructures de marché. Il fournit sur demande aux autorités compétentes et aux autorités concernées des informations sur tout risque de cet ordre qu'il a identifié. Il informe également sans tarder l'autorité compétente et les autorités concernées de tout incident opérationnel, autre que lié à un risque informatique, résultant de ces risques.».

(5) Au paragraphe 7, le premier alinéa est remplacé par le texte suivant:

«L'AEMF élabore, en étroite coopération avec les membres du SEBC, des projets de normes techniques de réglementation pour préciser les risques opérationnels, autres qu'informatiques, visés aux paragraphes 1 et 6, et les méthodes visant à mesurer, à gérer ou à réduire au minimum ces risques, y compris les politiques de continuité de

l'activité et les plans de rétablissement après sinistre visés aux paragraphes 3 et 4 et les méthodes d'évaluation de ces politiques et plans.».

Article 55

Modifications du règlement (UE) nº 600/2014

Le règlement (UE) nº 600/2014 est modifié comme suit:

(1) L'article 27 *octies* est modifié comme suit:

(a) le paragraphe 4 est supprimé;

(b) au paragraphe 8, le point c) est remplacé par le texte suivant:

(c) «c) les exigences organisationnelles concrètes prévues aux paragraphes 3 et 5.»;

(2) l'article 27 *nonies* est modifié comme suit:

(a) le paragraphe 5 est supprimé;

(b) au paragraphe 8, le point e) est remplacé par le texte suivant:

«e) les exigences organisationnelles concrètes prévues au paragraphe 4.»;

(3) l'article 27 *decies* est modifié comme suit:

(a) le paragraphe 3 est supprimé;

(b) au paragraphe 5, le point b) est remplacé par le texte suivant:

«b) les exigences organisationnelles concrètes prévues aux paragraphes 2 et 4.».

Article 56

Entrée en vigueur et application

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

Il s'applique à partir du *OP: insérer la date correspondant à douze mois après la date d'entrée en vigueur*].

Toutefois, les articles 23 et 24 s'appliquent à partir du [*OP: insérer la date correspondant à 36 mois après la date d'entrée en vigueur du présent règlement*].

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

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaine(s) politique(s) concerné(s)

1.3. Nature de la proposition/de l'initiative

1.4. Objectif(s)

1.5. Justification(s) de la proposition/de l'initiative

1.6. Durée et incidence financière de la proposition/de l'initiative

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système(s) de gestion et de contrôle

2.3. Mesures de prévention des fraudes et irrégularités

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

3.2. Incidence estimée sur les dépenses

3.2.1. Synthèse de l'incidence estimée sur les dépenses

3.2.2. Incidence estimée sur les crédits

3.2.3. Incidence estimée sur les ressources humaines

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

Annexe

Hypothèses générales

Pouvoirs de supervision

FICHE FINANCIÈRE LÉGISLATIVE «AGENCES»

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

Proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier.

1.2. Domaine(s) politique(s) concerné(s)

Domaines politiques: stabilité financière, services financiers et union des marchés des capitaux

Activité: résilience opérationnelle numérique

1.3. La proposition porte sur:

☑ **une action nouvelle**

☐ **une action nouvelle suite à un projet pilote/une action préparatoire**[50]

☐ **la prolongation d'une action existante**

☐ **la fusion d'une ou plusieurs actions pour créer une action supplémentaire ou une action nouvelle**

1.4. Objectif(s)

1.4.1. Objectif(s) général(aux):

l'objectif général de l'initiative est de renforcer la résilience opérationnelle numérique des entités du secteur financier de l'Union européenne en rationalisant et en améliorant les règles en vigueur et en introduisant de nouvelles exigences dans les domaines où il existe des lacunes. Celle-ci permettrait également de renforcer le corpus réglementaire unique dans sa dimension numérique.

L'objectif global peut être structuré en trois objectifs généraux: 1) réduire le risque de perturbation et d'instabilité financières, 2) réduire la charge administrative et accroître l'efficacité de la surveillance, et 3) renforcer la protection des consommateurs et des investisseurs.

1.4.2. Objectif(s) spécifique(s)

Les objectifs spécifiques de la proposition sont les suivants:

parer aux risques informatiques (liés aux technologies de l'information et de la communication ou «TIC») de manière plus intégrée et renforcer le niveau global de résilience numérique du secteur financier;

rationaliser les notifications d'incidents liés à l'informatique et résoudre les problèmes de chevauchement des exigences en matière de notification;

permettre aux autorités de surveillance financière d'avoir accès aux informations sur les incidents liés à l'informatique;

[50] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

veiller à ce que les entités financières couvertes par la présente proposition évaluent l'efficacité de leurs mesures de prévention et de résilience et détectent les vulnérabilités liées aux TIC;

réduire la fragmentation du marché unique et favoriser la reconnaissance transfrontière des résultats des tests;

renforcer les garanties contractuelles dont disposent les entités financières lorsqu'elles ont recours à des services informatiques, y compris en ce qui concerne les règles d'externalisation (régissant la surveillance des tiers prestataires de services informatiques);

permettre une supervision des activités des tiers prestataires critiques de services informatiques;

encourager l'échange de renseignements sur les menaces dans le secteur financier.

1.4.3. Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

Un acte législatif sur la résilience opérationnelle numérique du secteur financier garantirait la mise en place d'un cadre global couvrant tous les aspects de la résilience opérationnelle numérique et contribuerait efficacement à améliorer la résilience opérationnelle globale du secteur financier. Cela permettrait de préserver la clarté et la cohérence du corpus réglementaire unique.

Cette initiative garantirait également une interaction plus claire et plus cohérente avec la directive SRI et sa révision. Elle apporterait de la clarté aux entités financières quant aux différentes règles en matière de résilience opérationnelle numérique auxquelles elles doivent se conformer, en particulier pour les entités financières détenant plusieurs agréments et opérant sur différents marchés au sein de l'Union européenne.

1.4.4. Indicateurs de performance

Préciser les indicateurs permettant de suivre l'avancement et les réalisations.

Indicateurs possibles:

Nombre d'incidents liés à l'informatique dans le secteur financier de l'Union européenne et leurs incidences

Nombre d'incidents majeurs liés à l'informatique notifiés aux autorités de surveillance prudentielle

Nombre d'entités financières qui seraient tenues d'effectuer des tests de pénétration fondés sur la menace

Nombre d'entités financières utilisant des clauses contractuelles types pour conclure des accords contractuels avec des tiers prestataires de services informatiques

Nombre de tiers prestataires critiques de services informatiques soumis à la surveillance des AES/autorités de surveillance prudentielle

Nombre d'entités financières participant aux solutions de partage de renseignements sur les menaces

Nombre d'autorités destinataires de rapports sur le même incident lié à l'informatique

Nombre de tests de pénétration fondés sur la menace au niveau transfrontière

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

Le secteur financier repose dans une large mesure sur les technologies de l'information et de la communication (TIC). Malgré les progrès considérables accomplis grâce à des initiatives stratégiques et législatives ciblées menées aux niveaux national et européen, les risques informatiques représentent toujours un défi pour la résilience opérationnelle, la performance et la stabilité du système financier de l'Union. La réforme qui a suivi la crise financière de 2008 a principalement renforcé la résilience financière du secteur financier de l'Union et visait à préserver la compétitivité et la stabilité de l'Union du point de vue économique, prudentiel et du comportement sur le marché. Bien que la sécurité informatique et la résilience opérationnelle numérique en général fassent partie du risque opérationnel, elles n'étaient pas

au cœur du programme de réglementation post-crise et ne se sont développées que dans certains domaines des politiques publiques et réglementations applicables aux marchés financiers de l'Union, ou seulement dans quelques États membres. Cette situation engendre les défis suivants, que la proposition est censée relever:

Le cadre juridique de l'Union européenne régissant le risque informatique et la résilience opérationnelle dans l'ensemble du secteur financier est fragmenté et n'est pas totalement cohérent.

Le manque de cohérence des exigences concernant la notification des incidents liés à l'informatique empêche les autorités de surveillance de disposer d'une vue d'ensemble complète de la nature, de la fréquence, de l'importance et des répercussions de ces incidents.

Certaines entités financières sont soumises, pour un même incident lié à l'informatique, à des exigences de notification complexes, qui se chevauchent et sont parfois incohérentes entre elles.

Les lacunes dans le partage d'informations et la coopération en matière de renseignement sur les cybermenaces aux niveaux stratégique, tactique et opérationnel empêchent les entités financières individuelles d'évaluer et de surveiller les cybermenaces de manière adéquate, ainsi que de se défendre contre elles et d'y répondre.

Pour certains sous-secteurs financiers, les tests de pénétration et la résilience peuvent faire l'objet de plusieurs cadres différents, non coordonnés entre eux, et sans reconnaissance transfrontière des résultats, alors que d'autres sous-secteurs ne disposent tout simplement pas de tels cadres.

Le manque de visibilité en matière de surveillance des activités des entités financières qui ont recours à des tiers prestataires de services informatiques expose les entités financières individuellement, et le système financier dans son ensemble, à des risques opérationnels.

Les autorités de surveillance financière ne disposent pas d'un mandat suffisant, ni des outils nécessaires pour surveiller et gérer la concentration et les risques systémiques découlant de la dépendance des entités financières à l'égard de tiers prestataires de services informatiques.

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs: gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

Justification de l'action au niveau européen (ex ante):

La résilience opérationnelle numérique est une question d'intérêt commun pour les marchés financiers de l'Union européenne. Une action au niveau de l'Union apporterait plus d'avantages et aurait plus de valeur que des mesures prises séparément au niveau national. Si l'on n'y ajoutait pas ces dispositions opérationnelles sur les risques informatiques, le corpus réglementaire unique fournirait certes les outils nécessaires pour parer à tous les autres types de risques au niveau européen, mais laisserait de côté les aspects liés à la résilience opérationnelle numérique, qui seraient alors soumis à des initiatives nationales fragmentées et non coordonnées. La proposition apporterait une réponse juridique claire à la question de savoir si, et comment, des dispositions s'appliquent en matière de résilience opérationnelle numérique, en particulier aux entités financières transfrontières, et les États membres n'auraient plus à agir individuellement pour améliorer les règles, les normes et les attentes en

matière de résilience opérationnelle et de cybersécurité, en réponse à la couverture actuellement limitée des règles européennes et au caractère général de la directive SRI.

Valeur ajoutée de l'Union escomptée (ex post):

L'intervention de l'Union augmenterait considérablement l'efficacité de cette politique, tout en en réduisant la complexité et en allégeant la charge financière et administrative qu'elle représente pour toutes les entités financières. Elle permettrait d'harmoniser un secteur de l'économie profondément intégré et interconnecté qui bénéficie déjà d'un corpus de règles unique et fait déjà l'objet d'une surveillance harmonisée. En ce qui concerne la notification des incidents liés à l'informatique, la proposition réduirait la charge de travail – et les coûts implicites – qu'entraîne la notification d'un même incident à plusieurs autorités européennes et/ou nationales. Elle facilitera également la reconnaissance/l'acceptation mutuelle des résultats des tests d'entités opérant au niveau transfrontière qui sont soumises à plusieurs règles de tests dans des États membres différents.

1.5.3. Leçons tirées d'expériences similaires

Nouvelle initiative

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

L'objectif de cette proposition est cohérent avec un certain nombre d'autres politiques et initiatives existantes de l'Union, notamment la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI) et la directive sur les infrastructures critiques européennes (ICE). La proposition permettrait de conserver les avantages du cadre horizontal sur la cybersécurité en maintenant les trois sous-secteurs financiers dans le champ d'application de la directive SRI. En restant associées à l'écosystème SRI, les autorités de surveillance financière seraient en mesure d'échanger des informations pertinentes avec les autorités SRI et de participer au groupe de coopération SRI. La proposition n'aurait pas d'incidence sur la directive SRI, mais s'appuierait plutôt sur celle-ci, en supprimant d'éventuels chevauchements au travers d'une exemption dite de lex specialis: l'interaction entre la réglementation relative aux services financiers et la directive SRI resterait soumise à la clause d'application de la disposition la plus spécialisée, ce qui permettrait d'exempter les entités financières des exigences de fond de la directive SRI et d'éviter tout chevauchement entre les deux actes. En outre, la proposition est conforme à la directive sur les infrastructures critiques européennes (ICE), qui fait actuellement l'objet d'une révision visant à renforcer la protection et la résilience des infrastructures critiques contre les menaces autres que cybernétiques.

Cette proposition n'aurait pas d'incidence sur le cadre financier pluriannuel (CFP). Premièrement, le cadre de supervision des tiers prestataires critiques de services informatiques sera entièrement financé par les redevances perçues auprès de ces prestataires; deuxièmement, les tâches réglementaires supplémentaires confiées aux AES en ce qui concerne la résilience opérationnelle numérique seront assurées par le redéploiement interne du personnel existant.

Cela se traduira par une proposition visant à augmenter le personnel autorisé de l'agence lors de la future procédure budgétaire annuelle. L'agence poursuivra ses efforts en vue de tirer le meilleur parti des synergies et des gains d'efficacité (notamment par l'intermédiaire des systèmes informatiques), et assurera un suivi étroit de la charge de travail supplémentaire liée à cette proposition, qui se reflétera dans le niveau de personnel autorisé demandé par l'agence dans le cadre de la procédure budgétaire annuelle.

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

Plusieurs options de financement ont été envisagées:

Premièrement, les coûts supplémentaires pourraient être financés par le mécanisme de financement habituel des AES. Cette mesure entraînerait toutefois une augmentation substantielle de la contribution de l'Union aux ressources financières des AES.

Cette option est retenue pour les coûts liés aux tâches réglementaires découlant de cette proposition. En effet, il sera demandé aux AES de redéployer leur personnel existant afin d'élaborer un certain nombre de normes techniques. Toutefois, les coûts supplémentaires liés à la supervision des tiers prestataires critiques ne peuvent pas être couverts par un redéploiement des ressources internes des AES, qui assument aussi d'autres tâches, en plus de celles prévues dans la présente proposition, notamment aux fins d'autres actes législatifs de l'Union. En outre, les tâches de surveillance liées à la résilience opérationnelle numérique nécessitent des connaissances et une expertise techniques spécifiques. Le niveau actuel de ces ressources étant insuffisant au sein des AES, des ressources supplémentaires sont nécessaires.

Enfin, selon la proposition, des redevances seront prélevées auprès des tiers prestataires critiques de services informatiques soumis à cette supervision. Ces redevances sont destinées à couvrir toutes les ressources supplémentaires dont les AES auront besoin pour s'acquitter de leurs nouvelles tâches et compétences.

1.6. Durée et incidence financière de la proposition/de l'initiative

☐ **durée limitée**

☐ Proposition/initiative en vigueur à partir de [JJ/MM]AAAA jusqu'en [JJ/MM]AAAA

☐ Incidence financière de AAAA jusqu'en AAAA

☑ **durée illimitée**

Application avec une période de démarrage à compter de 2021,

puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) de gestion prévu(s)[51]

Gestion directe par la Commission via

☐ des agences exécutives

☐ **Gestion partagée** avec les États membres

☑ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

☐ à des organisations internationales et à leurs agences (à préciser);

☐ à la BEI et au Fonds européen d'investissement;

☑ aux organismes visés aux articles 70 et 71;

☐ à des organismes de droit public;

☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

Commentaires

Sans objet

[51] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/FR/man/budgmanag/Pages/budgmanag.aspx.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

Conformément aux modalités déjà en place, les AES élaborent des rapports d'activité réguliers (y compris des rapports internes aux hauts dirigeants, des rapports aux conseils et un rapport annuel), et l'utilisation de leurs ressources et leurs performances font l'objet d'audits par la Cour des comptes et le service d'audit interne de la Commission. Le suivi des actions contenues dans la proposition et les rapports les concernant respecteront les exigences existantes ainsi que les nouvelles exigences découlant de la présente proposition.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposée

La gestion sera indirecte et sera assurée par l'intermédiaire des AES. Le mécanisme de financement passera par le prélèvement de redevances auprès des tiers prestataires critiques de services informatiques concernés.

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

En ce qui concerne l'utilisation légale, économique, effective et efficace des crédits résultant de la proposition, il est prévu que cette dernière n'entraîne pas de nouveaux risques significatifs qui ne seraient pas couverts par un cadre de contrôle interne existant. Toutefois, la perception rapide de ces redevances pourrait constituer un défi nouveau.

2.2.3. Estimation et justification du rapport coût-efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

Les systèmes de gestion et de contrôle prévus par les règlements instituant les AES fonctionnent déjà. Les AES travaillent en étroite collaboration avec le service d'audit interne de la Commission afin de veiller à ce que les normes appropriées soient respectées dans tous les domaines du cadre de contrôle interne. Ces dispositions s'appliqueront également au rôle des AES prévu par la présente proposition. En outre, à chaque exercice financier, le Parlement européen, sur recommandation du Conseil, octroie la décharge à chaque AES pour l'exécution de son budget.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées, par exemple au titre de la stratégie antifraude.

Afin de prévenir la fraude, la corruption et toute autre activité illégale, les dispositions du règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) s'appliquent sans restriction aux AES.

Les AES ont une stratégie antifraude spécifique et un plan d'action correspondant. Les actions renforcées des AES dans le domaine de la lutte contre la fraude seront conformes aux règles et orientations inscrites dans le règlement financier (mesures antifraude en tant qu'éléments d'une bonne gestion financière), aux politiques de l'OLAF en matière de prévention des fraudes, aux dispositions de la stratégie antifraude de la Commission [COM(2011)376] et à celles de l'approche commune concernant les agences décentralisées de l'Union européenne (juillet 2012) et de la feuille de route y relative.

En outre, les règlements instituant les AES ainsi que les règlements financiers des AES fixent les dispositions relatives à la mise en œuvre et au contrôle du budget des AES, ainsi que les règles financières applicables, y compris celles visant à prévenir la fraude et les irrégularités.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Type de dépenses	Participation			
	Numéro	CD/CND[52]	de pays AELE[53]	de pays candidats[54]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier

Nouvelles lignes budgétaires, dont la création est demandée

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Type de dépenses	Participation			
	Numéro	CD/CND	de pays AELE	de pays candidats	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier

52 CD = crédits dissociés / CND = crédits non dissociés.

53 AELE: Association européenne de libre-échange.

54 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

3.2. Incidence estimée sur les dépenses

3.3. Synthèse de l'incidence estimée sur les dépenses

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	Numéro	Rubrique

DG: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**TOTAL**
	Engagements	(1)									
	Paiements	(2)									
TOTAL des crédits pour la DG	Engagements										
	Paiements										

Rubrique du cadre financier pluriannuel		

En Mio EUR (à la 3e décimale)

		2022	2023	2024	2025	2026	2027	**TOTAL**
DG:								
• Ressources humaines								
• Autres dépenses administratives <>								
TOTAL DG	Crédits							

TOTAL des crédits sous la RUBRIQUE du cadre financier pluriannuel	(Total engagements = Total paiements)							

En Mio EUR (à la 3e décimale) à prix constants

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAL**
TOTAL des crédits sous les RUBRIQUES 1 du cadre financier pluriannuel	Engagements							
	Paiements							

3.3.1. Incidence estimée sur les crédits

☑ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

☐ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en millions d'euros (à la 3e décimale) à prix constants

Indiquer les objectifs et les réalisations ⇩			2022		2023		2024		2025		2026		2027		**TOTAL**	
	RÉALISATIONS															
	Type[55]	Coût moyen	N°	Coût	N°	Coût	N°	Coût	N°	Coût	N°	Coût	N°	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[56] …																
-																
Sous-total objectif spécifique nº 1																
OBJECTIF SPÉCIFIQUE nº 2…																
-																
Sous-total objectif spécifique nº 2																
COÛT TOTAL																

55 Les réalisations sont les produits et services à fournir (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

56 Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

3.3.2. Incidence estimée sur les ressources humaines

3.3.2.1. Résumé

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative

☑ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale) à prix constants

ABE, AEAPP, AEMF	2022	2023	2024	2025	2026	2027	**TOTAL**
Agents temporaires (grades AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Agents temporaires (grades AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Agents contractuels							
Experts nationaux détachés							
TOTAL	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Besoins en personnel (ETP):

ABE, AEAPP, AEMF	2022	2023	2024	2025	2026	2027	**TOTAL**
Agents temporaires (grades AD) ABE=5, AEAPP=5, AEMF=5	15	15	15	15	15	15	15
Agents temporaires (grades AST) ABE=1, AEAPP=1, AEMF=1	3	3	3	3	3	3	3
Agents contractuels							
Experts nationaux détachés							
TOTAL	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Besoins estimés en ressources humaines pour les DG (de tutelle)

☑ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

☐ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en valeur entière (ou au plus avec une décimale)

		2022	2023	2024	2025	2026	2027
• **Emplois du tableau des effectifs (fonctionnaires et agents temporaires)**							
• **Personnel externe (en équivalent temps plein - ETP)**[57]							
XX 01 02 01 (AC, END, INT de l'enveloppe globale)							
XX 01 02 02 (AC, AL, END, INT et JPD dans les délégations)							
XX 01 04 ***yy***[58]	- au siège[59]						
	- en délégation						
XX 01 05 02 (AC, END, INT sur recherche indirecte)							
10 01 05 02 (AC, END, INT sur recherche directe)							
Autres lignes budgétaires (à préciser)							
TOTAL							

XX est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	
Personnel externe	

Il convient de faire figurer à l'annexe V, section 3, la description du calcul des coûts pour les équivalents temps plein.

[57] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

[58] Sous-plafonds de personnel externe financés sur crédits opérationnels (anciennes lignes «BA»).

[59] Essentiellement pour les Fonds structurels, le Fonds européen agricole pour le développement rural (Feader) et le Fonds européen pour la pêche (FEP).

3.3.3. Compatibilité avec le cadre financier pluriannuel actuel

☑ La proposition/l'initiative est compatible avec le cadre financier pluriannuel actuel.

☐ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel[60].

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants. […]

3.3.4. Participation de tiers au financement

☐ La proposition/l'initiative ne prévoit pas de cofinancement par des tierces parties.

☑ La proposition/l'initiative prévoit un cofinancement estimé ci-après:

En Mio EUR (à la 3e décimale)

ABE

	2022	2023	2024	2025	2026	2027	Total
Les coûts seront couverts à 100 % par les redevances prélevées auprès des entités surveillées.[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL crédits cofinancés	1,373	1,948	1,748	1,748	1,748	1,748	10,313

AEAPP

	2022	2023	2024	2025	2026	2027	Total
Les coûts seront couverts à 100 % par les redevances prélevées auprès des entités surveillées.[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL crédits cofinancés	1,305	1,811	1,611	1,611	1,611	1,611	9,560

AEMF

60 Voir les articles 11 et 17 du règlement (UE, Euratom) nº 1311/2013 du Conseil fixant le cadre financier pluriannuel pour la période 2014-2020.

61 100 % du coût total estimé plus la totalité des cotisations de l'employeur au régime des pensions

62 100 % du coût total estimé plus la totalité des cotisations de l'employeur au régime des pensions

	2022	2023	2024	2025	2026	2027	Total
Les coûts seront couverts à 100 % par les redevances prélevées auprès des entités surveillées.[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL crédits cofinancés	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Incidence estimée sur les recettes

☑ La proposition/l'initiative est sans incidence financière sur les recettes.

☐ La proposition/l'initiative a une incidence financière décrite ci-après:

☐ sur les ressources propres

☐ sur les autres recettes

☐ veuillez indiquer si les recettes sont affectées à des lignes de dépenses

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[64]						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)		
Article …….								

Pour les recettes diverses qui seront «affectées», préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

[…]

Préciser la méthode de calcul de l'incidence sur les recettes.

[…]

63 100 % du coût total estimé plus la totalité des cotisations de l'employeur au régime des pensions

64 En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.

ANNEXE

Hypothèses générales

Titre 1 – Dépenses en personnel:

Les hypothèses spécifiques suivantes ont été appliquées pour calculer les dépenses en personnel, sur la base des besoins en personnel définis et expliqués ci-dessous:

- Le coût du personnel supplémentaire engagé en 2022 est calculé pour six mois, compte tenu du temps supposé nécessaire à son recrutement.
- Le coût annuel moyen d'un agent temporaire est de 150 000 EUR, dont 25 000 EUR de coûts d'«infrastructure» (bâtiments, informatique, etc.).
- Les coefficients correcteurs applicables aux salaires du personnel à Paris (ABE et AEMF) et à Francfort (AEAPP) sont respectivement de 117,7 et 99,4.
- Les cotisations de l'employeur au régime de pension des agents temporaires ont été établies à partir des salaires de base standard inclus dans les coûts annuels moyens standard, soit 95 660 EUR.
- Les agents temporaires supplémentaires sont des agents de grade AD5 et des AST.

Titre II – Dépenses d'infrastructure et d'exploitation

Les coûts sont calculés en multipliant le nombre de membres du personnel, au prorata du nombre de mois d'occupation de l'année considérée, par le coût standard d'infrastructure, soit 25 000 EUR.

Titre III – Dépenses opérationnelles

Les coûts sont estimés en fonction des hypothèses suivantes:

- Les coûts de traduction sont fixés à 350 000 EUR par an pour chacune des AES.
- Les coûts informatiques ponctuels de 500 000 EUR par AES sont supposés être mis en œuvre au cours des années 2022 et 2023 sur la base d'une ventilation 50 %/50 %. Les coûts de maintenance annuels à partir de 2024 sont estimés à 50 000 EUR par AES.
- Les coûts annuels de surveillance sur place sont estimés à 200 000 EUR par AES.

Les estimations présentées ci-dessus donnent les coûts suivants par an:

Rubrique du cadre financier pluriannuel	Numéro	

Prix constants

ABE:			2022	2023	2024	2025	2026	2027	**TOTAL**
Titre 1:	Engagements	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Paiements	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titre 2:	Engagements	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Paiements	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titre 3:	Engagements	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Paiements	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL des crédits pour l'ABE	Engagements	= 1 + 1a + 3 a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Paiements	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

AEAPP:			2022	2023	2024	2025	2026	2027	**TOTAL**
Titre 1:	Engagements	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Paiements	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Titre 2:	Engagements	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Paiements	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titre 3:	Engagements	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Paiements	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL des crédits	Engagements	= 1 + 1a + 3 a	1,305	1,811	1,611	1,611	1,611	1,611	9,560

pour l'AEAPP	Paiements	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

AEMF:			2022	2023	2024	2025	2026	2027	**TOTAL**
Titre 1:	Engagements	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Paiements	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titre 2:	Engagements	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Paiements	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titre 3:	Engagements	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Paiements	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL des crédits pour l'AEMF	Engagements	= 1 + 1a + 3 a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Paiements	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

La proposition engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en millions d'euros (à la 3e décimale) à prix constants

ABE

Indiquer les objectifs et les réalisations ⇩			2022		2023		2024		2025		2026		2027			
	RÉALISATIONS															
	Type[65]	Coût moyen	N°	Coût	N°	Coût	N°	Coût	N°	Coût	N°	Coût	N°	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE n° 1[66] Supervision directe des tiers prestataires critiques de services informatiques																
-				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Sous-total objectif spécifique n° 1																
OBJECTIF SPÉCIFIQUE n° 2…																
-																
Sous-total objectif spécifique n° 2																
COÛT TOTAL				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

AEAPP

Indiquer les objectifs et les réalisations ⇩			2022		2023		2024		2025		2026		2027			
	RÉALISATIONS															
	Type[67]	Coût moyen	N°	Coût	N°	Coût	N°	Coût	N°	Coût	N°	Coût	N°	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE n° 1[68] Supervision directe des tiers prestataires critiques de services																

[65] Les réalisations sont les produits et services à fournir (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[66] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

[67] Les réalisations sont les produits et services à fournir (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[68] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

informatiques																
-				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Sous-total objectif spécifique nº 1																
OBJECTIF SPÉCIFIQUE nº 2…																
-																
Sous-total objectif spécifique nº 2																
COÛT TOTAL				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

AEMF

Indiquer les objectifs et les réalisations ⇩			2022		2023		2024		2025		2026		2027			
	RÉALISATIONS															
	Type[69]	Coût moyen	Nº	Coût	Nº	Coût	Nº	Coût	Nº	Coût	Nº	Coût	Nº	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[70] Supervision directe des tiers prestataires critiques de services informatiques																
-				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Sous-total objectif spécifique nº 1																
OBJECTIF SPÉCIFIQUE nº 2…																
-																
Sous-total objectif spécifique nº 2																
COÛT TOTAL				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Les réalisations sont les produits et services à fournir (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[70] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

Les activités de supervision seront entièrement financées par les redevances perçues auprès des entités supervisées, comme suit:

ABE

	2022	2023	2024	2025	2026	2027	Total
Les coûts seront couverts à 100 % par les redevances prélevées auprès des entités supervisées.[71]	1 373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL crédits cofinancés	1,373	1,948	1,748	1,748	1,748	1,748	10,313

AEAPP

	2022	2023	2024	2025	2026	2027	Total
Les coûts seront couverts à 100 % par les redevances prélevées auprès des entités supervisées.[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL crédits cofinancés	1,305	1,811	1,611	1,611	1,611	1,611	9,560

AEMF

	2022	2023	2024	2025	2026	2027	Total
Les coûts seront couverts à 100 % par les redevances prélevées auprès des entités supervisées.[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL crédits cofinancés	1,373	1,948	1,748	1,748	1,748	1,748	10,313

INFORMATIONS SPÉCIFIQUES

Pouvoirs de supervision directe

[71] 100 % du coût total estimé plus la totalité des cotisations de l'employeur au régime des pensions
[72] 100 % du coût total estimé plus la totalité des cotisations de l'employeur au régime des pensions
[73] 100 % du coût total estimé plus la totalité des cotisations de l'employeur au régime des pensions

En guise d'introduction, il convient de rappeler que les entités soumises à la surveillance directe de l'AEMF doivent s'acquitter de certains frais auprès de celle-ci (coûts d'enregistrement ponctuels et coûts récurrents pour la surveillance continue). C'est le cas des agences de notation de crédit [voir le règlement délégué (UE) nº 272/2012 de la Commission] et des référentiels centraux [voir le règlement délégué (UE) nº 1003/2013 de la Commission].

Dans le cadre de la présente proposition législative, les AES se verront confier de nouvelles tâches visant à promouvoir la convergence des approches des autorités de surveillance en matière de risque lié aux tiers prestataires de services informatiques dans le secteur financier, en soumettant les tiers qui sont des prestataires critiques de services informatiques à un cadre de supervision de l'Union.

Le cadre de supervision prévu par la présente proposition s'appuie sur l'architecture institutionnelle existante dans le domaine des services financiers, en vertu de laquelle le comité mixte des AES assure une coordination intersectorielle pour toutes les questions relatives aux risques informatiques, conformément aux tâches qui lui incombent en matière de cybersécurité, avec le soutien du sous-comité compétent (forum de supervision), qui prépare les décisions individuelles et les recommandations collectives destinées aux tiers prestataires critiques de services informatiques.

Dans ce cadre, l'AES désignée comme superviseur principal pour chacun des tiers prestataires critiques de services informatiques se voit conférer des pouvoirs pour faire en sorte que les prestataires de services technologiques qui jouent un rôle critique pour le fonctionnement du secteur financier fassent l'objet d'une surveillance adéquate à l'échelle paneuropéenne. Les fonctions de supervision sont définies dans la proposition et précisées dans l'exposé des motifs. Elles incluent le droit de demander toute information et documentation pertinentes pour mener des enquêtes générales et des inspections, de formuler des recommandations et de présenter ensuite des rapports sur les mesures prises ou les solutions mises en œuvre pour donner suite à ces recommandations.

Afin d'accomplir les nouvelles tâches prévues dans la présente proposition, les AES engageront donc du personnel supplémentaire spécialisé dans les risques informatiques, qui sera chargé principalement d'évaluer les relations de dépendance avec des tiers.

Les besoins en ressources humaines peuvent être estimés à 6 ETP pour chaque autorité (5 AD et 1 AST pour appuyer les AD). Les AES supporteront également des coûts informatiques supplémentaires estimés, pour chacune des trois AES, à 500 000 EUR de coûts ponctuels et à 50 000 EUR de coûts de maintenance annuels. Un élément important de ces nouvelles tâches consiste dans la réalisation de missions d'inspection et d'audit sur place, dont le coût peut être estimé à 200 000 EUR par an pour chaque AES. Les coûts de traduction des différents documents que les AES recevront des tiers prestataires critiques de services informatiques sont également inclus dans la ligne relative aux coûts d'exploitation et s'élèvent à 350 000 EUR par an.

Tous les coûts administratifs mentionnés ci-dessus seront entièrement financés par les redevances annuelles prélevées par les AES auprès des tiers prestataires critiques de services informatiques dont elles assureront la supervision (et seront donc sans incidence sur le budget de l'Union).