UNION EUROPÉENNE

LE PARLEMENT EUROPÉEN | **LE CONSEIL**

Bruxelles, le 17 novembre 2022
(OR. en)

2020/0266 (COD) | **PE-CONS 41/22**

EF 197
ECOFIN 699
TELECOM 308
CYBER 249
CODEC 1071

ACTES LÉGISLATIFS ET AUTRES INSTRUMENTS

Objet:	RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011

RÈGLEMENT (UE) 2022/…
DU PARLEMENT EUROPÉEN ET DU CONSEIL

du …

sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011

(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[1],

vu l'avis du Comité économique et social européen[2],

statuant conformément à la procédure législative ordinaire[3],

---

[1] JO C 343 du 26.8.2021, p. 1.
[2] JO C 155 du 30.4.2021, p. 38.
[3] Position du Parlement européen du 10 novembre 2022 (non encore parue au Journal officiel) et décision du Conseil du … .

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. Elles contribuent à la bonne marche de nos économies dans des secteurs clés, tels que le secteur financier, et améliorent le fonctionnement du marché intérieur. Le degré croissant de numérisation et d'interconnexion accentue également le risque lié aux TIC, ce qui expose davantage la société dans son ensemble, et le système financier en particulier, aux cybermenaces ou aux dysfonctionnements des TIC. Si l'utilisation généralisée de systèmes de TIC ainsi qu'une numérisation et une connectivité poussées sont aujourd'hui des caractéristiques essentielles des activités des entités financières de l'Union, leur résilience numérique doit encore être mieux étudiée et intégrée dans leurs cadres opérationnels plus larges.

(2) Au cours des dernières décennies, l'utilisation des TIC est devenue centrale dans la fourniture de services financiers, au point qu'elles ont désormais acquis une importance cruciale dans l'exécution des fonctions quotidiennes typiques de toutes les entités financières. La numérisation couvre maintenant, 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 gestion de créances et les opérations de post-marché. Le secteur des assurances a également été transformé par l'utilisation des TIC avec l'apparition des intermédiaires d'assurance offrant des services en ligne et fonctionnant avec les technologies du domaine de l'assurance (InsurTech) ou la souscription d'assurance. 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 au sein du secteur financier et avec les prestataires tiers d'infrastructures et de services.

(3) Dans un rapport de 2020 consacré au cyberrisque systémique, 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 de TIC, était susceptible de constituer une vulnérabilité systémique, car des cyberincidents localisés pourraient rapidement se propager de l'une des quelque 22 000 entités financières de l'Union à l'ensemble du système financier, sans aucune entrave géographique. Les atteintes graves à la sécurité des TIC qui se produisent dans le secteur financier 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, telles que la création de fuites de liquidités et une érosion générale de la confiance dans les marchés financiers.

(4) Ces dernières années, le risque lié aux TIC a attiré l'attention des décideurs politiques, des régulateurs et des organismes de normalisation internationaux, nationaux et de l'Union, dans un effort visant à renforcer la résilience numérique, 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 le G7 et le G20 s'efforcent de fournir aux autorités compétentes et aux opérateurs de marché des diverses juridictions des outils leur permettant de renforcer la résilience de leurs systèmes financiers. Ces travaux ont également été motivés par la nécessité de tenir dûment compte du risque lié aux TIC dans le contexte d'un système financier mondial fortement interconnecté et de veiller à une plus grande cohérence des bonnes pratiques pertinentes.

(5) Malgré des initiatives stratégiques et législatives ciblées aux niveaux de l'Union et national, le risque lié aux TIC représente toujours un défi pour la résilience opérationnelle, la performance et la stabilité du système financier de l'Union. Les réformes qui ont suivi la crise financière de 2008 ont principalement renforcé la résilience financière du secteur financier de l'Union et visaient 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 des TIC et la résilience numérique fassent partie du risque opérationnel, le programme réglementaire d'après-crise financière 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.

(6) Dans sa communication du 8 mars 2018 intitulée "Plan d'action pour les technologies financières: Pour un secteur financier européen plus compétitif et plus innovant", la Commission a souligné l'importance primordiale de rendre le secteur financier de l'Union plus résilient, notamment 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 des TIC et des incidents liés aux TIC, permettant, en fin de compte, la fourniture efficace et sans accrocs de services financiers 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 européenne de surveillance (Autorité bancaire européenne ou ABE) instituée par le règlement (UE) n° 1093/2010 du Parlement européen et du Conseil[1], l'Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles ou AEAPP) instituée par le règlement (UE) n° 1094/2010 du Parlement européen et du Conseil[2] et l'Autorité européenne de surveillance (Autorité européenne des marchés financiers ou AEMF) instituée par le règlement (UE) n° 1095/2010 du Parlement européen et du Conseil[3] (regroupées conjointement sous le nom "autorités européennes de surveillance" ou AES) ont publié des avis techniques conjoints préconisant une approche cohérente du risque lié aux TIC 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.

---

[1] Règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12).

[2] Règlement (UE) n° 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/79/CE de la Commission (JO L 331 du 15.12.2010, p. 48).

[3] Règlement (UE) n° 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission (JO L 331 du 15.12.2010, p. 84).

(8) Le secteur financier de l'Union est soumis à un corpus réglementaire unique et régi par un système européen de surveillance financière. Néanmoins, les dispositions relatives à la résilience opérationnelle numérique et à la sécurité des TIC 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 la résilience opérationnelle numérique, et les mandats des autorités compétentes devraient ainsi être renforcés pour leur permettre de superviser la gestion du risque lié aux TIC dans le secteur financier afin de protéger l'intégrité et l'efficacité du marché intérieur et de faciliter son bon fonctionnement.

(9) Les disparités législatives et les approches nationales inégales en matière de réglementation ou de surveillance en ce qui concerne le risque lié aux TIC créent des obstacles au fonctionnement du marché intérieur des services financiers, lesquels entravent le plein exercice de la liberté d'établissement et la prestation de services des entités financières exerçant leurs activités sur une base transfrontière. La concurrence entre le même type d'entités financières opérant dans différents États membres pourrait également être faussée. C'est le cas, en particulier, 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 prestataires tiers de services TIC. Les disparités découlant des développements envisagés au niveau national pourraient créer de nouveaux obstacles au fonctionnement du marché intérieur, au détriment des acteurs du marché et de la stabilité financière.

(10) À ce jour, étant donné que les dispositions relatives au risque lié aux TIC ne sont que partiellement abordées au niveau de l'Union, il existe des lacunes ou des chevauchements dans des domaines importants, tels que la notification des incidents liés aux TIC et les tests de résilience opérationnelle numérique, ainsi que des incohérences imputables à l'émergence de règles nationales divergentes ou une inefficacité par rapport au coût du fait de règles qui se chevauchent. Cette situation est particulièrement préjudiciable pour un gros utilisateur de TIC tel que 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 au risque lié aux TIC et d'atténuer les effets négatifs des incidents liés aux TIC 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 au risque lié aux TIC ou au risque opérationnel, il est nécessaire de procéder à une harmonisation plus poussée des exigences clés en matière de résilience opérationnelle numérique pour toutes les entités financières. Le renforcement des capacités en matière de TIC et la résilience globale des entités financières, sur la base de ces exigences clés, 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 intérieur, il devrait reposer sur les dispositions de l'article 114 du traité sur le fonctionnement de l'Union européenne, interprétées conformément à la jurisprudence constante de la Cour de justice de l'Union européenne (ci-après dénommée "Cour de justice").

(12) Le présent règlement vise à consolider et à mettre à niveau les exigences en matière de risque lié aux TIC dans le cadre des exigences en matière de risque opérationnel qui ont, jusqu'à présent, été scindées dans divers actes juridiques de l'Union. Si ces actes 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 n'ont pas, au moment de leur adoption, couvert de manière exhaustive toutes les composantes de la résilience opérationnelle. Ces actes juridiques de l'Union, lorsqu'ils ont précisé les règles 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 le risque lié aux TIC) plutôt que des règles qualitatives ciblées en matière de protection, de détection, de confinement, de rétablissement et de réparation en cas d'incidents liés aux TIC ou en matière de capacités de notification et de tests numériques. Ces actes étaient principalement destinés à définir et à actualiser les règles essentielles en matière de surveillance prudentielle, d'intégrité du marché ou de conduite sur le marché.

Par la consolidation et l'actualisation des différentes règles relatives au risque lié aux TIC, toutes les dispositions traitant du risque lié aux TIC dans le secteur financier seraient pour la première fois réunies de manière cohérente dans un seul et même acte législatif. Par conséquent, le présent règlement comble les lacunes ou remédie aux incohérences de certains des actes juridiques antérieurs, notamment en ce qui concerne la terminologie qui y est utilisée, et fait explicitement référence au risque lié aux TIC au travers de règles ciblées sur les capacités de gestion du risque lié aux TIC, la notification des incidents et les tests de résilience opérationnelle, ainsi que le suivi des risques des tiers liés aux TIC. Le présent règlement devrait donc également mieux sensibiliser au risque lié aux TIC et souligner que les incidents liés aux TIC et l'absence de résilience opérationnelle ont la possibilité de compromettre la solidité des entités financières.

(13) Les entités financières devraient suivre la même approche et les mêmes règles de principe lorsqu'elles abordent le risque lié aux TIC, en tenant compte de leur taille et de leur profil de risque global, ainsi que de la nature, de l'ampleur et de la complexité de leurs services, activités et opérations. La cohérence contribue à renforcer la confiance dans le système financier et à préserver sa stabilité, en particulier en période de forte dépendance à l'égard des systèmes, plateformes et infrastructures des TIC, 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 dysfonctionnements des TIC.

(14) Un règlement permet de réduire la complexité réglementaire, favorise la convergence en matière de surveillance et accroît la sécurité juridique, et contribue également 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 constitue donc le moyen le plus approprié de garantir une application homogène et cohérente de toutes les composantes de la gestion du risque lié aux TIC par le secteur financier de l'Union.

(15) La directive (UE) 2016/1148 du Parlement européen et du Conseil[1] a constitué le premier cadre horizontal en matière de cybersécurité adopté au niveau de l'Union, s'appliquant également 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 prévoyait un mécanisme d'identification au niveau national des opérateurs de services essentiels, seuls certains établissements de crédit, plates-formes de négociation et contreparties centrales qui ont été identifiés par les États membres ont été inclus en pratique dans son champ d'application et sont ainsi tenus de se conformer aux exigences en matière de sécurité des TIC et de notification des incidents qui y sont définies. La directive (UE) .../... du Parlement européen et du Conseil[2+] fixe un critère uniforme visant à déterminer les entités qui relèvent de son champ d'application (règle associée à un plafond), tout en maintenant les trois types d'entités financières dans son champ d'application.

---

[1] 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).

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

[+] JO: veuillez insérer dans le texte le numéro de la directive figurant dans le document PE-CONS 32/22 (2020/0359 (COD)) et dans la note de bas de page le numéro, la date d'adoption et la référence de publication de ladite directive.

(16) Toutefois, étant donné que le présent règlement rehausse le niveau d'harmonisation des diverses composantes de la résilience numérique, en instaurant, en matière de gestion du risque lié aux TIC et de notification des incidents liés aux TIC, des exigences plus strictes que celles prévues par l'actuel droit de l'Union sur les services financiers, ce niveau accru constitue une harmonisation plus poussée, y compris par rapport aux exigences énoncées dans la directive (UE) .../...[+]. Par conséquent, le présent règlement constitue une lex specialis en ce qui concerne la directive (UE) …/…[+]. Dans le même temps, il est indispensable de maintenir un lien étroit entre le secteur financier et le cadre horizontal de l'Union en matière de cybersécurité tel qu'il est actuellement défini dans la directive (UE) .../...[+] afin de garantir la cohérence avec les stratégies de cybersécurité adoptées par les États membres et de permettre aux autorités de surveillance financière d'être informées des cyberincidents touchant d'autres secteurs couverts par ladite directive.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

(17) Conformément à l'article 4, paragraphe 2, du traité sur l'Union européenne et sans préjudice du contrôle juridictionnel exercé par la Cour de justice, le présent règlement ne devrait pas avoir d'incidence sur la responsabilité des États membres pour ce qui est des fonctions essentielles de l'État en matière de sécurité publique, de défense et de sauvegarde de la sécurité nationale, par exemple en ce qui concerne la fourniture d'informations qui serait contraire à la sauvegarde de la sécurité nationale.

(18) Afin de favoriser l'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) .../...[+] devraient continuer à faire partie de l'"écosystème" de ladite directive (par exemple, le groupe de coopération et les centres de réponse aux incidents de sécurité informatique (CSIRT)). Les AES et les autorités nationales compétentes devraient pouvoir participer aux discussions stratégiques et aux travaux techniques du groupe de coopération relevant de ladite directive, et échanger des informations et coopérer davantage avec les points de contact uniques désignés ou établis conformément à ladite directive. Les autorités compétentes au titre du présent règlement devraient également consulter les CSIRT et coopérer avec ceux-ci. Les autorités compétentes devraient aussi pouvoir demander des conseils techniques aux autorités compétentes désignées ou établies conformément à la directive (UE) .../...[+] et établir des accords de coopération visant à assurer la mise en place de mécanismes de coordination efficaces et rapides.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

(19) En raison des liens étroits entre la résilience numérique et la résilience physique des entités financières, une approche cohérente en ce qui concerne la résilience des entités critiques est nécessaire dans le présent règlement et dans la directive (UE) .../... du Parlement européen et du Conseil[1+]. Étant donné que la résilience physique des entités financières est traitée de manière globale par les obligations en matière de gestion et de notification du risque lié aux TIC couvertes par le présent règlement, les obligations prévues aux chapitres III et IV de la directive (UE) .../...[++] ne devraient pas s'appliquer aux entités financières qui relèvent du champ d'application de ladite directive.

---

[1] Directive (UE) .../... du Parlement européen et du Conseil du … sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L ... du ..., p. ...).

[+] JO: veuillez insérer dans le texte le numéro de la directive figurant dans le document PE-CONS 51/22 (2020/0365 (COD)) et dans la note de bas de page le numéro, la date d'adoption et la référence de publication de ladite directive.

[++] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 51/22 (2020/0365 (COD)).

(20) Les fournisseurs de services d'informatique en nuage constituent une catégorie d'infrastructure numérique relevant de la directive (UE) .../...[+]. Le cadre de supervision de l'Union (ci-après dénommé "cadre de supervision") établi par le présent règlement s'applique à tous les prestataires tiers critiques de services TIC, y compris les fournisseurs de services d'informatique en nuage fournissant des services TIC à des entités financières et devrait être considéré comme complémentaire de la surveillance prévue par la directive (UE) …/…[+]. 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 établissant une autorité de supervision numérique.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

(21) Afin de conserver la maîtrise totale du risque lié aux TIC, les entités financières doivent disposer de capacités globales permettant une gestion solide et efficace du risque lié aux TIC, ainsi que de mécanismes et de politiques spécifiques pour le traitement de tous les incidents liés aux TIC et pour la notification des incidents majeurs liés aux TIC. De même, les entités financières devraient disposer de politiques pour le test des systèmes de TIC, contrôles des TIC et processus des TIC, ainsi que pour la gestion des risques liés aux prestataires tiers de services TIC. Le niveau de référence en matière de résilience opérationnelle numérique des entités financières devrait être relevé tout en permettant également une application proportionnée des exigences à certaines entités financières, en particulier les microentreprises, ainsi que les entités financières soumises à un cadre de gestion du risque lié aux TIC simplifié. Pour favoriser une surveillance efficace des institutions de retraite professionnelle qui soit proportionnée et réponde au besoin de réduire les charges administratives pesant sur les autorités compétentes, les dispositions nationales pertinentes en matière de surveillance applicables à ces entités financières devraient tenir compte de leur taille et de leur profil de risque global, ainsi que de la nature, de l'ampleur et de la complexité de leurs services, activités et opérations, même lorsque les seuils pertinents fixés à l'article 5 de la directive (UE) 2016/2341 du Parlement européen et du Conseil[1] sont dépassés. En particulier, les activités de surveillance devraient porter essentiellement sur la nécessité de faire face aux risques graves associés à la gestion du risque lié aux TIC d'une entité donnée.

---

[1] Directive (UE) 2016/2341 du Parlement européen et du Conseil du 14 décembre 2016 concernant les activités et la surveillance des institutions de retraite professionnelle (IRP) (JO L 354 du 23.12.2016, p. 37).

Les autorités compétentes devraient également maintenir une approche vigilante, mais proportionnée, en ce qui concerne la surveillance des institutions de retraite professionnelle qui, conformément à l'article 31 de la directive (UE) 2016/2341, externalisent une partie importante de leurs activités de base, telles que la gestion d'actifs, les calculs actuariels, la comptabilité et la gestion de données, à des prestataires de services.

(22) Les seuils et les taxinomies de notification des incidents liés aux TIC 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) instituée par le règlement (UE) 2019/881 du Parlement européen et du Conseil[1] et le groupe de coopération relevant de la directive (UE) .../...[+], des approches divergentes sur la fixation des seuils et l'utilisation des taxinomies existent toujours ou peuvent apparaître pour les autres entités financières. En raison de ces divergences, il existe de multiples exigences auxquelles les entités financières doivent se conformer, notamment lorsqu'elles sont actives dans plusieurs États membres et lorsqu'elles font partie d'un groupe financier. En outre, ces divergences sont susceptibles d'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 au risque lié aux TIC en cas d'attaques à grande échelle susceptibles d'avoir des conséquences systémiques.

---

[1] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

(23) Pour réduire la charge administrative et les obligations de notification susceptibles d'être redondantes pour certaines entités financières, l'obligation de notification des incidents au titre de la directive (UE) 2015/2366 du Parlement européen et du Conseil[1] devrait cesser de s'appliquer aux prestataires de services de paiement qui relèvent du champ d'application du présent règlement. Par conséquent, les établissements de crédit, les établissements de monnaie électronique, les établissements de paiement et les prestataires de services d'information sur les comptes, visés à l'article 33, paragraphe 1, de ladite directive, devraient, à compter de la date d'application du présent règlement, signaler, conformément au présent règlement, tous les incidents opérationnels ou de sécurité liés au paiement qui ont été précédemment signalés au titre de ladite directive, que ces incidents soient liés ou non aux TIC.

[1] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

(24) Afin de permettre aux autorités compétentes de remplir un rôle de surveillance en obtenant une vue d'ensemble complète de la nature, de la fréquence, de l'importance et des conséquences des incidents liés aux TIC, et afin d'améliorer l'échange d'informations entre les autorités publiques compétentes, y compris les autorités répressives et les autorités de résolution, le présent règlement devrait établir un régime solide de notification des incidents liés aux TIC dans le cadre duquel les exigences pertinentes remédieraient aux lacunes actuelles du droit sur les services financiers, et supprimerait les chevauchements et doubles emplois existant afin d'alléger les coûts. Il est essentiel d'harmoniser le régime de notification des incidents liés aux TIC en imposant à toutes les entités financières de les notifier à leurs autorités compétentes au moyen d'un cadre rationalisé unique défini dans le présent règlement. En outre, les AES devraient être habilitées à préciser davantage les éléments nécessaires au cadre de notification des incidents liés aux TIC, tels que la taxinomie, les délais, les ensembles de données, les modèles et les seuils applicables. Pour veiller à une pleine cohérence avec la directive (UE) .../...[+], les entités financières devraient être autorisées à notifier, à titre volontaire, les cybermenaces importantes à l'autorité compétente concernée lorsqu'elles estiment que la cybermenace est pertinente pour le système financier, les utilisateurs de services ou les clients.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

(25) Les exigences en matière de tests de résilience opérationnelle numérique ont été renforcées dans certains sous-secteurs financiers, définissant des cadres qui ne sont pas toujours tout à fait harmonisés. Cette situation entraîne une potentielle multiplication des coûts pour les entités financières transfrontières et complique la reconnaissance mutuelle des résultats des tests de résilience opérationnelle numérique, ce qui, à son tour, peut fragmenter le marché intérieur.

(26) En outre, lorsqu'aucun test des TIC n'est requis, les vulnérabilités ne sont pas détectées et ont pour effet d'exposer l'entité financière au risque lié aux TIC et, en fin de compte, de créer un risque plus élevé pour la stabilité et l'intégrité du secteur financier. Sans une intervention au niveau de l'Union, les tests de résilience opérationnelle numérique demeureraient incompatibles et seraient dépourvus d'un système de reconnaissance mutuelle des résultats des tests des TIC d'un pays à l'autre. En outre, puisqu'il est peu probable que d'autres sous-secteurs financiers adoptent des mécanismes de test à une échelle significative, ils passeraient à côté des avantages qui peuvent découler d'un cadre de tests, en ce qui concerne la mise au jour des vulnérabilités et du risque lié aux TIC et le test des capacités de défense et de la continuité des activités, qui contribue à renforcer la confiance 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 le régime de tests et ainsi de faciliter la reconnaissance mutuelle des tests avancés pour les entités financières remplissant les critères énoncés dans le présent règlement.

(27) La dépendance des entités financières à l'égard de l'utilisation des services TIC 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 de TIC pour gérer des processus internes complexes.

(28) L'utilisation étendue des services TIC 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, même lorsque ces derniers sont inscrits dans leurs accords contractuels. En outre, nombre de ces accords contractuels 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 prestataires tiers de services TIC fournissent souvent des services standardisés à différents types de clients, ces accords contractuels ne répondent pas toujours de manière appropriée aux besoins individuels ou particuliers des acteurs du secteur financier.

(29) Bien que le droit de l'Union sur les services financiers contienne certaines règles générales sur l'externalisation, le suivi de la dimension contractuelle n'est pas pleinement consacré dans le droit de l'Union. En l'absence de normes de l'Union claires et adaptées applicables aux accords contractuels conclus avec des prestataires tiers de services TIC, la source extérieure du risque lié aux TIC 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 prestataires tiers de services TIC, qui revêtent une importance particulière lorsque les entités financières ont recours à des prestataires tiers de services TIC pour soutenir leurs fonctions critiques ou importantes. Ces principes devraient être assortis d'un ensemble de droits contractuels fondamentaux ayant trait à plusieurs éléments de l'exécution et de la résiliation des accords contractuels, en vue de consacrer certaines garanties minimales visant à renforcer la capacité des entités financières à assurer un suivi efficace de tous les risques liés aux TIC qui se posent au niveau des prestataires tiers de services. Ces principes complètent le droit sectoriel applicable à l'externalisation.

(30) Un certain manque d'homogénéité et de convergence en ce qui concerne le suivi des risques liés aux prestataires tiers de services TIC et de la dépendance à l'égard de ceux-ci est aujourd'hui évident. Malgré certains efforts pour couvrir l'externalisation, tels que les orientations de l'ABE de 2019 relatives à l'externalisation et les orientations de l'AEMF de 2021 relatives à la sous-traitance à des prestataires de services en nuage, la question plus large de la lutte contre le risque systémique qui peut être déclenché par l'exposition du secteur financier à un nombre limité de prestataires tiers critiques de services TIC n'est pas suffisamment pris en compte dans le droit de l'Union. Le manque de règles au niveau de l'Union est aggravé par l'absence de règles nationales en matière de mandats et d'outils qui permettent aux autorités de surveillance financière d'acquérir une solide compréhension des relations de dépendance à l'égard des prestataires tiers de services TIC afin d'assurer un suivi adéquat des risques découlant de la concentration de ces relations de dépendance.

(31) Compte tenu du risque systémique potentiel induit par des pratiques accrues d'externalisation et par la concentration des dépendances à l'égard des prestataires tiers de services TIC, et eu égard à l'insuffisance des mécanismes nationaux fournissant aux autorités de surveillance financière des outils adéquats permettant de quantifier et de qualifier le risque lié aux TIC se produisant chez les prestataires tiers critiques de services TIC et de remédier à leurs conséquences, il est nécessaire de mettre en place un cadre de supervision approprié permettant d'assurer un suivi continu des activités des prestataires tiers de services TIC qui sont des prestataires tiers critiques de services TIC pour les entités financières, tout en veillant à ce que la confidentialité et la sécurité des clients autres que les entités financières soient préservées. Bien que la fourniture de services TIC intra-groupe comporte des risques et des avantages spécifiques, elle ne devrait pas être automatiquement considérée comme moins risquée que la fourniture de services TIC par des prestataires extérieurs à un groupe financier, et devrait donc être soumise au même cadre réglementaire. Toutefois, lorsque les services TIC sont fournis au sein du même groupe financier, les entités financières peuvent avoir un contrôle plus strict sur les prestataires intra-groupe, ce qui doit être pris en considération dans l'évaluation générale des risques.

(32) Face à la complexité et à la sophistication croissantes du risque lié aux TIC, l'efficacité des mesures de détection et de prévention du risque lié aux TIC 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. Cela renforce à son tour la capacité des entités financières à empêcher les cybermenaces de devenir des incidents réels liés aux TIC et leur permet de contenir plus efficacement l'impact des incidents liés aux TIC et de se rétablir plus rapidement. En l'absence d'orientations au niveau de l'Union, plusieurs facteurs semblent avoir entravé ce partage de renseignements, notamment l'incertitude quant à sa compatibilité avec les règles en matière de protection des données, de pratiques anticoncurrentielles et de responsabilité.

(33) En outre, les doutes 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. Par conséquent, l'étendue et la qualité du partage d'informations demeurent actuellement limitées et fragmentées, puisque les échanges pertinents se font 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 système financier intégré. Il importe donc de renforcer ces canaux de communication.

(34) Les entités financières devraient être encouragées à échanger entre elles des informations et des renseignements sur les cybermenaces et 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, en participant à des dispositifs de partage d'information. 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 du secteur financier de prévenir les cybermenaces et d'y répondre collectivement en limitant rapidement la propagation du risque lié aux TIC et en empêchant une éventuelle contagion à travers les canaux financiers. Ces mécanismes devraient être conformes aux règles applicables du droit de la concurrence de l'Union énoncées dans la communication de la Commission du 14 janvier 2011 intitulée "Lignes directrices sur l'applicabilité de l'article 101 du traité sur le fonctionnement de l'Union européenne aux accords de coopération horizontale", ainsi qu'avec les règles de l'Union en matière de protection des données, en particulier le règlement (UE) 2016/679 du Parlement européen et du Conseil[1]. Ils devraient fonctionner sur la base du recours à une ou plusieurs des bases juridiques énoncées à l'article 6 dudit règlement, par exemple dans le cadre du traitement de données à caractère personnel qui est 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, ainsi que dans le cadre du traitement de données à caractère personnel qui est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, visé à l'article 6, paragraphe 1, points c) et e), respectivement, dudit règlement.

---

[1] 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).

(35) Afin de maintenir un niveau élevé de résilience opérationnelle numérique pour l'ensemble du secteur financier et, dans le même temps, de rester en phase avec les évolutions technologiques, le présent règlement devrait lutter contre le risque émanant de tous les types de services TIC. À cette fin, la définition des services TIC dans le contexte du présent règlement devrait être comprise de manière large, englobant les services numériques et de données fournis en continu par l'intermédiaire des systèmes de TIC à un ou plusieurs utilisateurs internes ou externes. Cette définition devrait, par exemple, inclure les services dits "par contournement", qui relèvent de la catégorie des services de communications électroniques. Elle ne devrait exclure que la catégorie limitée des services traditionnels de téléphonie analogique pouvant être considérés comme des services de réseau téléphonique commuté public (RTCP), des services de réseau fixe, un service téléphonique traditionnel (POTS) ou des services de téléphonie fixe.

(36) 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 leur taille et de leur profil de risque global. En règle générale, lorsqu'elles répartissent des ressources et des capacités aux fins de la mise en œuvre du cadre de gestion du risque lié aux TIC, les entités financières devraient assurer un juste équilibre entre leurs besoins liés aux TIC et leur taille et leur profil de risque global, ainsi que la nature, l'ampleur et la complexité de leurs services, activités et opérations, tandis que les autorités compétentes devraient poursuivre l'évaluation et le réexamen de l'approche suivie pour cette répartition.

(37) Les prestataires de services d'information sur les comptes, visés à l'article 33, paragraphe 1, de la directive (UE) 2015/2366, sont explicitement inclus dans le champ d'application du présent règlement, compte tenu de la nature spécifique de leurs activités et des risques qui en découlent. En outre, les établissements de monnaie électronique et les établissements de paiement exemptés en vertu de l'article 9, paragraphe 1, de la directive 2009/110/CE du Parlement européen et du Conseil[1] et de l'article 32, paragraphe 1, de la directive (UE) 2015/2366 sont inclus dans le champ d'application du présent règlement même s'ils n'ont pas obtenu un agrément les autorisant à émettre de la monnaie électronique conformément à la directive 2009/110/CE ou s'ils n'ont pas obtenu un agrément les autorisant à fournir et à exécuter des services de paiement conformément à la directive (UE) 2015/2366. Toutefois, les offices des chèques postaux, visés à l'article 2, paragraphe 5, point 3), de la directive 2013/36/UE du Parlement européen et du Conseil[2], sont exclus du champ d'application du présent règlement. L'autorité compétente pour les établissements de paiement exemptés en vertu de la directive (UE) 2015/2366, les établissements de monnaie électronique exemptés en vertu de la directive 2009/110/CE et les prestataires de services d'information sur les comptes visés à l'article 33, paragraphe 1, de la directive (UE) 2015/2366 devrait être l'autorité compétente désignée conformément à l'article 22 de la directive (UE) 2015/2366.

---

[1] 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).

[2] Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

(38) Étant donné que les grandes entités financières pourraient disposer de ressources plus importantes et 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 prestataires tiers de services TIC ou à la gestion des crises, pour organiser leur gestion du risque lié aux TIC selon le modèle reposant sur trois lignes de défense, ou pour établir un modèle de gestion des risques et de contrôle internes, et pour soumettre leur cadre de gestion du risque lié aux TIC aux audits internes.

(39) Certaines entités financières bénéficient d'exemptions ou sont soumises à un cadre réglementaire très léger en vertu du droit sectoriel applicable de l'Union. Ces entités financières comprennent les gestionnaires de fonds d'investissement alternatifs visés à l'article 3, paragraphe 2, de la directive 2011/61/UE du Parlement européen et du Conseil[1], les entreprises d'assurance et de réassurance visées à l'article 4 de la directive 2009/138/CE du Parlement européen et du Conseil[2] et les institutions de retraite professionnelle gérant des régimes de retraite qui, ensemble, n'ont pas plus de 15 affiliés au total. Compte tenu de ces exemptions, il ne serait pas proportionné d'inclure ces entités financières dans le champ d'application du présent règlement. En outre, le présent règlement tient compte des spécificités de la structure du marché de l'intermédiation en assurance, de sorte que les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire qui sont considérés comme des microentreprises ou des petites ou moyennes entreprises ne devraient pas relever du présent règlement.

(40) Étant donné que les entités visées à l'article 2, paragraphe 5, points 4) à 23), de la directive 2013/36/UE sont exclues du champ d'application de ladite directive, les États membres devraient par conséquent pouvoir choisir d'exempter de l'application du présent règlement lesdites entités qui sont situées sur leur territoire respectif.

---

[1] Directive 2011/61/UE du Parlement européen et du Conseil du 8 juin 2011 sur les gestionnaires de fonds d'investissement alternatifs et modifiant les directives 2003/41/CE et 2009/65/CE ainsi que les règlements (CE) n° 1060/2009 et (UE) n° 1095/2010 (JO L 174 du 1.7.2011, p. 1).

[2] Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II) (JO L 335 du 17.12.2009, p. 1).

(41) De la même manière, afin que le présent règlement corresponde au champ d'application de la directive 2014/65/UE du Parlement européen et du Conseil[1], il convient également d'exclure du champ d'application du présent règlement les personnes physiques et morales visées aux articles 2 et 3 de ladite directive qui sont autorisées à fournir des services d'investissement sans être tenues d'obtenir un agrément en vertu de la directive 2014/65/UE. Toutefois, l'article 2 de la directive 2014/65/UE exclut également du champ d'application de ladite directive les entités qui sont considérées comme des entités financières aux fins du présent règlement, telles que les dépositaires centraux de titres, les organismes de placement collectif ou les entreprises d'assurance et de réassurance. L'exclusion du champ d'application du présent règlement des personnes et entités visées aux articles 2 et 3 de ladite directive ne devrait pas concerner ces dépositaires centraux de titres, organismes de placement collectif ou entreprises d'assurance et de réassurance.

---

[1] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349).

(42) En vertu du droit sectoriel de l'Union, certaines entités financières sont soumises à des exigences moins strictes ou à des exemptions pour des raisons liées à leur taille ou aux services qu'elles fournissent. Cette catégorie d'entités financières inclut les petites entreprises d'investissement non interconnectées, les petites institutions de retraite professionnelle qui peuvent être exclues du champ d'application de la directive (UE) 2016/2341 dans les conditions prévues à l'article 5 de ladite directive par l'État membre concerné et qui gèrent des régimes de pension qui, ensemble, n'ont pas plus de 100 affiliés au total, ainsi que les institutions exemptées en vertu de la directive 2013/36/UE. Par conséquent, conformément au principe de proportionnalité et afin de préserver l'esprit du droit sectoriel de l'Union, il convient également de soumettre ces entités financières à un cadre simplifié de gestion du risque lié aux TIC en vertu du présent règlement. Le caractère proportionné du cadre de gestion du risque lié aux TIC couvrant ces entités financières ne devrait pas être modifié par les normes techniques de réglementation qui doivent être élaborées par les AES. De plus, conformément au principe de proportionnalité, il convient de soumettre également les établissements de paiement visés à l'article 32, paragraphe 1, de la directive (UE) 2015/2366 et les établissements de monnaie électronique visés à l'article 9 de la directive 2009/110/CE exemptés conformément aux dispositions de droit national transposant ces actes juridiques de l'Union à un cadre simplifié de gestion du risque lié aux TIC en vertu du présent règlement, tandis que les établissements de paiement et les établissements de monnaie électronique qui n'ont pas été exemptés conformément aux dispositions de leur droit national respectif transposant le droit sectoriel de l'Union devraient respecter le cadre général établi par le présent règlement.

(43) De la même manière, les entités financières qui sont considérées comme des microentreprises ou sont soumises au cadre simplifié de gestion du risque lié aux TIC en vertu du présent règlement ne devraient pas être tenues d'instituer un rôle de suivi des accords qu'elles ont conclu avec des prestataires tiers de services TIC sur l'utilisation des services TIC, ni de désigner un membre de la direction générale chargé de superviser l'exposition aux risques connexe et la documentation pertinente, de confier la responsabilité de la gestion et de la surveillance du risque lié aux TIC à une fonction de contrôle et de veiller à un niveau approprié d'indépendance de cette fonction de contrôle afin d'éviter les conflits d'intérêts, de documenter et de réexaminer au moins une fois par an le cadre de gestion du risque lié aux TIC, de soumettre le cadre de gestion du risque lié aux TIC à un audit interne régulier, d'effectuer des évaluations approfondies après des changements majeurs dans leurs infrastructures de réseau et de système d'information et les procédures, de procéder régulièrement à des analyses de risque sur les systèmes de TIC hérités, de soumettre la mise en œuvre des plans de réponse et de rétablissement des TIC à des audits internes indépendants, à disposer d'une fonction de gestion de crise, à 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 de TIC principale vers les installations redondantes, de communiquer aux autorités compétentes, à leur demande, une estimation des coûts et des pertes annuels agrégés causés par des incidents majeurs liés aux TIC, de maintenir des capacités en matière de TIC redondantes, de communiquer aux autorités nationales compétentes les changements mis en œuvre à la suite des examens post-incident lié aux TIC, d'assurer un suivi continu des évolutions technologiques pertinentes, d'établir un programme solide et complet de tests de résilience opérationnelle numérique, qui fait partie intégrante du cadre de gestion du risque lié aux TIC prévu par le présent règlement, ou d'adopter et de régulièrement réexaminer une stratégie en matière de risques liés aux prestataires tiers de services TIC.

En outre, les microentreprises ne devraient être tenues d'évaluer la nécessité de maintenir ces capacités en matière de TIC redondantes qu'en se fondant sur leur profil de risque. Les microentreprises devraient faire l'objet d'un régime plus flexible en ce qui concerne les programmes de test de résilience opérationnelle numérique. Lorsqu'elles examinent le type et la fréquence des tests à effectuer, elles devraient trouver un juste équilibre entre l'objectif consistant à maintenir une résilience opérationnelle numérique élevée, les ressources disponibles et leur profil de risque global. Les microentreprises et les entités financières soumises au cadre simplifié de gestion du risque lié aux TIC au titre du présent règlement devraient être exemptées de l'obligation de procéder à des tests avancés d'outils de TIC, de systèmes de TIC et de processus de TIC sur la base de tests de pénétration fondés sur la menace, étant donné que seules les entités financières remplissant les critères énoncés dans le présent règlement devraient être tenues de procéder à ces tests. Compte tenu de leurs capacités limitées, les microentreprises devraient pouvoir convenir avec le prestataire tiers de services TIC de déléguer les droits d'accès, d'inspection et d'audit de l'entité financière à un tiers indépendant, à désigner par le prestataire tiers de services TIC, à condition que l'entité financière soit en mesure de demander, à tout moment, toutes les informations et garanties sur la performance du prestataire tiers de services TIC auprès du tiers indépendant.

(44) Étant donné que seules les entités reconnues 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 supportés par un petit pourcentage d'entités financières.

(45) Pour garantir une concordance complète et une cohérence globale entre les stratégies d'entreprise des entités financières, d'une part, et la mise en œuvre de la gestion du risque lié aux TIC, d'autre part, les organes de direction des entités financières devraient être tenus de conserver un rôle actif et déterminant dans la conduite et l'adaptation du cadre de gestion du risque lié aux TIC et de la stratégie globale de résilience opérationnelle numérique. L'approche adoptée par les organes de direction devrait non seulement être axée sur les moyens de garantir la résilience des systèmes de TIC, 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 du risque lié aux TIC 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 du risque lié aux TIC.

(46) De plus, le principe de la responsabilité entière et ultime de l'organe de direction en ce qui concerne la gestion du risque lié aux TIC de l'entité financière va de pair avec la nécessité de mobiliser des investissements liés aux TIC et un budget global pour l'entité financière qui lui permettraient d'atteindre un niveau élevé en matière de résilience opérationnelle numérique.

(47) S'inspirant des bonnes pratiques, lignes directrices, recommandations et approches internationales, nationales et sectorielles pertinentes en matière de gestion du cyberrisque, le présent règlement promeut un ensemble de principes facilitant la structure globale de la gestion du risque lié aux TIC. Par conséquent, tant que les principales capacités mises en place par les entités financières abordent les différentes fonctions associées à la gestion du risque lié aux TIC (identification, protection et prévention, détection, réponse et rétablissement, apprentissage et évolution et communication) définies dans le présent règlement, les entités financières devraient rester libres d'utiliser des modèles de gestion du risque lié aux TIC qui sont formulés ou classés différemment.

(48) Afin de rester en phase avec l'évolution des cybermenaces, les entités financières devraient maintenir des systèmes de TIC à jour qui soient fiables et capables non seulement de garantir le traitement des données requis pour leurs services, mais aussi d'assurer une résilience technologique suffisante pour leur permettre de faire face de manière adéquate aux besoins de traitement supplémentaires résultant d'épisodes de tensions sur les marchés ou d'autres situations défavorables.

(49) 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 aux TIC, en particulier les cyberattaques, en limitant les dégâts et en donnant la priorité à la reprise des activités et aux mesures de rétablissement conformément à leurs politiques de sauvegarde. Toutefois, cette reprise ne doit en aucun cas compromettre la disponibilité, l'authenticité, l'intégrité ou la sécurité des données.

(50) Si le présent règlement laisse aux entités financières une certaine latitude pour définir leurs objectifs en matière de délai et de point de rétablissement et, partant, pour fixer ces objectifs en tenant pleinement compte de la nature et de la criticité des fonctions concernées et de tout besoin spécifique, il devrait néanmoins leur imposer de mener une évaluation des incidences globales potentielles sur l'efficience du marché lors de la détermination de ces objectifs.

(51) Les propagateurs de cyberattaques cherchent généralement des gains financiers directement à la source, exposant ainsi les entités financières à des répercussions importantes. Pour prévenir toute perte d'intégrité des systèmes de TIC ou toute indisponibilité de ceux-ci, et ainsi éviter toute violation de données et tout dommage à l'infrastructure physique de TIC, les entités financières devraient améliorer et rationaliser considérablement la notification des incidents majeurs liés aux TIC. La notification des incidents liés aux TIC devrait être harmonisée par l'introduction d'une obligation pour toutes les entités financières de soumettre une notification directement à leurs autorités compétentes concernées. Lorsqu'une entité financière est soumise à une surveillance par plus d'une autorité compétente nationale, les États membres devraient désigner une seule autorité compétente comme destinataire de cette notification. Les établissements de crédit classés comme importants conformément à l'article 6, paragraphe 4, du règlement (UE) n° 1024/2013 du Conseil[1] devraient soumettre cette notification à l'autorité compétente nationale, qui devrait ensuite transmettre le rapport à la Banque centrale européenne (BCE).

---

[1] Règlement (UE) n° 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).

(52) La notification directe devrait permettre aux autorités de surveillance financière d'avoir un accès immédiat aux informations sur les incidents majeurs liés aux TIC. Les autorités de surveillance financière devraient à leur tour transmettre des informations détaillées sur les incidents majeurs liés aux TIC aux autorités non financières publiques (telles que les autorités compétentes et les points de contact uniques relevant de la directive (UE) .../...[+], les autorités nationales de protection des données et les services répressifs pour les incidents majeurs de nature criminelle liés aux TIC), afin de sensibiliser ces autorités à ces incidents et, dans le cas des CSIRT, de faciliter la fourniture d'une assistance rapide aux entités financières, le cas échéant. Les États membres devraient en outre être en mesure de déterminer que les entités financières elles-mêmes devraient fournir ces informations aux autorités publiques en dehors du domaine des services financiers. Ces flux d'information devraient permettre aux entités financières de bénéficier rapidement de toute contribution technique pertinente, de conseils sur les mesures correctives et d'un suivi ultérieur de la part de ces autorités. Les informations sur les incidents majeurs liés aux TIC 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 cybermenaces et les vulnérabilités liées à un incident, afin de contribuer à la défense collective au sens large.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

(53) Toutes les entités financières devraient être tenues de notifier des incidents, mais cette obligation ne devrait pas toutes les concerner de la même manière. En effet, les seuils d'importance significative, ainsi que les délais de notification, devraient être dûment fixés, dans le contexte des actes délégués fondés sur les normes techniques de réglementation qui doivent être élaborées par les AES, de manière à ne rendre compte que des incidents majeurs liés aux TIC. En outre, il convient de tenir compte des spécificités des entités financières lors de la fixation du calendrier des obligations de notification.

(54) Le présent règlement devrait imposer aux établissements de crédit, aux établissements de paiement, aux prestataires de services d'information sur les comptes et aux établissements de monnaie électronique de signaler tous les incidents opérationnels ou de sécurité liés au paiement qui ont été précédemment signalés au titre de la directive (UE) 2015/2366, que l'incident soit ou non lié aux TIC.

(55) Les AES devraient être chargées d'examiner la faisabilité et les conditions de la possibilité de centraliser les rapports sur les incidents liés aux TIC au niveau de l'Union. Cette centralisation pourrait consister en une plateforme unique de l'Union en matière de notification des incidents majeurs liés aux TIC, qui soit recevrait directement les rapports pertinents et en informerait automatiquement les autorités nationales compétentes, soit se contenterait de centraliser les rapports pertinents que lui transmettraient les autorités nationales compétentes et assumerait donc un rôle de coordination. Les AES devraient être chargées d'élaborer, en consultation avec la BCE et l'ENISA, un rapport conjoint évaluant la faisabilité de la création d'une plateforme unique de l'Union.

(56) Dans le but d'assurer un niveau élevé de résilience opérationnelle numérique, et conformément aux normes internationales pertinentes (par exemple, les éléments fondamentaux du G7 concernant les tests de pénétration fondés sur la menace) ainsi qu'aux cadres appliqués dans l'Union, tels que le TIBER-EU, les entités financières devraient tester régulièrement leurs systèmes de TIC et leur personnel ayant des responsabilités liées aux TIC 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 divers sous-secteurs financiers et au sein de ceux-ci en ce qui concerne le niveau de préparation des entités financières à la cybersécurité, les tests devraient comprendre un large éventail d'outils et d'actions, allant de l'évaluation des exigences de base (par exemple, évaluations et analyses de la vulnérabilité, analyses de 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 au moyen de tests de pénétration fondés sur la menace. Ces tests avancés ne devraient être requis que pour les entités financières qui sont suffisamment matures du point de vue des TIC pour raisonnablement effectuer de tels tests. Les tests de résilience opérationnelle numérique requis par le présent règlement devraient donc être plus exigeants pour les entités financières remplissant les critères énoncés dans le présent règlement (par exemple, les grands établissements de crédit systémiques et matures du point de vue des TIC, les bourses, les dépositaires centraux de titres et les contreparties centrales) que pour les autres entités financières. Dans le même temps, les tests de résilience opérationnelle numérique effectués au moyen de tests de pénétration fondés sur la menace devraient être plus pertinents pour les entités financières qui exercent des activités dans les sous-secteurs essentiels des services financiers et qui jouent un rôle systémique(par exemple, les paiements, les services bancaires et les services de compensation et de règlement), et moins pertinents pour d'autres sous-secteurs (par exemple, les gestionnaires d'actifs et les agences de notation de crédit).

(57) Les entités financières qui participent à des activités transfrontières et 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 (à savoir des tests de pénétration fondés sur la menace) dans leur État membre d'origine, qui devraient englober toutes les infrastructures de TIC que ces groupes financiers transfrontières détiennent dans les différentes juridictions dans lesquelles ils opèrent au sein de l'Union, ce qui permettrait à ces groupes financiers transfrontières de ne supporter les coûts associés aux tests liés aux TIC que dans une seule juridiction.

(58) Afin de tirer parti de l'expertise déjà acquise par certaines autorités compétentes, en particulier en ce qui concerne la mise en œuvre du cadre TIBER-EU, le présent règlement devrait permettre aux États membres de désigner une autorité publique unique comme responsable dans le secteur financier, au niveau national, de toutes les questions relatives aux tests de pénétration fondés sur la menace, ou aux autorités compétentes de déléguer, en l'absence d'une telle désignation, la réalisation des tâches liées à ces tests à une autre autorité financière nationale compétente.

(59) Étant donné que le présent règlement n'exige pas des entités financières qu'elles couvrent toutes les fonctions critiques ou importantes dans le cadre d'un test unique de pénétration fondé sur la menace, les entités financières devraient être libres de déterminer combien de fonctions critiques ou importantes, et lesquelles, devraient être incluses dans le champ d'application de ce test.

(60) Les tests groupés au sens du présent règlement, dans le cadre desquels plusieurs entités financières participent à un test de pénétration fondé sur la menace et un prestataire tiers de services TIC peut conclure des accords contractuels directement avec un testeur externe, ne devraient être autorisés que lorsque l'on peut raisonnablement s'attendre à ce que la qualité ou la sécurité des services fournis par le prestataire tiers de services TIC à des clients qui sont des entités ne relevant pas du champ d'application du présent règlement ou la confidentialité des données relatives à de tels services subissent une incidence négative. Les tests groupés devraient également être soumis à des garanties (direction par une entité financière désignée, précision du nombre d'entités financières participantes) afin de veiller à ce que l'exercice de test soit rigoureux pour les entités financières participantes qui satisfont aux objectifs du test de pénétration fondé sur la menace conformément au présent règlement.

(61) Afin de tirer parti des ressources internes disponibles au niveau de l'entreprise, le présent règlement devrait autoriser le recours à des testeurs internes aux fins de la réalisation de tests de pénétration fondés sur la menace, sous réserve de l'accord des autorités de contrôle, de l'absence de conflit d'intérêts et de l'alternance périodique entre le recours à des testeurs internes et à des testeurs externes (tous les trois tests), tout en exigeant que le fournisseur de renseignements sur les menaces dans le test soit toujours externe à l'entité financière. L'exécution des tests de pénétration fondés sur la menace devrait continuer de relever de la responsabilité intégrale de l'entité financière. Les attestations délivrées par les autorités ne devraient être fournies qu'à des fins de reconnaissance mutuelle et ne devraient empêcher aucune action de suivi nécessaire pour faire face au risque lié aux TIC auquel l'entité financière est exposée, ni être considérées comme une validation par les autorités de surveillance des capacités de gestion et d'atténuation du risque lié aux TIC d'une entité financière.

(62) Afin d'assurer un suivi efficace du risque lié aux prestataires tiers de services TIC dans le secteur financier, il convient d'établir un ensemble de règles de principe destinées à guider les entités financières lors du suivi des risques engendrés par l'externalisation de fonctions à des prestataires tiers de services TIC, en particulier pour les services TIC qui soutiennent des fonctions critiques ou importantes, ainsi que, plus généralement, par les relations de dépendance à l'égard de tous les prestataires tiers de services TIC.

(63) Afin de remédier à la complexité des différentes sources du risque lié aux TIC, tout en tenant compte de la multitude et de la diversité des fournisseurs de solutions technologiques qui permettent une fourniture sans accrocs de services financiers, le présent règlement devrait couvrir un large éventail de prestataires tiers de services TIC, y compris les fournisseurs de services d'informatique en nuage, de logiciels, de services d'analyse de données et les fournisseurs de services de centres de données. De la même manière, étant donné que les entités financières devraient identifier et gérer de manière efficace et cohérente tous les types de risques, y compris dans le contexte des services TIC acquis au sein d'un groupe financier, il convient de préciser que les entreprises qui font partie d'un groupe financier et fournissent des services TIC principalement à leur entreprise mère, ou à des filiales ou succursales de leur entreprise mère, ainsi que les entités financières fournissant des services TIC à d'autres entités financières, devraient également être considérées comme des prestataires tiers de services TIC au titre du présent règlement. Enfin, compte tenu de l'évolution du marché des services de paiement, qui dépend de plus en plus de solutions techniques complexes, et des types émergents de services de paiement et de solutions liées au paiement, les participants à l'écosystème des services de paiement, qui exercent des activités de traitement du paiement ou exploitent des infrastructures de paiement, devraient également être considérés comme des prestataires tiers de services TIC au titre du présent règlement, à l'exception des banques centrales lorsqu'elles exploitent des systèmes de paiement ou de règlement des opérations sur titres et des autorités publiques lorsqu'elles fournissent des services liés aux TIC dans le contexte de l'exercice de fonctions de l'État.

(64) Une entité financière devrait à tout moment demeurer pleinement responsable du respect des obligations qui lui incombent en vertu du présent règlement. Les entités financières devraient adopter une approche proportionnée du suivi des risques survenant au niveau des prestataires tiers de services TIC en tenant dûment compte de la nature, de l'ampleur, de la complexité et de l'importance de leurs relations de dépendance liées aux TIC, 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.

(65) La réalisation de ce suivi devrait se fonder sur une approche stratégique du risque lié aux prestataires tiers de services TIC, laquelle serait formalisée par l'adoption, par l'organe de direction de l'entité financière, d'une stratégie dédiée en matière de risques liés aux prestataires tiers de services TIC reposant sur une analyse continue de toutes les relations de dépendance à l'égard de tous les prestataires tiers de services TIC. Afin que les autorités de surveillance cernent mieux les relations de dépendance à l'égard de prestataires tiers de services TIC, et en vue d'appuyer les travaux menés dans le contexte du cadre de supervision établi par le présent règlement, toutes les entités financières devraient être tenues de disposer d'un registre d'informations contenant tous les accords contractuels relatifs à l'utilisation des services TIC fournis par des prestataires tiers de services TIC. Les autorités de surveillance financière devraient pouvoir demander le registre complet, ou en demander des parties spécifiques, et ainsi obtenir des informations essentielles pour améliorer leur compréhension des relations de dépendance des entités financières à l'égard de prestataires tiers de services TIC.

(66) Une analyse précontractuelle approfondie devrait étayer et précéder la conclusion formelle des accords contractuels, en particulier en se concentrant sur des éléments tels que la criticité ou l'importance des services faisant l'objet du contrat TIC envisagé, les accords nécessaires des autorités de contrôle ou d'autres conditions, l'éventuel risque de concentration encouru, ainsi qu'en appliquant la diligence requise dans le processus de sélection et d'évaluation des prestataires tiers de services TIC et en analysant les éventuels conflits d'intérêts. En ce qui concerne les accords contractuels portant sur des fonctions critiques ou importantes, les entités financières devraient prendre en considération l'utilisation par les prestataires tiers de services TIC des normes les plus actualisées et les plus élevées en matière de sécurité de l'information. La résiliation des accords contractuels pourrait être déclenchée à tout le moins par un ensemble de circonstances révélant des insuffisances au niveau du prestataire tiers de services TIC, notamment des violations des dispositions législatives ou contractuelles, des circonstances révélant une possible altération de l'exécution des fonctions prévues par les accords contractuels, des faiblesses avérées du prestataire tiers de services TIC dans sa gestion globale du risque lié aux TIC, ou des circonstances indiquant l'incapacité de l'autorité compétente concernée à surveiller efficacement l'entité financière.

(67) Afin de remédier à l'effet systémique du risque de concentration des prestataires tiers de services TIC, le présent règlement privilégie une solution équilibrée au moyen d'une approche souple et progressive en ce qui concerne ce risque de concentration, car l'imposition de tout plafond rigide ou de toute limitation stricte serait susceptible d'entraver la conduite des affaires et de restreindre la liberté contractuelle. Les entités financières devraient procéder à une évaluation rigoureuse des accords contractuels qu'elles envisagent afin de déterminer la probabilité qu'un tel risque apparaisse, y compris au moyen d'analyses approfondies des accords de sous-traitance, en particulier lorsqu'ils sont conclus avec des prestataires tiers de services TIC 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 règles concernant des plafonds et des limites stricts pour les expositions aux prestataires tiers de services TIC. Dans le contexte du cadre de supervision, un superviseur principal nommé conformément au présent règlement devrait, en ce qui concerne les prestataires tiers critiques de services TIC, veiller tout particulièrement à saisir pleinement l'ampleur des interdépendances, à détecter les cas spécifiques dans lesquels un degré élevé de concentration de prestataires tiers critiques de services TIC dans l'Union est susceptible de mettre à mal la stabilité et l'intégrité du système financier de l'Union et à maintenir un dialogue avec les prestataires tiers critiques de services TIC lorsque ce risque spécifique est avéré.

(68) Afin d'évaluer et de contrôler régulièrement la capacité du prestataire tiers de services TIC à fournir en toute sécurité des services à une entité financière sans effets préjudiciables sur la résilience opérationnelle numérique d'une entité financière, plusieurs éléments contractuels clés avec les prestataires tiers de services TIC devraient être harmonisés. Cette harmonisation devrait couvrir les domaines minimaux qui sont fondamentaux pour permettre à l'entité financière d'assurer un suivi complet des risques qui pourraient apparaître chez le prestataire tiers de services TIC, dans la perspective de la nécessité d'une entité financière de garantir sa résilience numérique, car celle-ci dépend fortement de la stabilité, de la fonctionnalité, de la disponibilité et de la sécurité des services TIC reçus.

(69) Lorsqu'elles renégocient les accords contractuels en vue de les faire correspondre aux exigences du présent règlement, les entités financières et les prestataires tiers de services TIC devraient veiller à ce que les principales dispositions contractuelles prévues par le présent règlement soient couvertes.

(70) La définition de "fonction critique ou importante" figurant dans le présent règlement englobe la définition des "fonctions critiques" figurant à l'article 2, paragraphe 1, point 35, de la directive 2014/59/UE du Parlement européen et du Conseil[1]. Par conséquent, les fonctions considérées comme critiques en vertu de la directive 2014/59/UE sont incluses dans la définition des fonctions critiques au sens du présent règlement.

---

[1] Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement et modifiant la directive 82/891/CEE du Conseil ainsi que les directives du Parlement européen et du Conseil 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE et 2013/36/UE et les règlements du Parlement européen et du Conseil (UE) n° 1093/2010 et (UE) n° 648/2012 (JO L 173 du 12.6.2014, p. 190).

(71) Indépendamment de la criticité ou de l'importance de la fonction que sous-tendent les services TIC, 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 seront traitées, ainsi qu'une description des niveaux de service. Parmi les autres éléments essentiels pour permettre à une entité financière de procéder au suivi des risques liés aux prestataires tiers de services TIC figurent les dispositions contractuelles précisant en quoi l'accessibilité, la disponibilité, l'intégrité, la sécurité et la protection des données à caractère personnel sont assurées par le tiers prestataire de services TIC, les dispositions établissant les garanties pertinentes permettant l'accès, la récupération et la restitution des données en cas d'insolvabilité, de résolution ou d'interruption des activités du prestataire tiers de services TIC, ainsi que les dispositions imposant au prestataire tiers de services TIC de fournir une assistance en cas d'incidents liés aux TIC en rapport avec les services fournis, sans frais supplémentaires ou à un coût déterminé ex ante; les dispositions relatives à l'obligation pour le prestataire tiers de services TIC de coopérer pleinement avec les autorités compétentes et les autorités de résolution de l'entité financière; et les dispositions relatives aux droits de résiliation et aux délais de préavis minimaux correspondant pour la résiliation de l'accord contractuel, conformément aux attentes des autorités compétentes et des autorités de résolution.

(72) Outre ces dispositions contractuelles, et afin que les entités financières conservent la pleine maîtrise de toutes les évolutions survenant au niveau des tiers et susceptibles de nuire à leur sécurité des TIC, il convient que les contrats de fourniture de services TIC qui soutiennent des fonctions critiques ou importantes prévoient également les éléments suivants: des descriptions complètes des niveaux de service, ainsi que des objectifs de performance quantitatifs et qualitatifs précis, pour prendre sans retard injustifié des mesures correctives appropriées lorsque les niveaux de service convenus ne sont pas atteints; les délais de préavis pertinents et les obligations de notification incombant au prestataire tiers de services TIC en cas d'évolutions susceptibles d'avoir une incidence significative sur la capacité de ce dernier à fournir efficacement leurs services TIC respectifs; l'obligation pour le prestataire tiers de services TIC 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 des TIC qui permettent une prestation de services sûre, et de participer et de coopérer pleinement au test de pénétration fondé sur la menace effectué par l'entité financière.

(73) Les contrats de fourniture de services TIC qui soutiennent des fonctions critiques ou importantes devraient également contenir des dispositions permettant l'exercice des droits d'accès, d'inspection et d'audit par l'entité financière ou par un tiers désigné, et le droit de prendre des copies en tant qu'outils essentiels pour permettre aux entités financières d'assurer un suivi permanent des performances du prestataire tiers de services TIC, parallèlement à la coopération totale de ce prestataire de services lors des inspections. De la même manière, l'autorité compétente de l'entité financière devrait être habilitée, moyennant préavis, à inspecter et à auditer le prestataire tiers de services TIC, dans le respect de la protection des informations confidentielles.

(74) Ces accords contractuels devraient également 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 prestataires tiers de services TIC seraient tenus de continuer à fournir les services concernés en vue de réduire le risque de perturbations au niveau de l'entité financière, de permettre à celle-ci de passer à l'utilisation d'autres prestataires tiers de services TIC, ou encore de recourir à des solutions en interne, en fonction de la complexité du service TIC fourni. En outre, les entités financières relevant du champ d'application de la directive 2014/59/UE devraient veiller à ce que les contrats de services TIC pertinents soient solides et pleinement exécutoires en cas de résolution de ces entités financières. Par conséquent, conformément aux attentes des autorités de résolution, ces entités financières devraient veiller à ce que les contrats de services TIC pertinents soient résilients en matière de résolution. Tant qu'elles continuent d'honorer leurs obligations de paiement, ces entités financières devraient faire en sorte, entre autres exigences, que les contrats de services TIC pertinents comportent des clauses de non-résiliation, de non-suspension et de non-modification pour des motifs de restructuration ou de résolution.

(75) En outre, le recours volontaire aux clauses contractuelles types élaborées par les autorités publiques ou les institutions de l'Union, en particulier le recours aux clauses contractuelles élaborées par la Commission pour les services d'informatique en nuage pourrait procurer un degré accru de confiance aux entités financières et aux prestataires tiers de services TIC, en améliorant le niveau de sécurité juridique relatif à l'utilisation des services d'informatique en nuage dans le secteur financier, dans le respect total des exigences et des attentes définies par le droit de l'Union sur les services financiers. L'élaboration de clauses contractuelles types 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.

(76) Afin de promouvoir la convergence et l'efficacité des approches des autorités de surveillance lorsqu'elles traitent le risque lié aux prestataires tiers de services TIC dans le secteur financier, ainsi que de renforcer la résilience opérationnelle numérique des entités financières qui dépendent de prestataires tiers critiques de services TIC pour la prestation de services TIC qui soutiennent la fourniture de services financiers, et de contribuer ainsi à préserver la stabilité du système financier de l'Union et l'intégrité du marché intérieur des services financiers, les prestataires tiers critiques de services TIC devraient être soumis à un cadre de supervision de l'Union. Bien que la mise en place du cadre de supervision soit justifiée par la valeur ajoutée d'une action au niveau de l'Union et en vertu du rôle et des spécificités inhérents à l'utilisation des services TIC dans la fourniture de services financiers, il convient dans le même temps de rappeler que cette solution ne semble appropriée que dans le contexte du présent règlement, qui traite spécifiquement de la résilience opérationnelle numérique dans le secteur financier. Toutefois, ce cadre de supervision ne devrait pas être considéré comme un nouveau modèle de surveillance par l'Union dans les domaines des services et activités financiers.

(77) Le cadre de supervision ne devrait s'appliquer qu'aux prestataires tiers critiques de services TIC. Un mécanisme de désignation devrait donc 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 prestataires tiers de services TIC. Ce mécanisme devrait consister en un ensemble de critères quantitatifs et qualitatifs définissant les paramètres de criticité servant de référence aux fins de l'inclusion dans le cadre de supervision. Afin de veiller à l'exactitude de cette évaluation, et indépendamment de la structure sociale du prestataire tiers de services TIC, ces critères devraient, dans le cas d'un prestataire tiers de services TIC faisant partie d'un groupe plus large, prendre en considération l'ensemble de la structure du groupe du prestataire tiers de services TIC. D'une part, les prestataires tiers critiques de services TIC, qui ne sont pas automatiquement désignés par suite de l'application de ces critères, devraient avoir la possibilité d'adhérer au cadre de supervision à titre volontaire; d'autre part, les prestataires tiers de services TIC, qui sont déjà soumis à des cadres de supervision à l'appui de la réalisation des missions du Système européen de banques centrales visées à l'article 127, paragraphe 2, du traité sur le fonctionnement de l'Union européenne, devraient en être exemptés.

(78) De la même manière, les entités financières fournissant des services TIC à d'autres entités financières, bien qu'appartenant à la catégorie des prestataires tiers de services TIC au titre du présent règlement, devraient également être exemptées du cadre de supervision étant donné qu'elles sont déjà soumises aux mécanismes de surveillance établis par le droit de l'Union applicable aux services financiers. Le cas échéant, les autorités compétentes devraient tenir compte, dans le contexte de leurs activités de surveillance, du risque lié aux TIC que les entités financières fournissant des services TIC représentent pour les entités financières. De même, en raison des mécanismes de suivi des risques existants au niveau du groupe, la même exemption devrait être instaurée pour les prestataires tiers de services TIC qui fournissent des services principalement aux entités de leur propre groupe. Les prestataires tiers de services TIC fournissant des services TIC uniquement dans un État membre à des entités financières qui ne sont actives que dans cet État membre devraient également être exemptés du mécanisme de désignation en raison de leurs activités limitées et de l'absence d'incidence transfrontière.

(79) La transformation numérique que connaissent les services financiers a entraîné un niveau d'utilisation et de dépendance sans précédent à l'égard des services TIC. Étant donné qu'il est devenu inconcevable de fournir des services financiers sans recourir aux services d'informatique en nuage, aux solutions logicielles et aux services liés aux données, l'écosystème financier de l'Union est devenu intrinsèquement codépendant de certains services TIC fournis par des prestataires de services TIC. Certains de ces prestataires, innovants dans l'élaboration et l'application de technologies fondées sur les TIC, jouent un rôle considérable dans la fourniture de services financiers ou se sont intégrés dans la chaîne de valeur des services financiers. Ils sont donc devenus essentiels pour la stabilité et l'intégrité du système financier de l'Union. Cette dépendance généralisée à l'égard des services fournis par des prestataires tiers critiques de services TIC, associée à l'interdépendance des systèmes d'information de divers opérateurs de marché, crée un risque direct, et potentiellement grave, pour le système de services financiers de l'Union et pour la continuité de la fourniture des services financiers si des prestataires tiers critiques de services TIC venaient à subir des perturbations opérationnelles ou des cyberincidents majeurs. Les cyberincidents ont une capacité particulière à se multiplier et à se propager dans l'ensemble du système financier à un rythme beaucoup plus rapide que les autres types de risques faisant l'objet d'un suivi dans le secteur financier et peuvent s'étendre à d'autres secteurs et au-delà des frontières géographiques. Ils sont susceptibles d'évoluer en une crise systémique, dans le cadre de laquelle la confiance dans le système financier est érodée en raison de la perturbation des fonctions qui sous-tendent l'économie réelle ou de pertes financières considérables, atteignant un niveau auquel le système financier n'est pas en mesure de faire face, ou qui nécessite le déploiement d'importantes mesures d'absorption des chocs. Afin d'éviter que ces scénarios se produisent et mettent ainsi en péril la stabilité financière et l'intégrité de l'Union, il est essentiel de veiller à la convergence des pratiques de surveillance relatives aux risques liés aux prestataires tiers de services TIC dans le secteur financier, en particulier au moyen de nouvelles règles permettant à l'Union de superviser les prestataires tiers critiques de services TIC.

(80) Le cadre de supervision dépend dans une large mesure du degré de collaboration entre le superviseur principal et le prestataire tiers critique de services TIC fournissant aux entités financières des services ayant une incidence sur la fourniture de services financiers. Une supervision menée à bien repose notamment sur la capacité du superviseur principal à mener avec efficacité des missions de surveillance et des inspections afin d'évaluer les règles, les contrôles et les processus utilisés par les prestataires tiers critiques de services TIC, ainsi que pour évaluer les éventuelles incidences cumulées de leurs activités sur la stabilité financière et l'intégrité du système financier. Dans le même temps, il est essentiel que les prestataires tiers critiques de services TIC suivent les recommandations du superviseur principal et répondent à ses préoccupations. Étant donné que le manque de coopération d'un prestataire tiers critique de services TIC fournissant des services ayant une incidence sur la fourniture de services financiers, tel que le refus d'accorder l'accès à ses locaux ou de communiquer des informations, priverait en fin de compte le superviseur principal de ses outils essentiels lors de l'évaluation des risques liés aux prestataires tiers de services TIC et pourrait nuire à la stabilité financière et à l'intégrité du système financier, il est nécessaire de prévoir également un régime proportionné de sanctions.

(81) Dans ce contexte, la nécessité pour le superviseur principal d'imposer des astreintes pour contraindre les prestataires tiers critiques de services TIC à se conformer aux obligations en matière de transparence et d'accès énoncées dans le présent règlement ne devrait pas être compromise par les difficultés liées à l'exécution de ces astreintes en ce qui concerne les prestataires tiers critiques de services TIC établis dans des pays tiers. Afin de garantir le caractère exécutoire de ces astreintes, ainsi que de permettre une mise en œuvre rapide des procédures permettant de veiller au respect des droits de la défense des prestataires tiers critiques de services TIC dans le contexte du mécanisme de désignation et de la formulation de recommandations, ces prestataires tiers critiques de services TIC, qui fournissent à des entités financières des services ayant une incidence sur la fourniture de services financiers, devraient être tenus de maintenir une présence adéquate dans l'Union. En raison de la nature de la supervision, et de l'absence de dispositifs comparables dans d'autres juridictions, il n'existe aucun autre mécanisme approprié qui garantisse la réalisation de cet objectif au moyen d'une coopération efficace avec les autorités de surveillance financière des pays tiers en ce qui concerne la surveillance de l'incidence des risques opérationnels numériques que représentent les prestataires tiers systémiques de services TIC pouvant être considérés comme des prestataires tiers critiques de services TIC établis dans des pays tiers. Par conséquent, afin de continuer à fournir des services TIC à des entités financières dans l'Union, un prestataire tiers de services TIC établi dans un pays tiers qui a été désigné comme critique conformément au présent règlement devrait prendre, dans un délai de 12 mois à compter de cette désignation, toutes les dispositions nécessaires pour veiller à sa constitution dans l'Union, en établissant une filiale, définie dans l'ensemble de l'acquis de l'Union, notamment dans la directive 2013/34/UE du Parlement européen et du Conseil[1].

---

[1] Directive 2013/34/UE du Parlement européen et du Conseil du 26 juin 2013 relative aux états financiers annuels, aux états financiers consolidés et aux rapports y afférents de certaines formes d'entreprises, modifiant la directive 2006/43/CE du Parlement européen et du Conseil et abrogeant les directives 78/660/CEE et 83/349/CEE du Conseil (JO L 182 du 29.6.2013, p. 19).

(82) L'obligation de créer une filiale dans l'Union ne devrait pas empêcher le prestataire tiers critique de services TIC de fournir des services TIC et un appui technique connexe à partir d'installations et d'infrastructures situées en dehors de l'Union. Le présent règlement n'impose pas une localisation des données étant donné qu'il n'exige pas que le stockage ou le traitement des données soit effectué dans l'Union.

(83) Les prestataires tiers critiques de services TIC devraient être en mesure de fournir des services TIC depuis n'importe quel endroit du monde, pas nécessairement ou pas uniquement depuis des locaux situés dans l'Union. Les activités de supervision devraient d'abord être menées dans des locaux situés dans l'Union et en interaction avec des entités situées dans l'Union, y compris les filiales établies par des prestataires tiers critiques de services TIC conformément au présent règlement. Toutefois, ces actions au sein de l'Union pourraient ne pas suffire à permettre au superviseur principal de s'acquitter pleinement et efficacement de ses missions au titre du présent règlement. Le superviseur principal devrait donc également être en mesure d'exercer ses pouvoirs de supervision dans les pays tiers. L'exercice de ces pouvoirs dans les pays tiers devrait permettre au superviseur principal d'examiner les installations à partir desquelles les services TIC ou d'appui technique sont effectivement fournis ou gérés par le prestataire tiers critique de services TIC et offrir au superviseur principal une compréhension globale et opérationnelle de la gestion du risque lié aux TIC du prestataire tiers critique de services TIC. La possibilité pour le superviseur principal, en tant qu'agence de l'Union, d'exercer ses pouvoirs en dehors du territoire de l'Union devrait être dûment encadrée par des conditions pertinentes, en particulier le consentement du prestataire tiers critique de services TIC concerné. De même, les autorités compétentes du pays tiers devraient être informées de l'exercice des activités du superviseur principal sur leur propre territoire et ne pas s'y être opposées. Toutefois, afin de veiller à une mise en œuvre efficace, et sans préjudice des compétences respectives des institutions de l'Union et des États membres, ces pouvoirs doivent également être pleinement ancrés dans les accords de coopération administrative conclus avec les autorités compétentes du pays tiers concerné. Le présent règlement devrait donc permettre aux AES de conclure des accords de coopération administrative avec les autorités compétentes de pays tiers, qui ne devraient par ailleurs pas créer d'obligations juridiques à l'égard de l'Union et de ses États membres.

(84) Afin de faciliter la communication avec le superviseur principal et de veiller à une représentation adéquate, les prestataires tiers critiques de services TIC qui font partie d'un groupe devraient désigner une personne morale comme leur point de coordination.

(85) Le cadre de supervision devrait être sans préjudice de la compétence des États membres à mener leurs propres missions de supervision ou de surveillance des prestataires tiers de services TIC qui ne sont pas désignés comme critiques au titre du présent règlement, mais qui sont jugés importants au niveau national.

(86) Afin de tirer parti de l'architecture institutionnelle à plusieurs niveaux dans le domaine des services financiers, le comité mixte des AES devrait continuer à assurer la coordination intersectorielle globale pour toutes les questions relatives au risque lié aux TIC, conformément aux tâches qui lui incombent en matière de cybersécurité. Il devrait être soutenu par un nouveau sous-comité (ci-après dénommé "forum de supervision") chargé de préparer aussi bien les décisions individuelles à l'adresse des prestataires tiers critiques de services TIC que la publication des recommandations collectives, en particulier en ce qui concerne l'analyse comparative des programmes de supervision des prestataires tiers critiques de services TIC et l'identification des bonnes pratiques pour parer aux risques de concentration informatique.

(87) Afin que les prestataires tiers critiques de services TIC fassent l'objet d'une supervision appropriée et efficace à l'échelle de l'Union, le présent règlement prévoit que l'une des trois AES pourrait être désignée comme superviseur principal. L'assignation individuelle d'un prestataire tiers critique de services TIC à l'une des trois AES devrait découler d'une évaluation de la prépondérance des entités financières opérant dans les secteurs financiers pour lesquels cette AES assume des responsabilités. Cette approche devrait conduire à une répartition équilibrée des tâches et des responsabilités entre les trois AES, dans le contexte de l'exercice des fonctions de supervision, et devrait permettre une utilisation optimale des ressources humaines et de l'expertise technique disponibles dans chacune des trois AES.

(88) Les superviseurs principaux devraient se voir confier les pouvoirs nécessaires pour mener des enquêtes, réaliser des inspections sur place et hors site des locaux et sites des prestataires tiers critiques de services TIC et obtenir des informations complètes et actualisées. Ces pouvoirs devraient permettre au superviseur principal de se faire une idée précise du type, de la dimension et des incidences du risque que les prestataires tiers de services TIC représentent pour les entités financières et, en définitive, pour le système financier de l'Union. Il est indispensable d'accorder aux AES le rôle de superviseur principal afin de cerner et de prendre en compte la dimension systémique du risque lié aux TIC dans le secteur financier. L'incidence des prestataires tiers critiques de services TIC sur le secteur financier de l'Union et les problèmes éventuels causés par le risque de concentration informatique qui en découlent nécessitent l'adoption d'une approche collective au niveau de l'Union. La réalisation simultanée d'une multiplicité d'audits et de droits d'accès, exercés séparément par de nombreuses autorités compétentes avec une coordination limitée, voire inexistante, empêcherait les autorités de surveillance financière de disposer d'une vue d'ensemble complète et exhaustive du risque lié aux prestataires tiers de services TIC dans l'Union, tandis qu'elle engendrerait également une redondance, des charges et une complexité pour les prestataires tiers critiques de services TIC s'ils étaient confrontés à de nombreuses demandes de surveillance et d'inspection.

(89) En raison de l'incidence considérable de la désignation comme prestataire tiers critique, le présent règlement devrait veiller au respect des droits des prestataires tiers critiques de services TIC tout au long de la mise en œuvre du cadre de supervision. Avant d'être désignés comme critiques, ces prestataires devraient, par exemple, avoir le droit de présenter au superviseur principal une déclaration motivée contenant toute information pertinente aux fins de l'évaluation relative à leur désignation. Étant donné que le superviseur principal devrait être habilité à soumettre des recommandations sur le risque lié aux TIC et les mesures correctives appropriées, qui incluent le pouvoir de s'opposer à certains accords contractuels susceptibles d'affecter à terme la stabilité de l'entité financière ou du système financier, les prestataires tiers critiques de services TIC devraient également avoir la possibilité, avant la finalisation de ces recommandations, de fournir des explications en ce qui concerne l'incidence attendue des solutions, envisagées dans les recommandations, sur les clients qui sont des entités ne relevant pas du champ d'application du présent règlement et de formuler des solutions pour atténuer les risques. Les prestataires tiers critiques de services TIC qui ne sont pas d'accord avec les recommandations devraient présenter une déclaration motivée de leur intention de ne pas suivre la recommandation. Lorsque cette déclaration motivée fait défaut ou est jugée insuffisante, le superviseur principal devrait émettre une communication au public dans laquelle il décrit brièvement la non-conformité.

(90) Les autorités compétentes devraient dûment inclure la tâche consistant à vérifier le respect matériel des recommandations formulées par le superviseur principal dans le cadre de leurs fonctions en ce qui concerne la surveillance prudentielle des entités financières. Les autorités compétentes devraient pouvoir exiger des entités financières qu'elles prennent des mesures supplémentaires pour faire face aux risques recensés dans les recommandations du superviseur principal et devraient, en temps utile, émettre des notifications à cet effet. Lorsque le superviseur principal adresse des recommandations à des prestataires tiers critiques de services TIC qui font l'objet d'une surveillance au titre de la directive (UE) .../...[+], les autorités compétentes devraient pouvoir, à titre volontaire et avant d'adopter des mesures supplémentaires, consulter les autorités compétentes en vertu de ladite directive afin de favoriser une approche coordonnée concernant les prestataires tiers critiques de services TIC en question.

(91) L'exercice de la supervision devrait être fondé sur trois principes opérationnels visant: a) une coopération étroite entre les AES dans leur rôle de superviseur principal, au moyen d'un réseau de supervision commun, b) la cohérence avec le cadre établi par la directive (UE) .../...[+] (par une consultation volontaire des organismes relevant de ladite directive afin d'éviter la duplication des mesures visant les prestataires tiers critiques de services TIC), et c) l'application d'une diligence afin de réduire au minimum l'éventuel risque de perturbation des services fournis par les prestataires tiers critiques de services TIC aux clients qui sont des entités ne relevant pas du champ d'application du présent règlement.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

(92) Le cadre de supervision ne devrait pas remplacer, ni se substituer en aucune façon, même partiellement, à l'obligation pour les entités financières de gérer elles-mêmes les risques que comporte le recours à des prestataires tiers de services TIC, y compris leur obligation de maintenir un suivi permanent des accords contractuels conclus avec des prestataires tiers critiques de services TIC. De même, le cadre de supervision ne devrait changer en rien l'entière responsabilité qui incombe aux entités financières de se conformer à toutes les obligations juridiques énoncées dans le présent règlement et dans le droit applicable aux services financiers et de s'en acquitter.

(93) 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 prestataires tiers critiques de services TIC et devraient, à cet égard, se fonder sur l'évaluation du superviseur principal concerné. Toute mesure devrait en tout état de cause faire l'objet d'une coordination et d'un accord préalables avec le superviseur principal dans le contexte de l'exercice des missions du cadre de supervision.

(94) Dans le but de promouvoir la convergence au niveau international en ce qui concerne le recours aux bonnes pratiques dans le cadre de l'examen et du suivi de la gestion des risques numériques des prestataires tiers de services TIC, les AES devraient être encouragées à conclure des accords de coopération avec les autorités de pays tiers en matière de surveillance et de réglementation.

(95) Pour tirer parti des compétences, des aptitudes techniques et de l'expertise du personnel spécialisé dans le risque opérationnel et le risque lié aux TIC au sein des autorités compétentes, les trois AES et, à titre volontaire, les autorités compétentes en vertu de la directive (UE) .../...[+], et le superviseur principal devraient s'appuyer sur les capacités et les connaissances nationales dans le domaine de la surveillance et mettre en place des équipes d'examen spécifiques pour chaque prestataire tiers critique de services TIC, en constituant des équipes multidisciplinaires à l'appui de la préparation et de l'exécution des activités de supervision, y compris les enquêtes générales et les inspections auprès des prestataires tiers critiques de services TIC, ainsi que toute suite nécessaire à leur donner.

(96) Alors que les coûts résultant des tâches de supervision seraient entièrement financés par les redevances prélevées auprès des prestataires tiers critiques de services TIC, les AES sont toutefois susceptibles de supporter, avant le lancement du cadre de supervision, des coûts pour la mise en œuvre de systèmes de TIC spécifiques à l'appui de la future supervision, étant donné que des systèmes de TIC spécifiques devraient être développés et déployés au préalable. Le présent règlement prévoit donc un modèle de financement hybride, dans le cadre duquel le cadre de supervision serait, en tant que tel, entièrement financé par les redevances, tandis que le développement des systèmes de TIC des AES serait financé par des contributions des autorités compétentes nationales et de l'Union.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

(97) Les autorités compétentes devraient disposer de tous les pouvoirs de surveillance, d'enquête et de sanction requis pour garantir l'application du présent règlement. Elles devraient, en principe, publier des avis des sanctions administratives qu'elles imposent. Étant donné que les entités financières et les prestataires tiers de services TIC peuvent être établis dans des États membres différents et être soumis à la surveillance d'autorités compétentes différentes, l'application du présent règlement devrait être facilitée, d'une part, par la coopération entre les autorités compétentes concernées, y compris la BCE pour ce qui est des missions spécifiques qui lui sont conférées par le règlement (UE) n° 1024/2013 et, d'autre part, par une consultation avec les AES au moyen de l'échange réciproque d'informations et la fourniture d'une assistance mutuelle dans l'exercice des activités de surveillance concernées.

(98) Afin de mieux quantifier et qualifier les critères de désignation des prestataires tiers de services TIC comme critiques 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 compléter le présent règlement en précisant l'effet systémique qu'une défaillance ou une interruption de fonctionnement d'un prestataire tiers de services TIC pourrait avoir sur les entités financières auxquelles il fournit des services TIC, le nombre d'établissements d'importance systémique mondiale (EISm) ou d'autres établissements d'importance systémique (autres EIS) qui dépendent du prestataire tiers de services TIC concerné, le nombre de prestataires tiers de services TIC actifs sur un marché donné, les coûts de la migration des données et des charges de travail liées aux TIC vers d'autres prestataires tiers de services TIC, 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"[1]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil devraient recevoir tous les documents au même moment que les experts des États membres, et leurs experts devraient avoir systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

---

[1] JO L 123 du 12.5.2016, p. 1.

(99) Des normes techniques de réglementation devraient garantir l'harmonisation cohérente des exigences prévues par le présent règlement. Dans leur rôle en tant qu'organismes dotés de compétences très spécialisées, les AES devraient 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 du risque lié aux TIC, de la notification d'incidents majeurs liés aux TIC, des tests, ainsi qu'en ce qui concerne les exigences clés pour garantir un suivi solide du risque lié aux prestataires tiers de services TIC. 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 leur taille et à leur profil de risque global, ainsi qu'à la nature, à l'ampleur et à la complexité de leurs services, activités et opérations. La Commission devrait être habilitée à adopter ces normes techniques de réglementation par voie d'actes délégués en vertu de l'article 290 du traité sur le fonctionnement de l'Union européenne et conformément aux articles 10 à 14 des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

(100) Afin de faciliter la comparabilité des rapports sur les incidents majeurs liés aux TIC et les incidents opérationnels ou de sécurité majeurs liés au paiement, ainsi que de garantir la transparence des accords contractuels relatifs à l'utilisation de services TIC fournis par des prestataires tiers de services TIC, les AES devraient 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 aux TIC et un incident opérationnel ou de sécurité majeur lié au paiement, 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 le profil de risque global de l'entité financière, ainsi que la nature, l'ampleur et la complexité de ses services, activités et opérations. La Commission devrait être habilitée à adopter ces normes techniques d'exécution par voie 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) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

(101) 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) n° 1060/2009[1], (UE) n° 648/2012[2], (UE) n° 600/2014[3] et (UE) n° 909/2014[4] du Parlement européen et du Conseil, 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 du risque lié aux TIC.

---

1 Règlement (CE) n° 1060/2009 du Parlement européen et du Conseil du 16 septembre 2009 sur les agences de notation de crédit (JO L 302 du 17.11.2009, p. 1).

2 Règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (JO L 201 du 27.7.2012, p. 1).

3 Règlement (UE) n° 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) n° 648/2012 (JO L 173 du 2.66.2014, p. 84).

4 Règlement (UE) n° 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres, et modifiant les directives 98/26/CE et 2014/65/UE ainsi que le règlement (UE) n° 236/2012 (JO L 257 du 28.8.2014, p. 1).

(102) Étant donné que le présent règlement, conjointement avec la directive (UE) .../... du Parlement européen et du Conseil[1+], consiste en une consolidation des dispositions relatives à la gestion du risque lié aux TIC énoncées dans de multiples règlements et directives de l'acquis de l'Union dans le domaine des services financiers, notamment les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014 et (UE) n° 909/2014 et le règlement (UE) 2016/1011 du Parlement européen et du Conseil[2], il convient, afin de garantir une cohérence totale, de modifier lesdits règlements pour y préciser que les dispositions pertinentes applicables au risque lié aux TIC sont énoncées dans le présent règlement.

(103) En conséquence, le champ d'application des articles pertinents relatifs au risque opérationnel, pour lesquels des délégations de pouvoirs énoncées dans les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) n° 2016/1011 prévoyaient l'adoption d'actes délégués et d'actes d'exécution, devrait être restreint en vue de transférer dans le présent règlement toutes les dispositions relatives aux aspects de la résilience opérationnelle numérique qui font actuellement partie desdits règlements.

---

1 Directive (UE) .../... du Parlement européen et du Conseil du ... modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier (JO L ..., du ..., p. ...).

\+ JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 42/22 (2020/0268 (COD)).

2 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) n° 596/2014 (JO L 171 du 29.6.2016, p. 1).

(104) L'éventuel cyberrisque systémique associé à l'utilisation d'infrastructures de TIC permettant le fonctionnement des systèmes de paiement et la fourniture d'activités de traitement des paiements devrait être dûment traité au niveau de l'Union au moyen de règles harmonisées en matière de résilience numérique. À cet effet, la Commission devrait évaluer rapidement la nécessité de réexaminer le champ d'application du présent règlement tout en alignant ce réexamen sur les résultats du réexamen exhaustif prévu par la directive (UE) 2015/2366. De nombreuses attaques à grande échelle survenues au cours des dix dernières années montrent que les systèmes de paiement sont exposés aux cybermenaces. Placés au cœur de la chaîne des services de paiement et forts de solides interconnexions avec l'ensemble du système financier, les systèmes de paiement et les activités de traitement des paiements ont acquis une importance cruciale pour le fonctionnement des marchés financiers de l'Union. Les cyberattaques menées contre ces systèmes peuvent entraîner de graves perturbations opérationnelles des activités ayant des répercussions directes sur les fonctions économiques essentielles, telles que la facilitation des paiements, et des effets indirects sur les processus économiques connexes. Jusqu'à ce qu'un régime harmonisé et la supervision des opérateurs de systèmes de paiement et des entités de traitement soient mis en place au niveau de l'Union, les États membres peuvent, en vue d'appliquer des pratiques de marché similaires, s'inspirer des exigences en matière de résilience opérationnelle numérique prévues par le présent règlement lorsqu'ils appliquent des règles aux opérateurs de systèmes de paiement et aux entités de traitement supervisées dans leur propre juridiction.

(105) Étant donné que l'objectif du présent règlement, à savoir atteindre un niveau élevé de résilience opérationnelle numérique pour toutes les entités financières réglementées, ne peut pas être atteint de manière suffisante par les États membres, puisqu'il suppose d'harmoniser différentes règles du droit de l'Union et du droit national, mais qu'il peut, en raison de ses dimensions et de ses 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.

(106) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil[1] et a rendu un avis le 10 mai 2021[2],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

---

[1] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

[2] JO C 229 du 15.6.2021, p. 16.

Chapitre I
Dispositions générales

Article premier

Objet

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

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

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

      ii) la notification, aux autorités compétentes, des incidents majeurs liés aux TIC et la notification, à titre volontaire, des cybermenaces importantes aux autorités compétentes;

      iii) la notification aux autorités compétentes, par les entités financières visées à l'article 2, paragraphe 1, points a) à d), des incidents opérationnels ou de sécurité majeurs liés au paiement;

      iv) les tests de résilience opérationnelle numérique;

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

vi) les mesures destinées à garantir la gestion saine du risque lié aux prestataires tiers de services TIC;

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

c) les règles relatives à l'établissement du cadre de supervision applicable aux prestataires tiers critiques de services TIC lorsqu'ils fournissent des services à des entités financières, ainsi que celles liées à l'exercice des tâches dans ce cadre;

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'entités essentielles ou importantes conformément aux dispositions nationales transposant l'article 3 de la directive (UE) .../...[+], le présent règlement est considéré comme un acte juridique sectoriel de l'Union aux fins de l'article 4 de ladite directive.

3. Le présent règlement est sans préjudice de la responsabilité des États membres pour ce qui est des fonctions essentielles de l'État en matière de sécurité publique, de défense et de sécurité nationale conformément au droit de l'Union.

[+] JO: veuillez insérer, dans le texte, le numéro de la directive figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

Article 2

Champ d'application

1. Sans préjudice des paragraphes 3 et 4, le présent règlement s'applique aux entités suivantes:

   a) les établissements de crédit;

   b) les établissements de paiement, y compris les établissements de paiement exemptés en vertu de la directive (UE) 2015/2366;

   c) les prestataires de services d'information sur les comptes;

   d) les établissements de monnaie électronique, y compris les établissements de monnaie électronique exemptés en vertu de la directive 2009/110/CE;

   e) les entreprises d'investissement;

   f) les prestataires de services sur crypto-actifs agréés en vertu du règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant les règlements (UE) n° 1093/2010 et (UE) n° 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 (ci-après dénommé "règlement sur les marchés de crypto-actifs") et les émetteurs de jetons se référant à un ou des actifs;

   g) les dépositaires centraux de titres;

h) les contreparties centrales;

i) les plates-formes de négociation;

j) les référentiels centraux;

k) les gestionnaires de fonds d'investissement alternatifs;

l) les sociétés de gestion;

m) les prestataires de services de communication de données;

n) les entreprises d'assurance et de réassurance;

o) les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire;

p) les institutions de retraite professionnelle;

q) les agences de notation de crédit;

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 prestataires tiers de services TIC.

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

3. Le présent règlement ne s'applique pas aux:

a) gestionnaires de fonds d'investissement alternatifs visés à l'article 3, paragraphe 2, de la directive 2011/61/UE;

b) entreprises d'assurance et de réassurance visées à l'article 4 de la directive 2009/138/CE;

c) institutions de retraite professionnelle qui gèrent des régimes de retraite qui, ensemble, ne comptent pas plus de 15 affiliés au total;

d) personnes physiques ou morales exemptées en vertu des articles 2 et 3 de la directive 2014/65/UE;

e) intermédiaires d'assurance, intermédiaires de réassurance et intermédiaires d'assurance à titre accessoire qui sont des microentreprises ou des petites ou moyennes entreprises;

f) offices des chèques postaux visés à l'article 2, paragraphe 5, point 3), de la directive 2013/36/UE.

4. Les États membres peuvent exclure du champ d'application du présent règlement les entités visées à l'article 2, paragraphe 5, points 4) à 23), de la directive 2013/36/UE qui sont situées sur leur territoire respectif. Lorsqu'un État membre fait usage de cette option, il en informe la Commission ainsi que de toute modification ultérieure. La Commission met ces informations à la disposition du public sur son site internet ou par d'autres moyens facilement accessibles.

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 et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC 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, y compris en cas de perturbations;

2) "réseau et système d'information": un réseau et système d'information au sens de l'article 6, point 1), de la directive (UE) …/…[+];

[+] JO: veuillez insérer, dans le texte, le numéro de la directive figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

3) "système de TIC hérité": un système de TIC qui a atteint la fin de son cycle de vie (fin de vie), qui ne se prête pas à des mises à jour ou des corrections, pour des raisons technologiques ou commerciales, ou qui n'est plus pris en charge par son fournisseur ou par un prestataire tiers de services TIC, mais qui est toujours utilisé et soutient les fonctions de l'entité financière;

4) "sécurité des réseaux et des systèmes d'information": la sécurité des réseaux et des systèmes d'information au sens de l'article 6, point 2), de la directive (UE) …/…[+];

5) "risque lié aux TIC": toute circonstance raisonnablement identifiable liée à l'utilisation des réseaux et des systèmes d'informationqui, 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 etdes processus ou de la fourniture de servicesen produisant des effets préjudiciables dans l'environnement numérique ou physique;

6) "actif informationnel": un ensemble d'informations, matérielles ou immatérielles, qui justifie une protection;

7) "actif de TIC": un actif logiciel ou matériel dans les réseaux et les systèmes d'informationutilisés par l'entité financière;

[+] JO: veuillez insérer, dans le texte, le numéro de la directive figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

8) "incident lié aux TIC": un événement ou une série d'événements liés entre eux que l'entité financière n'a pas prévu qui compromet la sécurité des réseaux et des systèmes d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou sur les services fournis par l'entité financière;

9) "incident opérationnel ou de sécurité lié au paiement": un événement ou une série d'événements liés entre eux que les entités financières visées à l'article 2, paragraphe 1, points a) à d), n'ont pas prévu, lié ou non aux TIC, qui a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données liées au paiement ou sur les services liés au paiement fournis par l'entité financière;

10) "incident majeur lié aux TIC": un incident lié aux TIC qui a une incidence négative élevée sur les réseaux et les systèmes d'information qui soutiennent les fonctions critiques ou importantes de l'entité financière;

11) "incident opérationnel ou de sécurité majeur lié au paiement": un incident opérationnel ou de sécurité lié au paiement qui a une incidence négative élevée sur les services fournis liés au paiement;

12) "cybermenace": une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;

13) "cybermenace importante": une cybermenace dont les caractéristiques techniques indiquent qu'elle pourrait donner lieu à un incident majeur lié aux TIC ou à un incident opérationnel ou de sécurité majeur lié au paiement;

14) "cyberattaque": un incident lié aux TIC malveillant causé par 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;

15) "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 permettre une compréhension pertinente et suffisante en vue d'atténuer les effets d'un incident lié aux TIC 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;

16) "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;

17) "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 critiques en environnement de production de l'entité financière;

18) "risque lié aux prestataires tiers de services TIC": un risque lié aux TIC auquel une entité financière peut être exposée du fait de son recours à des services TIC fournis par des prestataires tiers de services TIC ou par des sous-traitants, y compris au moyen d'accords d'externalisation;

19) "prestataire tiers de services TIC": une entreprise qui fournit des services TIC;

20) "prestataire de services TIC intra-groupe": une entreprise qui fait partie d'un groupe financier et qui fournit principalement des services TIC à des entités financières du même groupe ou à des entités financières appartenant au même système de protection institutionnel, y compris à leurs entreprises mères, filiales et succursales ou à d'autres entités détenues ou contrôlées par la même entité;

21) "services TIC": les services numériques et de données fournis de manière permanente par l'intermédiaire des systèmes de TIC à un ou plusieurs utilisateurs internes ou externes, dont le matériel en tant que service et les services matériels qui englobent la fourniture d'assistance technique au moyen de mises à jour de logiciels ou de micrologiciels réalisées par le fournisseur de matériel, à l'exclusion des services de téléphonie analogique traditionnels;

22) "fonction critique ou importante": une fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'une entité financière, ou à la solidité ou à la continuité de ses services et activités, ou une interruption, une anomalie ou une défaillance de l'exécution de cette fonction 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 du droit relatif aux services financiers;

23) "prestataire tiers critique de services TIC": un prestataire tiers de services TIC désigné comme étant critique conformément à l'article 31;

24) "prestataire tiers de services TIC établi dans un pays tiers": un prestataire tiers de services TIC qui est une personne morale établie dans un pays tierset qui a conclu un accord contractuel avec une entité financière pour la fourniture de services TIC;

25) "filiale": une entreprise filiale au sens de l'article 2, point 10), et de l'article 22 de la directive 2013/34/UE;

26) "groupe": un groupe au sens de l'article 2, point 11), de la directive 2013/34/UE;

27) "entreprise mère": une entreprise mère au sens de l'article 2, point 9), et de l'article 22 de la directive 2013/34/UE;

28) "sous-traitant de TIC établi dans un pays tiers": un sous-traitant de TIC qui est une personne morale établie dans un pays tierset qui a conclu un accord contractuel soit avec un prestataire tiers de services TIC, soit avec un prestataire tiers de services TIC établi dans un pays tiers;

29) "risque de concentration de TIC": une exposition à des prestataires tiers critiques de services TIC 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 financièreà assurer des fonctions critiques ou importantes, ou l'exposer à subir d'autres types d'effets préjudiciables, y compris des pertes importantes, ou mettre en péril la stabilité financière de l'Union dans son ensemble;

30) "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 du Parlement européen et du Conseil[1], de l'article 2, paragraphe 1, point 45), du règlement (UE) n° 909/2014, de l'article 3, paragraphe 1, point 20), du règlement (UE) 2016/1011, et de la disposition pertinente du règlement sur les marchés de crypto-actifs, ou les personnes assimilées qui dirigent effectivement l'entité ou qui exercent des fonctions clés conformément au droit de l'Union ou au droit national applicable;

---

[1] Directive 2009/65/CE du Parlement européen et du Conseil du 13 juillet 2009 portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières (OPCVM) (JO L 302 du 17.11.2009, p. 32).

31) "établissement de crédit": un établissement de crédit au sens de l'article 4, paragraphe 1, point 1), du règlement (UE) n° 575/2013 du Parlement européen et du Conseil[1];

32) "établissement exempté en vertu de la directive 2013/36/UE": une entité visée à l'article 2, paragraphe 5, points 4) à 23), de la directive 2013/36/UE;

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

34) "petite entreprise d'investissement non interconnectée": une entreprise d'investissement qui répond aux conditions énoncées à l'article 12, paragraphe 1, du règlement (UE) 2019/2033 du Parlement européen et du Conseil[2];

35) "établissement de paiement": un établissement de paiement au sens de l'article 4, point 4), de la directive (UE) 2015/2366;

36) "établissement de paiement exempté en vertu de la directive (UE) 2015/2366": un établissement de paiement bénéficiant d'une exemption au titre de l'article 32, paragraphe 1, de la directive (UE) 2015/2366;

37) "prestataires de services d'information sur les comptes": un prestataire de services d'information sur les comptes visé à l'article 33, paragraphe 1, de la directive (UE) 2015/2366;

---

[1] Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1).

[2] Règlement (UE) 2019/2033 du Parlement européen et du Conseil du 27 novembre 2019 concernant les exigences prudentielles applicables aux entreprises d'investissement et modifiant les règlements (UE) n° 1093/2010, (UE) n° 575/2013, (UE) n° 600/2014 et (UE) n° 806/2014 (JO L 314 du 5.12.2019, p. 1).

38) "établissement de monnaie électronique": un établissement de monnaie électronique au sens de l'article 2, point 1), de la directive 2009/110/CE;

39) "établissement de monnaie électronique exempté en vertu de la directive 2009/110/CE": un établissement de monnaie électronique bénéficiant d'une exemption visé à l'article 9, paragraphe 1, de la directive 2009/110/CE;

40) "contrepartie centrale": une contrepartie centrale au sens de l'article 2, point 1), du règlement (UE) n° 648/2012;

41) "référentiel central": un référentiel central au sens de l'article 2, point 2), du règlement (UE) n° 648/2012;

42) "dépositaire central de titres": un dépositaire central de titres au sens de l'article 2, paragraphe 1, point 1), du règlement (UE) n° 909/2014;

43) "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;

44) "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;

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

46) "prestataire de services de communication de données": un prestataire de services de communication de données au sens du règlement (UE) n° 600/2014, tel que visé à l'article 2, paragraphe 1, points 34 à 36, dudit règlement;

47) "entreprise d'assurance": une entreprise d'assurance au sens de l'article 13, point 1), de la directive 2009/138/CE;

48) "entreprise de réassurance": une entreprise de réassurance au sens de l'article 13, point 4), de la directive 2009/138/CE;

49) "intermédiaire d'assurance": un intermédiaire d'assurance au sens de l'article 2, paragraphe 1, point 3), de la directive (UE) 2016/97 du Parlement européen et du Conseil[1];

50) "intermédiaire d'assurance à titre accessoire": un intermédiaire d'assurance à titre accessoire au sens de l'article 2, paragraphe 1, point 4), de la directive (UE) 2016/97;

51) "intermédiaire de réassurance": un intermédiaire de réassurance au sens de l'article 2, paragraphe 1, point 5), de la directive (UE) 2016/97;

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

---

[1] Directive (UE) 2016/97 du Parlement européen et du Conseil du 20 janvier 2016 sur la distribution d'assurances (JO L 26 du 2.2.2016, p. 19).

53) "petite institution de retraite professionnelle": une institution de retraite professionnelle qui gère des régimes de retraite qui, ensemble, comptent moins de 100 affiliés au total;

54) "agence de notation de crédit": une agence de notation de crédit au sens de l'article 3, paragraphe 1, point b), du règlement (CE) n° 1060/2009;

55) "prestataire de services sur crypto-actifs": un prestataire de services sur crypto-actifs au sens de la disposition pertinente du règlement sur les marchés de crypto-actifs;

56) "émetteur de jetons se référant à un ou des actifs": un émetteur de jetons se référant à un ou des actifsau sens de la disposition pertinente du règlement sur les marchés de crypto-actifs;

57) "administrateur d'indices de référence d'importance critique": un administrateur d'"indices de référence d'importance critique" au sens de l'article 3, paragraphe 1, point 25, du règlement (UE) 2016/1011;

58) "prestataire de services de financement participatif": un prestataire de services de financement participatif au sens de l'article 2, paragraphe 1, point e), du règlement (UE) 2020/1503 du Parlement européen et du Conseil[1];

59) "référentiel des titrisations": un référentiel des titrisations au sens de l'article 2, point 23, du règlement (UE) 2017/2402 du Parlement européen et du Conseil[2];

---

[1] Règlement (UE) 2020/1503 du Parlement européen et du Conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs, et modifiant le règlement (UE) 2017/1129 et la directive (UE) 2019/1937 (JO L 347 du 20.10.2020, p. 1).

[2] Règlement (UE) 2017/2402 du Parlement européen et du Conseil du 12 décembre 2017 créant un cadre général pour la titrisation ainsi qu'un cadre spécifique pour les titrisations simples, transparentes et standardisées, et modifiant les directives 2009/65/CE, 2009/138/CE et 2011/61/UE et les règlements (CE) n° 1060/2009 et (UE) n° 648/2012 (JO L 347 du 28.12.2017, p. 35).

60) "microentreprise": une entité financière, autre qu'une plate-forme de négociation, une contrepartie centrale, un référentiel central ou un dépositaire central de titres, qui emploie moins de 10 personnes et dont le chiffre d'affaires annuel et/ou le total du bilan annuel n'excède pas 2 millions d'euros;

61) "superviseur principal": l'autorité européenne de surveillance désignée conformément à l'article 31, paragraphe 1, point b), du présent règlement;

62) "comité mixte": le comité visé à l'article 54 des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010;

63) "petite entreprise": une entité financière entreprise qui emploie dix personnes ou plus mais moins de cinquante personnes et dont le chiffre d'affaires annuel et/ou le total du bilan annuel dépasse 2 millions d'euros mais n'excède pas 10 millions d'euros;

64) "moyenne entreprise": une entité financière qui n'est pas une petite entreprise et qui emploie moins de 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros et/ou dont le bilan annuel n'excède pas 43 millions d'euros;

65) "autorité publique": tout gouvernement ou toute autre entité de l'administration publique, y compris les banques centrales nationales.

Article 4

Principe de proportionnalité

1. Les entités financières mettent en œuvre les règles énoncées au chapitre II conformément au principe de proportionnalité, en tenant compte de leur taille et de leur profil de risque global ainsi que de la nature, de l'ampleur et de la complexité de leurs services, activités et opérations.

2. En outre, l'application par les entités financières des chapitres III et IV et du chapitre V, section I, est proportionnée à leur taille et à leur profil de risque global, ainsi qu'à la nature, à l'ampleur et à la complexité de leurs services, activités et opérations, comme le prévoient expressément les règles pertinentes desdits chapitres.

3. Les autorités compétentes tiennent compte de l'application du principe de proportionnalité par les entités financières lorsqu'elles examinent la cohérence du cadre de gestion du risque lié aux TIC sur la base des rapports présentés à la demande des autorités compétentes conformément à l'article 6, paragraphe 5, et à l'article 16, paragraphe 2.

Chapitre II
Gestion du risque lié aux TIC

SECTION I

Article 5

Gouvernance et organisation

1. Les entités financières disposent d'un cadre de gouvernance et de contrôle interne qui garantit une gestion efficace et prudente du risque lié aux TIC, conformément à l'article 6, paragraphe 4, en vue d'atteindre un niveau élevé de résilience opérationnelle numérique.

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 du risque lié aux TIC visé à l'article 6, paragraphe 1.

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

   a) assume la responsabilité ultime de la gestion du risque lié aux TIC de l'entité financière;

   b) met en place des stratégies visant à garantir le maintien de normes élevées en matière de disponibilité, d'authenticité, d'intégrité et de confidentialité des données;

c) définit clairement les rôles et les responsabilités pour toutes les fonctions liées aux TIC et met en place des dispositifs de gouvernance appropriés pour assurer une communication, une coopération et une coordination efficaces et en temps utile entre ces fonctions;

d) assume la responsabilité globale de la définition et de l'approbation de la stratégie de résilience opérationnelle numérique visée à l'article 6, paragraphe 8, y compris la détermination du niveau approprié de tolérance au risque lié aux TIC de l'entité financière, tel que visé à l'article 6, paragraphe 8, point b);

e) approuve, supervise et examine périodiquement la mise en œuvre de la politique de continuité des activités de TIC de l'entité financière et des plans de réponse et de rétablissement des TIC visés, respectivement, à l'article 11, paragraphes 1 et 3, qui peuvent être adoptés en tant que politique spécifique faisant partie intégrante de la politique globale de continuité des activités et du plan de réponse et de rétablissement de l'entité financière;

f) approuve et examine périodiquement les plans internes d'audit des TIC et les audits des TIC de l'entité financière ainsi que les modifications significatives qui y sont apportées;

g) 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 les programmes pertinents de sensibilisation à la sécurité des TIC et les formations pertinentes à la résilience opérationnelle numérique visés à l'article 13, paragraphe 6, et les compétences en matière de TIC pour l'ensemble du personnel;

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

i) met en place, au niveau de l'entreprise, des canaux de notification lui permettant d'être dûment informé des éléments suivants:

i) des accords conclus avec des prestataires tiers de services TIC sur l'utilisation des services TIC;

ii) de tout changement significatif pertinent prévu concernant les prestataires tiers de services TIC;

iii) des incidences potentielles de ces changements sur les fonctions critiques ou importantes faisant l'objet de ces accords, notamment un résumé de l'analyse des risques visant à évaluer les incidences de ces changements, et au minimum des incidents majeurs liés aux TIC 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 prestataires tiers de services TIC sur l'utilisation des services TIC, 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 de l'entité financière maintiennent activement à jour des connaissances et des compétences suffisantes pour comprendre et évaluer le risque lié aux TIC et son incidence sur les opérations de l'entité financière, notamment en suivant régulièrement une formation spécifique proportionnée au risque lié aux TIC géré.

SECTION II

Article 6

Cadre de gestion du risque lié aux TIC

1. Les entités financières disposent d'un cadre de gestion du risque lié aux TIC solide, complet et bien documenté, faisant partie de leur système global de gestion des risques, qui leur permet de parer au risque lié aux TIC de manière rapide, efficiente et exhaustive et de garantir un niveau élevé de résilience opérationnelle numérique.

2. Le cadre de gestion du risque lié aux TIC englobe au moins les stratégies, les politiques, les procédures, les protocoles et les outils de TIC qui sont nécessaires pour protéger dûment et de manière appropriée tous les actifs informationnels et les actifs de TIC, y compris les logiciels, le matériel informatique, les serveurs, ainsi que toutes les composantes et infrastructures physiques pertinentes, telles queles locaux, centres de données et zones sensibles désignées, afin de garantir que tous les actifs informationnels et actifs de TIC sont correctement protégés contre les risques, y compris les dommages et les accès ou utilisations non autorisés.

3. Conformément à leur cadre de gestion du risque lié aux TIC, les entités financières réduisent au minimum l'incidence du risque lié aux TIC en déployant des stratégies, des politiques, des procédures, des protocoles et des outils de TIC adéquats. Elles fournissent des informations complètes et actualisées sur le risque lié aux TIC et sur leur cadre de gestion du risque lié aux TIC aux autorités compétentes à leur demande.

4. Les entités financières, autres que les microentreprises, confient la responsabilité de la gestion et de la surveillance du risque lié aux TIC à une fonction de contrôle et garantissent un niveau approprié d'indépendance de cette fonction de contrôle afin d'éviter les conflits d'intérêts. Les entités financières garantissent une séparation et une indépendance adéquates des fonctions de gestion du risque lié aux TIC, 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.

5. Le cadre de gestion du risque lié aux TIC est documenté et réexaminé au moins une fois par an, ou périodiquement pour les microentreprises, ainsi qu'en cas de survenance d'incidents majeurs liés aux ICT, 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. Un rapport sur le réexamen du cadre de gestion du risque lié aux TIC est présenté à l'autorité compétente à sa demande.

6. Le cadre de gestion du risque lié aux TIC des entités financières, autres que les microentreprises, fait l'objet d'audits internes réguliers réalisés par des auditeurs conformément au plan d'audit des entités financières. Ces auditeurs possèdent des connaissances, des compétences et une expertise suffisantes en matière de risque lié aux TIC, et font preuve d'une indépendance adéquate. La fréquence et l'objectif des audits des TIC sont proportionnés au risque lié aux TIC de l'entité financière.

7. Sur la base des conclusions de l'audit interne, les entités financières mettent en place un processus de suivi formel, comprenant des règles pour la vérification et la correction en temps utile des constatations d'importance critique de l'audit des TIC.

8. Le cadre de gestion du risque lié aux TIC comprend une stratégie de résilience opérationnelle numérique qui définit les modalités de mise en œuvre du cadre. À cette fin, la stratégie de résilience opérationnelle numérique précise les méthodes pour parer au risque lié aux TIC et atteindre des objectifs spécifiques en matière de TIC, en:

a) expliquant la manière dont le cadre de gestion du risque lié aux TIC soutient la stratégie d'entreprise et les objectifs de l'entité financière;

b) déterminant le niveau de tolérance au risque lié aux TIC, en fonction de l'appétit pour le risque de l'entité financière, et en analysant la tolérance à l'incidence des dysfonctionnements des TIC;

c) définissant des objectifs clairs en matière de sécurité de l'information, y compris des indicateurs de performance clés et des indicateurs de risque clés;

d) décrivant l'architecture des TIC de référence et les changements nécessaires pour atteindre des objectifs spécifiques de l'entité financière;

e) présentant les différents mécanismes mis en place pour détecter et prévenir les incidents liés aux TIC, ainsi que pour se protéger contre leurs effets;

f) déterminant la situation actuelle en matière de résilience opérationnelle numérique sur la base du nombre d'incidents majeurs liés aux TIC signalés et de l'efficacité des mesures de prévention;

g) mettant en œuvre des tests de résilience opérationnelle numérique, conformément au chapitre IV du présent règlement;

h) définissant une stratégie de communication en cas d'incidents liés aux TIC qui doivent être divulgués en vertu de l'article 14.

9. Les entités financières peuvent, dans le contexte de la stratégie de résilience opérationnelle numérique visée au paragraphe 8, définir une stratégie globale multi-fournisseurs en matière de TIC au niveau du groupe ou de l'entité, qui met en évidence les principales relations de dépendance à l'égard des prestataires tiers de services TIC et expose les raisons qui sous-tendent la combinaison de prestataires tiers de services TIC choisis.

10. Les entités financières peuvent, conformément au droit de l'Union et au droit sectoriel national, externaliser les tâches de vérification du respect des exigences en matière de gestion du risque lié aux TIC à des entreprises intra-groupe ou externes. Dans le cas d'une telle externalisation, l'entité financière reste pleinement responsable de la vérification du respect des exigences en matière de gestion du risque lié aux TIC.

Article 7

Systèmes, protocoles et outils de TIC

Afin d'atténuer et de gérer le risque lié aux TIC, les entités financières utilisent et tiennent à jour des systèmes, protocoles et outils de TIC qui sont:

a) adaptésà l'ampleur des opérations qui sous-tendent l'exercice de leurs activités, conformément au principe de proportionnalité visé à l'article 4;

b) fiables;

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

d) 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.

Article 8

Identification

1. Aux fins du cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1, les entités financières identifient, classent et documentent de manière adéquate toutes les fonctions "métiers", tous les rôles et toutes les responsabilités s'appuyant sur les TIC, les actifs informationnels et les actifs de TIC qui soutiennent ces fonctions, ainsi que leurs rôles et dépendances en ce qui concerne le risque lié aux TIC. Les entités financières examinent si nécessaire, et au moins une fois par an, le caractère adéquat de cette classification et de toute documentation pertinente.

2. Les entités financières identifient, de manière continue, toutes les sources de risque lié aux TIC, 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 des TIC qui concernent leurs fonctions "métiers" s'appuyant sur les TIC, leurs actifs informationnels et leurs actifs de TIC. 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 "métiers" s'appuyant sur les TIC, leurs actifs informationnels ou leurs actifs de TIC.

4. Les entités financières identifient tous les actifs informationnels et actifs de TIC, y compris ceux situés sur des sites extérieurs, les ressources du réseau et les équipements matériels, et répertorient ceux considérés comme critiques. Elles répertorient la configuration des actifs informationnels et des actifs de TIC et les liens et interdépendances entre les différents actifs informationnels et actifs de TIC.

5. Les entités financières identifient et documentent tous les processus qui dépendent de prestataires tiers de services TIC, et identifient les interconnexions avec des prestataires tiers de services TIC qui fournissent des services qui soutiennent des fonctions critiques ou importantes.

6. Aux fins des paragraphes 1, 4 et 5, les entités financières tiennent des inventaires pertinents et les mettent à jour périodiquement et chaque fois qu'a lieu une modification importante visée au paragraphe 3.

7. Les entités financières, autres que les microentreprises, procèdent régulièrement, et au moins une fois par an, à une évaluation spécifique du risque lié aux TIC sur tous les systèmes de TIC hérités, et, dans tous les cas, avant et après la connexion de technologies, d'applications ou de systèmes.

Article 9

Protection et prévention

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

2. Les entités financières conçoivent, acquièrent et mettent en œuvre des stratégies, des politiques, des procédures, des protocoles et des outils de sécurité de TIC qui visent à garantir la résilience, la continuité et la disponibilité des systèmes de TIC, en particulier ceux qui soutiennent des fonctions critiques ou importantes, et à maintenir des normes élevées en matière de disponibilité, d'authenticité, d'intégrité et de confidentialité 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 solutions et des processus de TIC qui sont appropriés conformément à l'article 4. Ces solutions et processus de TIC:

   a) garantissent la sécurité des moyens de transfert de données;

   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 le manque de disponibilité, les atteintes à l'authenticité et à l'intégrité, les violations de la confidentialité et la perte de données;

d) garantissent que les données sont protégées contre les risques découlant de la gestion des données, y compris une mauvaise administration, les risques relatifs au traitement et l'erreur humaine.

4. Aux fins du cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1, les entités financières:

a) élaborent et documentent une politique de sécurité de l'information qui définit des règles visant à protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, des actifs informationnels et des actifs de TIC, y compris ceux de leurs clients, le cas échéant;

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, qui peuvent inclure la mise en œuvre de mécanismes automatisés pour isoler les actifs informationnels affectés en cas de cyberattaques;

c) mettent en œuvre des politiques qui limitent l'accès physique ou logique aux actifs informationnels et aux actifs de TIC, à ce qui est nécessaire pour les fonctions et les activités légitimes et approuvées uniquement, et définissent à cette fin un ensemble de politiques, de procédures et de contrôles qui portent sur les droits d'accès et veillent à 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 spécifiques, et des mesures de protection des clés de chiffrement par lesquelles les données sont chiffrées sur la base des résultats des processus approuvés de classification des données et d'évaluation du risque lié aux TIC;

e) mettent en œuvre des politiques, des procédures et des contrôles documentés pour la gestion des changements dans les TIC, y compris les changements apportés aux logiciels, au matériel, aux composants de micrologiciels, aux systèmes ou aux paramètres de 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 de TIC sont consignés, testés, évalués, approuvés, mis en œuvre et vérifiés de manière contrôlée;

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

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

Aux fins du premier alinéa, point e), le processus de gestion des changements dans les TIC est approuvé par la structure hiérarchique appropriée et comporte des protocoles spécifiques.

Article 10

Détection

1. Les entités financières mettent en place des mécanismes permettant de détecter rapidement les activités anormales, conformément à l'article 17, y compris les problèmes de performance des réseaux de TIC et les incidents liés aux TIC, ainsi que de repérer les points uniques de défaillance potentiellement significatifs.

   Tous les mécanismes de détection visés au premier alinéa sont régulièrement testés conformément à l'article 25.

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 et de lancement des processus de réponse en cas d'incident lié aux TIC, y compris des mécanismes d'alerte automatique destinés au personnel compétent chargé de la réponse aux incidents liés aux TIC.

3. Les entités financières consacrent des ressources et des capacités suffisantes pour surveiller l'activité des utilisateurs, l'apparition d'anomalies liées aux TIC et d'incidents liés aux TIC, en particulier les cyberattaques.

4. Les prestataires de services de communication de données 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 de ces déclarations.

Article 11

Réponse et rétablissement

1. Aux fins du cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1, et sur la base des exigences en matière d'identification énoncées à l'article 8, les entités financières se dotent d'une politique de continuité des activités de TIC complète, qui peut être adoptée en tant que politique spécifique, et qui forme une partie intégrante de leur politique globale de continuité des activités.

2. Les entités financières mettent en œuvre la politique de continuité des activités de TIC au moyen de dispositifs, de plans, de procédures et de mécanismes spécifiques, appropriés et documentés visant à:

   a) garantir la continuité des fonctions critiques ou importantes de l'entité financière;

   b) répondre aux incidents liés aux TIC et les résoudre rapidement, dûment et efficacement de manière à limiter les dommages et à donner la priorité à la reprise des activités et aux mesures de rétablissement;

   c) activer, sans retard, des plans spécifiques permettant de déployer des mesures, des processus et des technologies d'endiguement adaptés à chaque type d'incident lié aux TIC et de prévenir tout dommage supplémentaire, ainsi que des procédures sur mesure de réponse et rétablissement, définies conformément à l'article 12;

d) estimer les incidences, les dommages et les pertes préliminaires;

e) 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 14, et leur déclaration aux autorités compétentes, conformément à l'article 19.

3. Aux fins du cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1, les entités financières mettent en œuvre des plans de réponse et de rétablissement des TIC qui, dans le cas des entités financières, autres que les microentreprises, font l'objet de revues indépendantes de l'audit interne.

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

5. Dans le cadre de la politique globale de continuité des activités, les entités financières procèdent à une analyse des incidences sur les activités de leurs expositions à de graves perturbations de leurs activités. Dans le cadre de cette analyse, les entités financières évaluent l'incidence potentielle de graves perturbations de leurs activités au moyen de critères quantitatifs et qualitatifs, à l'aide de données internes et externes et d'une analyse de scénarios, le cas échéant. L'analyse des incidences sur les activités tient compte du caractère critique des fonctions "métiers", des processus de soutien, des dépendances de tiers et des actifs informationnels identifiés et cartographiés, ainsi que de leurs interdépendances. Les entités financières veillent à ce que les actifs de TIC et les services TIC soient conçus et utilisés dans le respect total de l'analyse des incidences sur les activités, en particulier en garantissant de manière adéquate la redondance de toutes les composantes critiques.

6. Dans le cadre de leur gestion globale du risque lié aux TIC, les entités financières:

a) testent les plans de continuité des activités de TIC et les plans de réponse et de rétablissement des TIC concernant les systèmes de TIC soutenant toutes les fonctions au moins une fois par an ainsi qu'en cas de modifications substantielles apportées aux systèmes de TIC qui soutiennent des fonctions critiques ou importantes;

b) testent les plans de communication en situation de crise établis conformément à l'article 14.

Aux fins du premier alinéa, 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 de TIC principale et la capacité redondante, les sauvegardes et les installations redondantes nécessaires pour satisfaire aux obligations énoncées à l'article 12.

Les entités financières réexaminent régulièrement leur politique de continuité des activités de TIC et leurs plans de réponse et de rétablissement des TIC 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.

7. Les entités financières, autres que les microentreprises, disposent d'une fonction de gestion de crise qui, en cas d'activation de leurs plans de continuité des activités de TIC ou de leurs plans de réponse et de rétablissement des TIC, définit, entre autres, des procédures claires pour gérer les communications internes et externes en situation de crise, conformément à l'article 14.

8. Les entités financières tiennent un registre, facile d'accès, des activités avant et pendant les perturbations lorsque leurs plans de continuité des activités de TIC et leurs plans de réponse et de rétablissement des TIC sont activés.

9. Les dépositaires centraux de titres fournissent aux autorités compétentes des copies des résultats des tests de continuité des activités de TIC ou d'exercices similaires.

10. Les entités financières, autres que les microentreprises, communiquent aux autorités compétentes, à leur demande, une estimation des coûts et pertes annuels agrégés occasionnés par des incidents majeurs liés aux TIC.

11. Conformément à l'article 16 des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010, les AES, agissant par l'intermédiaire du comité mixte, élaborent, au plus tard le ... [18 mois à compter de la date d'entrée en vigueur du présent règlement], des orientations communes sur l'estimation des coûts et pertes annuels agrégés visés au paragraphe 10.

Article 12

Politiques et procédures de sauvegarde, procédures et méthodes de restauration et de rétablissement

1. Dans le but de veiller à la restauration des systèmes et des données des TIC en limitant au maximum la durée d'indisponibilité, les perturbations et les pertes, aux fins de leur cadre de gestion du risque lié aux TIC, les entités financières définissent et documentent:

   a) des politiques et procédures 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 niveau de confidentialité des données;

   b) des procédures et méthodes de restauration et de rétablissement.

2. Les entités financières mettent en place des systèmes de sauvegarde qui peuvent être activés conformément aux politiques et procédures de sauvegarde, ainsi qu'aux procédures et méthodes de restauration et de rétablissement. L'activation de systèmes de sauvegarde ne compromet pas la sécurité du réseau et des systèmes d'information ni la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données. Des tests des procédures de sauvegarde et des procédures et méthodes de restauration et de rétablissement sont effectués périodiquement.

3. Lorsqu'elles restaurent des données de sauvegarde à l'aide de leurs propres systèmes, les entités financières utilisent des systèmes de TIC qui sont séparés physiquement et logiquement du système de TIC source. Les systèmes de TIC sont protégés de manière sécurisée contre tout accès non autorisé ou toute corruption des TIC et permettent la restauration en temps utile des services grâce à la sauvegarde des données et des systèmes si nécessaire.

Dans le cas des contreparties centrales, 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.

Les prestataires de services de communication de données maintiennent en outre des ressources adéquates et disposent de dispositifs de sauvegarde et de restauration afin d'offrir et de maintenir leurs services à tout moment.

4. Les entités financières, autres que les microentreprises, maintiennent des capacités en matière de TIC redondantes dotées de ressources, de capacités et de fonctions adéquates pour répondre à leurs besoins. Les microentreprises évaluent la nécessité de maintenir ces capacités en matière de TIC redondantes en se fondant sur leur profil de risque.

5. Les dépositaires centraux de titres maintiennent au moins un site de traitement secondaire doté de ressources, de capacités, de fonctions et d'effectifs adéquats pour répondre à leurs besoins.

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 fonctions critiques ou importantes 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 fonctions critiques ou importantes en cas d'indisponibilité du site de traitement primaire.

6. Lorsqu'elles déterminent les objectifs en matière de délai de rétablissement et de point de rétablissement pour chaque fonction, les entités financières tiennent compte du caractère critique ou important de la fonction et 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 aux TIC, les entités financières effectuent les contrôles nécessaires, y compris tout contrôle multiple et rapprochement, 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 13

Apprentissage et évolution

1. Les entités financières disposent de capacités et d'effectifs pour recueillir des informations sur les vulnérabilités et les cybermenaces, et sur les incidents liés aux TIC, en particulier les cyberattaques, et analyser leurs incidences probables sur leur résilience opérationnelle numérique.

2. Les entités financières réalisent des examens post-incident lié aux TIC après qu'un incident majeur lié aux TIC a perturbé leurs activités principales, afin d'analyser les causes de la perturbation et de déterminer les améliorations à apporter aux opérations de TIC ou dans le cadre de la politique de continuité des activités de TIC visée à l'article 11.

Les entités financières, autres que les microentreprises, communiquent, sur demande, aux autorités compétentes les changements qui ont été apportés à la suite des examens post-incident lié aux TIC visés au premier alinéa.

Les examens post-incident lié aux TIC 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 aux TIC et de leur gravité;

b) la qualité et la rapidité de l'analyse technico-légale, le cas échéant;

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 26 et 27 et des incidents liés aux TIC en situation réelle, en particulier les cyberattaques, ainsi que les difficultés rencontrées lors de l'activation des plans de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC, 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 du risque lié aux TIC. Ces constatations permettent d'effectuer un examen approprié des composantes pertinentes du cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1.

4. Les entités financières contrôlent l'efficacité de la mise en œuvre de leur stratégie de résilience opérationnelle numérique définie à l'article 6, paragraphe 8. Elles retracent l'évolution du risque lié aux TIC dans le temps, analysent la fréquence, les types, l'ampleur et l'évolution des incidents liés aux TIC, en particulier les cyberattaques et leurs caractéristiques, afin de cerner le niveau d'exposition au risque lié aux TIC, en particulier en ce qui concerne les fonctions critiques ou importantes, et de renforcer la maturité et la préparation des TIC 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 des TIC et des formations à la résilience opérationnelle numérique qu'elles intègrent à leurs programmes de formation du personnel sous forme de modules obligatoires. Ces programmes et formations sont destinés à tous les employés et aux membres de la direction et présentent un niveau de complexité proportionné à leurs fonctions. Le cas échéant, les entités financières incluent également les prestataires tiers de services TIC dans leurs programmes de formation pertinents conformément à l'article 30, paragraphe 2, point i).

7. Les entités financières, autres que les microentreprises, assurent un suivi continu des évolutions technologiques pertinentes, notamment en vue de déterminer l'incidence que le déploiement de ces nouvelles technologies pourrait avoir sur les exigences en matière de sécurité des TIC et la résilience opérationnelle numérique. Elles se tiennent informées des processus de gestion du risque lié aux TIC les plus récents, afin de lutter efficacement contre les formes actuelles ou émergentes de cyberattaques.

Article 14

Communication

1. Aux fins du cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1, les entités financières mettent en place des plans de communication en situation de crise qui favorisent une divulgation responsable, au minimum, des incidents majeurs liés aux TIC ou des vulnérabilités majeures aux clients et aux contreparties ainsi qu'au public, le cas échéant.

2. Aux fins du cadre de gestion du risque lié aux TIC, les entités financières mettent en œuvre des politiques de communication à l'intention des membres du personnel interne 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 du risque lié aux TIC, en particulier le personnel responsable de la réponse et du rétablissement, et le personnel qui doit être informé.

3. Au moins une personne au sein de l'entité financière est chargée de mettre en œuvre la stratégie de communication concernant les incidents liés aux TIC et remplit la fonction d'information du public et des médias à cette fin.

Article 15

Harmonisation accrue des outils, méthodes, processus et politiques de gestion du risque lié aux TIC

Les AES élaborent, par l'intermédiaire du comité mixte, en concertation avec l'Agence de l'Union européenne pour la cybersécurité (ENISA), des projets communs de normes techniques de réglementation afin:

a) de préciser davantage les éléments à inclure dans les politiques, procédures, protocoles et outils de sécurité des TIC visés à l'article 9, 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 la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, y compris en recourant à des techniques cryptographiques, et de garantir une transmission précise et rapide des données sans perturbation majeure et sans retard injustifié;

b) d'approfondir les composantes relatives au contrôle des droits de gestion des accès visés à l'article 9, 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 au risque lié aux TIC au moyen d'indicateurs adéquats, notamment pour les manières d'utiliser le réseau et les heures d'utilisation du réseau, l'activité de TIC et les dispositifs inconnus;

c) d'approfondir les mécanismes précisés à l'article 10, paragraphe 1, qui permettent une détection rapide des activités anormales, ainsi que les critères définis à l'article 10, paragraphe 2, qui entraînent le déclenchement des processus de détection des incidents liés aux TIC et de réponse à ces incidents;

d) de détailler davantage les composantes de la politique de continuité des activités de TIC visée à l'article 11, paragraphe 1;

e) de détailler davantage les tests des plans de continuité des activités de TIC visés à l'article 11, paragraphe 6, afin de veiller à ce que ces tests tiennent dûment compte des scénarios dans lesquels la qualité de l'exécution d'une fonction critique ou importante se détériore à un niveau inacceptable ou dans lesquels l'exécution d'une fonction critique ou importante échoue, et à ce que ces tests prennent dûment en considération les incidences potentielles de l'insolvabilité ou d'autres défaillances de tout prestataire tiers de services TIC concerné et, le cas échéant, les risques politiques dans les juridictions des prestataires en question;

f) de détailler davantage les composantes des plans de réponse et de rétablissement des TIC visés à l'article 11, paragraphe 3;

g) de préciser davantage le contenu et le format du rapport sur le réexamen du cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 5.

Lors de l'élaboration de ces projets de normes techniques de réglementation, les AES tiennent compte de la taille et du profil de risque global de l'entité financière, ainsi que de la nature, de l'ampleur et de la complexité de ses services, activités et opérations, tout en tenant dûment compte de toute caractéristique particulière découlant de la nature distincte des activités dans les différents secteurs des services financiers.

Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le ... [12 mois à compter de la date d'entrée en vigueur du présent règlement].

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) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

Article 16

Cadre simplifié de gestion du risque lié aux TIC

1. Les articles 5 à 15 du présent règlement ne s'appliquent pas aux petites entreprises d'investissement non interconnectées et aux établissements de paiement exemptés en vertu de la directive (UE) 2015/2366; aux établissements exemptés en vertu de la directive 2013/36/UE pour lesquels les États membres ont décidé de ne pas appliquer l'option visée à l'article 2, paragraphe 4, du présent règlement; aux établissements de monnaie électronique exemptés en vertu de la directive 2009/110/CE; et aux petites institutions de retraite professionnelle.

Sans préjudice du premier alinéa, les entités énumérées au premier alinéa doivent:

a) mettre en place et maintenir un cadre de gestion du risque lié aux TIC solide et documenté qui détaille les mécanismes et les mesures permettant une gestion rapide, efficace et complète du risque lié aux TIC, y compris en ce qui concerne la protection des composantes et infrastructures physiques pertinentes;

b) surveiller en permanence la sécurité et le fonctionnement de tous les systèmes de TIC;

c) réduire au minimum l'incidence du risque lié aux TIC grâce à l'utilisation de systèmes, protocoles et outils de TIC solides, résilients et actualisés, aptes à soutenir l'exercice de leurs activités et la fourniture de services et à protéger de manière adéquate la disponibilité, l'authenticité, l'intégrité et la confidentialité des données dans le réseau et les systèmes d'information;

d) permettre d'identifier et de détecter rapidement les sources de risque et les anomalies liés aux TIC dans le réseau et les systèmes d'information et de traiter rapidement les incidents liés aux TIC;

e) recenser les principales dépendances vis-à-vis des prestataires tiers de services TIC;

f) assurer la continuité des fonctions critiques ou importantes, au moyen de plans de continuité des activités et de mesures de réponse et de rétablissement, qui comprennent au moins des mesures de sauvegarde et de restauration;

g) tester régulièrement les plans et mesures visés au point f), ainsi que l'efficacité des contrôles mis en œuvre conformément aux points a) et c);

h) mettre en œuvre, le cas échéant, les conclusions opérationnelles pertinentes résultant des tests visés au point g) et de l'analyse post-incident dans le processus d'évaluation du risque lié aux TIC et élaborer, en fonction des besoins et du profil de risque lié aux TIC, des programmes de sensibilisation en matière de sécurité des TIC et de formation à la résilience opérationnelle numérique à l'intention du personnel et de la direction.

2. Le cadre de gestion du risque lié aux TIC visé au paragraphe 1, deuxième alinéa, point a), est documenté et réexaminé périodiquement et en cas d'incidents majeurs liés aux TIC conformément aux instructions des autorités de surveillance. Il est amélioré en permanence sur la base des enseignements tirés de la mise en œuvre et du suivi. Un rapport sur le réexamen du cadre de gestion du risque lié aux TIC est présenté à l'autorité compétente à sa demande.

3. Les AES élaborent, par l'intermédiaire du comité mixte, en concertation avec l'ENISA, des projets communs de normes techniques de réglementation afin de:

a) préciser davantage les éléments à inclure dans le cadre de gestion du risque lié aux TIC visé au paragraphe 1, deuxième alinéa, point a);

b) préciser davantage les éléments relatifs aux systèmes, protocoles et outils visant à réduire au minimum l'incidence du risque lié aux TIC visés au paragraphe 1, deuxième alinéa, point c), 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 et de préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données;

c) détailler davantage les composantes des plans de continuité des activités de TIC visés au paragraphe 1, deuxième alinéa, point f);

d) préciser davantage les règles relatives aux tests des plans de continuité des activités, veiller à l'efficacité des contrôles visées au paragraphe 1, deuxième alinéa, point g), et veiller à ce que ces tests tiennent dûment compte des scénarios dans lesquels la qualité de l'exécution d'une fonction critique ou importante se détériore à un niveau inacceptable ou dans lesquels l'exécution d'une fonction critique ou importante échoue;

e) préciser davantage le contenu et le format du rapport sur le réexamen du cadre de gestion du risque lié aux TIC visé au paragraphe 2.

Lorsqu'elles élaborent ces projets de normes techniques de réglementation, les AES tiennent compte de la taille et du profil de risque global de l'entité financière, ainsi que de la nature, de l'ampleur et de la complexité de ses services, activités et opérations.

Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le ... [12 mois à compter de la date d'entrée en vigueur du présent règlement].

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) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

Chapitre III

Gestion, classification et notification des incidents liés aux TIC

Article 17

Processus de gestion des incidents liés aux TIC

1. Les entités financières définissent, établissent et mettent en œuvre un processus de gestion des incidents liés aux TIC afin de détecter, de gérer et de notifier les incidents liés aux TIC.

2. Les entités financières enregistrent tous les incidents liés aux TIC et les cybermenaces importantes. Les entités financières mettent en place des procédures et des processus adéquats pour assurer une surveillance, un traitement et un suivi cohérents et intégrés des incidents liés aux TIC, pour veiller à ce que les causes originelles soient identifiées et documentées et qu'il y soit remédié pour éviter que de tels incidents ne se produisent.

3. Le processus de gestion des incidents liés aux TIC visé au paragraphe 1:

a) met en place des indicateurs d'alerte précoce;

b) instaure des procédures destinées à identifier, suivre, consigner, catégoriser et classer les incidents liés aux TIC en fonction de leur priorité et de leur gravité et en fonction de la criticité des services touchés, conformément aux critères fixés à l'article 18, paragraphe 1;

c) attribue les rôles et les responsabilités qui doivent être activés pour différents types et scénarios d'incidents liés aux TIC;

d) établit des plans pour la communication à l'intention du personnel, des parties prenantes externes et des médias, conformément à l'article 14, et pour la notification aux clients, les procédures internes de remontée des informations, 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;

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

f) définit des procédures de réponse en cas d'incident lié aux TIC, afin d'en atténuer les effets et de garantir que les services redeviennent opérationnels et sécurisés en temps utile.

Article 18

Classification des incidents liés aux TIC et des cybermenaces

1. Les entités financières classent les incidents liés aux TIC et déterminent leur incidence sur la base des critères suivants:

   a) le nombre et/ou l'importance des clients ou des contreparties financières touchés et, le cas échéant, le volume ou le nombre de transactions touchées par l'incident lié aux TIC, et si cet incident a porté atteinte à la réputation;

   b) la durée de l'incident lié aux TIC, y compris les interruptions de service;

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

   d) les pertes de données occasionnées par l'incident lié aux TIC en ce qui concerne la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données;

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

   f) les conséquences économiques, en particulier les coûts et pertes directs et indirects, en termes absolus et relatifs, de l'incident lié aux TIC.

2. Les entités financières classent les cybermenaces comme significatives en fonction de la criticité des services à risque, y compris des transactions et des opérations de l'entité financière, du nombre et/ou de l'importance des clients ou des contreparties financières ciblés et de la répartition géographique des zones à risque.

3. Les AES élaborent, par l'intermédiaire du comité mixte et en concertation avec la BCE et 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 aux TIC ou, le cas échéant, les incidents opérationnels ou de sécurité majeurs liés au paiement, qui sont soumis à l'obligation de déclaration prévue à l'article 19, paragraphe 1;

b) les critères que les autorités compétentes doivent appliquer pour évaluer si des incidents majeurs liés aux TIC ou, le cas échéant, des incidents opérationnels ou de sécurité majeurs liés au paiement, sont pertinents pour les autorités compétentes concernées des autres États membres, et les détails des rapports d'incidents majeurs liés aux TIC ou, le cas échéant, d'incidents opérationnels ou de sécurité majeurs liés au paiement, à partager avec les autres autorités compétentes conformément à l'article 19, paragraphes 6 et 7;

c) les critères énoncés au paragraphe 2 du présent article, y compris les seuils d'importance significative élevés pour déterminer les cybermenaces importantes.

4. Lors de l'élaboration des projets communs de normes techniques de réglementation visés au paragraphe 3 du présent article, les AES tiennent compte des critères énoncés à l'article 4, paragraphe 2, ainsi que des normes, orientations et spécifications internationales élaborées et publiées par l'ENISA, y compris, le cas échéant, des spécifications relatives à d'autres secteurs économiques. Aux fins de l'application des critères énoncés à l'article 4, paragraphe 2, les AES tiennent dûment compte de la nécessité pour les microentreprises et les petites et moyennes entreprises de mobiliser des ressources et des capacités suffisantes pour garantir une gestion rapide des incidents liés aux TIC.

Les AES soumettent ces projets communs de normes techniques de réglementation à la Commission au plus tard le ... [12 mois à compter de la date d'entrée en vigueur du présent règlement].

Le pouvoir de compléter le présent règlement par l'adoption des normes techniques de réglementation visées au paragraphe 3 est délégué à la Commission conformément aux articles 10 à 14 des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

Article 19

Déclaration des incidents majeurs liés aux TIC et notification volontaire des cybermenaces importantes

1. Les entités financières déclarent à l'autorité compétente pertinente visée à l'article 46 les incidents majeurs liés aux TIC, conformément au paragraphe 4 du présent article.

Lorsqu'une entité financière est soumise à la surveillance de plusieurs autorités nationales compétentes visées à l'article 46, les États membres désignent une seule autorité compétente en tant qu'autorité compétente concernée chargée d'exercer les fonctions et missions prévues au présent article.

Les établissements de crédit classés comme importants, conformément à l'article 6, paragraphe 4, du règlement (UE) n° 1024/2013, déclarent les incidents majeurs liés aux TIC à l'autorité nationale compétente concernée désignée conformément à l'article 4 de la directive 2013/36/UE, qui transmet immédiatement cette déclaration à la BCE.

Aux fins du premier alinéa, les entités financières établissent, après avoir recueilli et analysé toutes les informations pertinentes, la notification initiale et les rapports visés au paragraphe 4 du présent article en utilisant les modèles visés à l'article 20, et les soumettent à l'autorité compétente. S'il s'avère qu'une impossibilité technique empêche la soumission de la notification initiale au moyen du modèle, les entités financières le notifient à l'autorité compétente par d'autres moyens.

La notification initiale et les rapports visés au paragraphe 4 comprennent toutes les informations nécessaires pour permettre à l'autorité compétente de déterminer l'importance de l'incident majeur lié aux TIC et d'évaluer les éventuelles incidences transfrontières.

Sans préjudice de la déclaration par l'entité financière à l'autorité compétente concernée en vertu du premier alinéa, les États membres peuvent en outre décider que certaines entités financières ou toutes les entités financières fournissent également la notification initiale et chacun des rapports visés au paragraphe 4 du présent article en utilisant les modèles visés à l'article 20 aux autorités compétentes ou aux centres de réponse aux incidents de sécurité informatique (CSIRT) désignés ou établis conformément à la directive (UE) .../...[+].

2. Les entités financières peuvent notifier, à titre volontaire, les cybermenaces importantes à l'autorité compétente concernée lorsqu'elles estiment que la menace est pertinente pour le système financier, les utilisateurs de services ou les clients. L'autorité compétente concernée peut communiquer ces informations à d'autres autorités compétentes conformément au paragraphe 6.

Les établissements de crédit classés comme importants, conformément à l'article 6, paragraphe 4, du règlement (UE) n° 1024/2013, peuvent, à titre volontaire, notifier les cybermenaces importantes à l'autorité nationale compétente concernée, désignée conformément à l'article 4 de la directive 2013/36/UE, qui transmet immédiatement la notification à la BCE.

Les États membres peuvent décider que les entités financières qui, à titre volontaire, notifient conformément au premier alinéa peuvent également transmettre cette notification aux CSIRT désignés ou établis conformément à la directive (UE) .../...[+].

[+] JO: veuillez insérer, dans le texte, le numéro de la directive figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

3. Lorsqu'un incident majeur lié aux TIC survient et a une incidence sur les intérêts financiers des clients, les entités financières informent leurs clients de cet incident majeur lié aux TIC et des mesures qui ont été prises pour atténuer les effets préjudiciables de cet incident sans retard injustifié dès qu'elles en ont connaissance.

En cas de cybermenace importante, les entités financières informent, le cas échéant, leurs clients susceptibles d'être affectés de toute mesure de protection appropriée que ces derniers pourraient envisager de prendre.

4. Les entités financières soumettent, dans les délais à fixer conformément à l'article 20, premier alinéa, point a) 2), à l'autorité compétente concernée les éléments suivants:

a) une notification initiale;

b) un rapport intermédiaire après la notification initiale visée au point a), dès que la situation de l'incident initial a sensiblement changé ou que le traitement de l'incident majeur lié aux TIC a changé sur la base des nouvelles informations disponibles, 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 originelles 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.

5. Les entités financières peuvent externaliser, conformément au droit sectoriel de l'Union et national, les obligations de déclaration prévues par le présent article à un prestataire tiers de services. Dans le cas d'une telle externalisation, l'entité financière reste pleinement responsable du respect des exigences en matière de déclaration des incidents.

6. Dès réception de la notification initiale et de chaque rapport visé au paragraphe 4, l'autorité compétente fournit, en temps utile, des détails sur l'incident majeur lié aux TIC aux destinataires suivants sur la base, selon le cas, de leurs compétences respectives:

a) à l'ABE, à l'AEMF ou à l'AEAPP;

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

c) aux autorités compétentes, aux points de contact uniques ou aux CSIRT désignés ou établis conformément à la directive (UE) .../...[+];

[+] JO: veuillez insérer, dans le texte, le numéro de la directive figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

d) aux autorités de résolution visées à l'article 3 de la directive 2014/59/UE et au Conseil de résolution unique (CRU) en ce qui concerne les entités visées à l'article 7, paragraphe 2, du règlement (UE) n° 806/2014 du Parlement européen et du Conseil[1] et, en ce qui concerne les entités et les groupes visés à l'article 7, paragraphe 4, point b), et à l'article 7, paragraphe 5, du règlement (UE) n° 806/2014, si ces détails concernent des incidents qui présentent un risque pour l'exercice de fonctions critiques au sens de l'article 2, paragraphe 1, point 35, de la directive 2014/59/UE; et

e) à d'autres autorités publiques compétentes en vertu du droit national.

7. Après réception des informations visées au paragraphe 6, l'ABE, l'AEMF ou l'AEAPP et la BCE, en consultation avec l'ENISA et en coopération avec l'autorité compétente concernée, évaluent si l'incident majeur lié aux TIC est pertinent pour les autorités compétentes d'autres États membres. À la suite de cette évaluation, l'ABE, l'AEMF ou l'AEAPP informent en conséquence, dès que possible, les autorités compétentes concernées des autres États membres. 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.

---

[1] Règlement (UE) n° 806/2014 du Parlement européen et du Conseil du 15 juillet 2014 établissant des règles et une procédure uniformes pour la résolution des établissements de crédit et de certaines entreprises d'investissement dans le cadre d'un mécanisme de résolution unique et d'un Fonds de résolution bancaire unique, et modifiant le règlement (UE) n° 1093/2010 (JO L 225 du 30.7.2014, p. 1).

8. La notification à effectuer par l'AEMF en vertu du paragraphe 7 du présent article est sans préjudice de la responsabilité de l'autorité compétente de transmettre d'urgence les détails de l'incident majeur lié aux TIC à l'autorité concernée de l'État membre d'accueil, lorsqu'un dépositaire central de titres exerce une activité transfrontière importante dans l'État membre d'accueil, que l'incident majeur lié aux TIC est susceptible d'avoir de graves conséquences sur les marchés financiers de l'État membre d'accueil et qu'il existe des accords de coopération entre les autorités compétentes en matière de surveillance des entités financières.

Article 20

Harmonisation du contenu et des modèles des rapports de notification

Les AES, agissant par l'intermédiaire du comité mixte et en concertation avec l'ENISA et la BCE, élaborent:

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

i) de définir le contenu des rapports relatifs aux incidents majeurs liés aux TIC afin de refléter les critères énoncés à l'article 18, paragraphe 1, et d'intégrer d'autres éléments, tels que des détails permettant de déterminer la pertinence de la notification pour les autres États membres et s'il s'agit d'un incident opérationnel ou de sécurité majeur lié au paiement;

ii) de fixer les délais pour la notification initiale et pour chaque rapport visé à l'article 19, paragraphe 4;

iii) d'établir le contenu de la notification en ce qui concerne les cybermenaces importantes.

Lorsqu'elles élaborent ces projets de normes techniques de réglementation, les AES tiennent compte de la taille et du profil de risque global de l'entité financière, ainsi que de la nature, de l'ampleur et de la complexité de ses services, activités et opérations, et en particulier en vue de garantir que, aux fins du point a) ii), du présent alinéa, différents délais puissent refléter, le cas échéant, les spécificités des secteurs financiers, sans préjudice du maintien d'une approche cohérente de la notification des incidents liés aux TIC en application du présent règlement et de la directive (UE) .../...[+]. Les AES fournissent, le cas échéant, une justification lorsqu'elles s'écartent des approches adoptées dans le cadre de ladite directive;

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 aux TIC et de notifier une cybermenace importante.

Les AES soumettent à la Commission les projets communs de normes techniques de réglementation visés au premier alinéa, point a), et les projets communs de normes techniques d'exécution visés au premier alinéa, point b), au plus tard le … [18 mois à compter de la date d'entrée en vigueur du présent règlement].

[+] JO: veuillez insérer, dans le texte, le numéro de la directive figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

Le pouvoir de compléter le présent règlement par l'adoption des normes techniques de réglementation communes visées au premier alinéa, point a), est délégué à la Commission conformément aux articles 10 à 14 des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

Le pouvoir d'adopter les normes techniques d'exécution communes visées au premier alinéa, point b), est conféré à la Commission conformément à l'article 15 des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

Article 21

Centralisation des notifications d'incidents majeurs liés aux TIC

1. Les AES, agissant par l'intermédiaire du comité mixte, et en consultation 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'une plateforme unique de l'Union pour la notification des incidents majeurs liés aux TIC par les entités financières. Le rapport conjoint étudie les moyens de faciliter le flux des notifications d'incidents liés aux TIC, de réduire les coûts connexes et d'étayer les analyses thématiques en vue de renforcer la convergence en matière de surveillance.

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

   a) les conditions préalables à la création de cette plateforme unique de l'Union;

b) les avantages, les limites et les risques, y compris les risques associés à la concentration élevée d'informations sensibles;

c) la capacité nécessaire pour assurer l'interopérabilité au regard d'autres mécanismes de notification pertinents;

d) les aspects de la gestion opérationnelle;

e) les conditions de participation;

f) les modalités techniques d'accès des entités financières et des autorités nationales compétentes à la plateforme unique de l'Union;

g) une évaluation préliminaire des coûts financiers engendrés par la mise en place de la plateforme opérationnelle qui soutiendra la plateforme unique de l'Union, 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 ... [24 mois à compter de la date d'entrée en vigueur du présent règlement].

Article 22

Retour d'information en matière de surveillance

1. Sans préjudice des contributions, avis ou mesures correctives techniques et du suivi correspondant pouvant être fournis, le cas échéant, conformément au droit national, par les CSIRT relevant de la directive (UE) .../...[+], dès qu'elle reçoit la notification initiale et chaque rapport visé à l'article 19, paragraphe 4, l'autorité compétente en accuse réception et peut, dans la mesure du possible, fournir en temps voulu à l'entité financière un retour d'information pertinent et adapté ou une orientation de haut niveau, notamment en rendant disponibles les informations et renseignements anonymisés pertinents sur des menaces similaires, et peut examiner les mesures correctives appliquées au niveau de l'entité financière et les moyens de réduire au maximum et d'atténuer les effets préjudiciables dans le secteur financier. Sans préjudice du retour d'information reçu en matière de surveillance, les entités financières restent pleinement responsables du traitement et des conséquences des incidents liés aux TIC déclarés conformément à l'article 19, paragraphe 1.

2. Les AES, agissant par l'intermédiaire du comité mixte, présentent chaque année un rapport anonymisé et agrégé sur les incidents majeurs liés aux TIC, dont les détails sont fournis par les autorités compétentes conformément à l'article 19, paragraphe 6, en indiquant au minimum le nombre d'incidents majeurs liés aux TIC, leur nature, leurs répercussions sur les opérations des entités financières ou des clients, les mesures correctives prises et les coûts.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

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

Article 23

Incidents opérationnels ou de sécurité liés au paiement concernant les établissements de crédit, les établissements de paiement, les prestataires de services d'information sur les comptes et les établissements de monnaie électronique

Les exigences énoncées au présent chapitre s'appliquent également aux incidents opérationnels ou de sécurité liés au paiement et aux incidents opérationnels ou de sécurité majeurs liés au paiement lorsqu'ils concernent des établissements de crédit, des établissements de paiement, des prestataires de services d'information sur les comptes et des établissements de monnaie électronique.

Chapitre IV
Tests de résilience opérationnelle numérique

Article 24

Exigences générales applicables

à la réalisation de tests de résilience opérationnelle numérique

1. Afin d'évaluer l'état de préparation en vue du traitement d'incidents liés aux TIC, de recenser les faiblesses, les défaillances et les lacunes en matière de résilience opérationnelle numérique et de mettre rapidement en œuvre des mesures correctives, les entités financières, autres que les microentreprises, établissent, maintiennent et réexaminent, en tenant compte des critères énoncés à l'article 4, paragraphe 2,un programme solide et complet de tests de résilience opérationnelle numérique, qui fait partie intégrante du cadre de gestion du risque lié aux TIC visé à l'article 6.

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 articles 25 et 26.

3. Lorsqu'elles exécutent le programme de tests de résilience opérationnelle numérique visé au paragraphe 1 du présent article, les entités financières, autres que les microentreprises, adoptent une approche fondée sur le risque tenant compte des critères énoncés à l'article 4, paragraphe 2, en prenant dûment en considération l'évolution du risque lié aux TIC, tout risque spécifique auquel l'entité financière concernée est ou pourrait être exposée, la criticité des actifs informationnels et des services fournis, ainsi que tout autre facteur que l'entité financière juge approprié.

4. Les entités financières, autres que les microentreprises, veillent à ce que les tests soient effectués par des parties indépendantes internes ou externes. Lorsque les tests sont effectués par un testeur interne, les entités financières leur accordent des ressources suffisantes et veillent à éviter les conflits d'intérêts pendant les phases de conception et d'exécution du test.

5. Les entités financières, autres que les microentreprises, définissent des procédures et des stratégies destinées à hiérarchiser, classer et résoudre tous les problèmes mis en évidence 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, autres que les microentreprises, veillent à soumettre, au moins une fois par an, tous les systèmes et applications de TIC qui soutiennent des fonctions critiques ou importantes à des tests appropriés.

Article 25

Test des outils et systèmes de TIC

1. Le programme de tests de résilience opérationnelle numérique visé à l'article 24 prévoit, conformément aux critères énoncés à l'article 4, paragraphe 2, l'exécution de tests appropriés, tels que des évaluations et des analyses de vulnérabilité, des analyses de sources ouvertes, des évaluations de la sécurité des réseaux, des analyses des écarts, des examens de la sécurité physique, des questionnaires et des solutions logicielles de balayage, 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 et des tests de pénétration.

2. Les dépositaires centraux de titres et les contreparties centrales procèdent à des évaluations de la vulnérabilité avant tout déploiement ou redéploiement d'applications et composantes d'infrastructures nouvelles ou existantes et de services TIC nouveaux ou existants qui soutiennent des fonctions critiques ou importantes de l'entité financière.

3. Les microentreprises effectuent les tests visés au paragraphe 1 en combinant une approche fondée sur les risques avec une planification stratégique des tests des TIC, en tenant dûment compte de la nécessité de maintenir une approche équilibrée entre, d'une part, l'ampleur des ressources et le temps à consacrer aux tests des TIC prévus au présent article et, d'autre part, l'urgence, le type de risque, la criticité des actifs informationnels et des services fournis, ainsi que tout autre facteur pertinent, y compris la capacité de l'entité financière à prendre des risques calculés.

Article 26

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

1. Les entités financières, autres que les entités visées à l'article 16, paragraphe 1, premier alinéa, et autres que les microentreprises, qui sont identifiées conformément au paragraphe 8, troisième alinéa, du présent article effectuent au moins tous les trois ans des tests avancés au moyen d'un test de pénétration fondé sur la menace. En fonction du profil de risque de l'entité financière et compte tenu des circonstances opérationnelles, l'autorité compétente peut, le cas échéant, demander à l'entité financière de réduire ou d'augmenter cette fréquence.

2. Chaque test de pénétration fondé sur la menace couvre plusieurs, voire la totalité, des fonctions critiques ou importantes d'une entité financière et est effectué sur des systèmes en environnement de production en direct qui soutiennent ces fonctions.

   Les entités financières recensent tous les systèmes, processus et technologies de TIC sous-jacents pertinents qui soutiennent des fonctions critiques ou importantes et des services TIC, y compris ceux qui soutiennent des fonctions critiques ou importantes qui ont été externalisés ou sous-traités à des prestataires tiers de services TIC.

   Les entités financières évaluent quelles fonctions critiques ou importantes doivent être couvertes par les tests de pénétration fondés sur la menace. Le résultat de cette évaluation détermine la portée précise de ces tests et est validé par les autorités compétentes.

3. Lorsque des prestataires tiers de services TIC sont inclus dans le champ d'application du test de pénétration fondé sur la menace, l'entité financière prend les mesures et garanties nécessaires pour assurer la participation de ces prestataires tiers de services TIC à ce test, et conserve à tout moment l'entière responsabilité de veiller au respect du présent règlement.

4. Sans préjudice du paragraphe 2, premier et deuxième alinéas, lorsque l'on peut raisonnablement s'attendre à ce que la participation d'un prestataire tiers de services TIC au test de pénétration fondé sur la menace, visée au paragraphe 3, ait une incidence négative sur la qualité ou sur la sécurité des services que le prestataire tiers de services TIC fournit à des clients qui sont des entités ne relevant pas du champ d'application du présent règlement, ou sur la confidentialité des données liées à ces services, l'entité financière et le prestataire tiers de services TIC peuvent convenir par écrit que le prestataire tiers de services TIC conclut directement des accords contractuels avec un testeur externe, aux fins de la réalisation, sous la direction d'une entité financière désignée, d'un test groupé de pénétration fondé sur la menace associant plusieurs entités financières (test groupé) auxquelles le prestataire tiers de services TIC fournit des services TIC.

Ce test groupé couvre la gamme pertinente de services TIC qui soutiennent des fonctions critiques ou importantes sous-traitées par les entités financières au prestataire tiers de services TIC concerné. Le test groupé est considéré comme un test de pénétration fondé sur la menace réalisé par les entités financières participant au test groupé.

Le nombre d'entités financières participant au test groupé est dûment calibré compte tenu de la complexité et des types de services concernés.

5. Les entités financières procèdent, avec la coopération de prestataires tiers de services TIC et d'autres parties concernées, y compris les testeurs mais à l'exception des autorités compétentes, à des contrôles efficaces de la gestion des risques afin d'atténuer les risques d'incidence potentielle sur les données, de dommages aux actifs et de perturbation des fonctions, services ou opérations critiques ou importants au sein de l'entité financière elle-même, de ses contreparties ou du secteur financier.

6. À l'issue du test, une fois que les rapports et les plans de mesures correctives ont été approuvés, l'entité financière et, s'il y a lieu, les testeurs externes fournissent à l'autorité, désignée conformément au paragraphe 9 ou 10, une synthèse des conclusions pertinentes, les plans de mesures correctives et la documentation démontrant que le test de pénétration fondé sur la menace a été effectué conformément aux exigences.

7. Les autorités fournissent aux entités financières une attestation qui confirme que le test a été effectué conformément aux exigences, comme prouvé dans la documentation, afin de permettre la reconnaissance mutuelle des tests de pénétration fondés sur la menace entre les autorités compétentes. L'entité financière notifie à l'autorité compétente concernée l'attestation, la synthèse des conclusions pertinentes et les plans de mesures correctives.

Sans préjudice de ladite attestation, les entités financières restent à tout moment pleinement responsables des incidences des tests visées au paragraphe 4.

8. Pour réaliser les tests de pénétration fondés sur la menace, les entités financières font appel à des testeurs, conformément à l'article 27. Lorsque des entités financières ont recours à des testeurs internes aux fins de la réalisation de ces tests, elles engagent un testeur externe tous les trois tests.

Les établissements de crédit, qui sont classés comme importants conformément à l'article 6, paragraphe 4, du règlement (UE) n° 1024/2013, ont uniquement recours à des testeurs externes conformément à l'article 27, paragraphe 1, points a) à e).

Les autorités compétentes désignent les entités financières qui sont tenues de réaliser un test de pénétration fondé sur la menace en tenant compte des critères énoncés à l'article 4, paragraphe 2, sur la base d'une appréciation des éléments suivants:

a) les facteurs d'incidence, en particulier la mesure dans laquelle les services fournis et les activités entreprises par l'entité financière affectent le secteur financier;

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

c) le profil du risque lié aux TIC spécifique, le niveau de maturité des TIC de l'entité financière ou les caractéristiques technologiques concernées.

9. Les États membres peuvent désigner une autorité publique unique au sein du secteur financier chargée des questions liées aux tests de pénétration fondés sur la menace dans le secteur financier au niveau national, et leur confient toutes les compétences et tâches nécessaires à cet effet.

10. En l'absence de désignation conformément au paragraphe 9 du présent article, et sans préjudice du pouvoir de désigner les entités financières qui sont tenues de réaliser un test de pénétration fondé sur la menace, une autorité compétente peut déléguer l'exercice de tout ou partie des tâches visées au présent article et à l'article 27 à une autre autorité nationale du secteur financier.

11. Les AES élaborent, en accord avec la BCE, des projets conjoints de normes techniques de réglementation conformément au cadre TIBER-EU afin de préciser:

a) les critères utilisés aux fins de l'application du paragraphe 8, deuxième alinéa;

b) les exigences et normes régissant le recours à des testeurs internes;

c) les exigences concernant:

i) la portée du test de pénétration fondé sur la menace visé au paragraphe 2;

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

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

d) le type de coopération en matière de surveillance et les autres types de coopération pertinents qui sont nécessaires pour l'exécution des tests de pénétration fondés sur la menace, et pour la facilitation de la reconnaissance mutuelle de ces tests, 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.

Lors de l'élaboration de ces projets de normes techniques de réglementation, les AES tiennent dûment compte de toute caractéristique particulière découlant de la nature distincte des activités dans les différents secteurs des services financiers.

Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le ... [18 mois à compter de la date d'entrée en vigueur du présent règlement].

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) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

Article 27

Exigences applicables aux testeurs

afin de réaliser des tests de pénétration fondés sur la menace

1. Afin de réaliser des tests de pénétration fondés sur la menace, les entités financières ont uniquement recours à des testeurs qui:

   a) possèdent l'aptitude et la réputation les plus élevées;

   b) possèdent des capacités techniques et organisationnelles et justifient d'une expertise spécifique en matière de renseignement sur les menaces, de tests de pénétration et de tests en mode 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) fournissent une assurance indépendante ou un rapport d'audit ayant trait à la bonne gestion des risques associés à la réalisation 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) 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. Lorsqu'elles ont recours à des testeurs internes, les entités financières veillent à ce que, outre les exigences du paragraphe 1, les conditions suivantes soient remplies:

a) le recours à ces testeurs internes a été approuvé par l'autorité compétente concernée ou par l'autorité publique unique désignée conformément à l'article 26, paragraphes 4 et 10;

b) l'autorité compétente concernée a vérifié que l'entité financière dispose des ressources suffisantes et a veillé à éviter les conflits d'intérêts pendant les phases de conception et d'exécution du test; et

c) le fournisseur de renseignements sur les menaces est externe à l'entité financière.

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

Chapitre V

Gestion des risques liés aux prestataires tiers de services TIC

SECTION I

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

Article 28

Principes généraux

1. Les entités financières gèrent les risques liés aux prestataires tiers de services TIC en tant que partie intégrante du risque lié aux TIC dans leur cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1, et conformément aux principes suivants:

   a) les entités financières qui ont conclu des accords contractuels pour l'utilisation de services TIC dans le cadre de leurs activités restent à tout moment pleinement responsables du respect et de l'exécution de toutes les obligations découlant du présent règlement et du droit applicable aux services financiers;

b) les entités financières gèrent les risques liés aux prestataires tiers de services TIC dans le respect du principe de proportionnalité, en tenant compte:

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

ii) des risques découlant des accords contractuels portant sur l'utilisation de services TIC conclus avec des prestataires tiers de services TIC, 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 disponibilité des services et activités financiers, au niveau individuel et au niveau du groupe.

2. Aux fins de leur cadre de gestion du risque lié aux TIC, les entités financières, autres que les entités visées à l'article 16, paragraphe 1, premier alinéa, et autres que les microentreprises, adoptent une stratégie en matière de risques liés aux prestataires tiers de services TIC, et la réexaminent régulièrement, en tenant compte de la stratégie multi-fournisseurs visée à l'article 6, paragraphe 9, le cas échéant. La stratégie en matière de risques liés aux prestataires tiers de services TIC inclut une politique relative à l'utilisation des services TIC qui soutiennent des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC et s'applique sur une base individuelle et, le cas échéant, sur une base sous-consolidée et consolidée. Sur la base d'une évaluation du profil de risque global de l'entité financière ainsi que de l'ampleur et de la complexité des services, l'organe de direction examine régulièrement les risques identifiés en ce qui concerne les accords contractuels relatifs à l'utilisation des services TIC qui soutiennent des fonctions critiques ou importantes.

3. Aux fins de leur cadre de gestion du risque lié aux TIC, 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 TIC fournis par des prestataires tiers de services TIC.

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

Les entités financières communiquent au moins une fois par an aux autorités compétentes le nombre de nouveaux accords relatifs à l'utilisation de services TIC, les catégories de prestataires tiers de services TIC, le type d'accords contractuels et les services et fonctions de TIC 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 de tout projet d'accord contractuel portant sur l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes ainsi que lorsqu'une fonction est devenue critique ou importante.

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

a) déterminent si l'accord contractuel couvre l'utilisation de services TIC qui soutiennent une fonction critique ou importante;

b) évaluent si les conditions 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 visé à l'article 29;

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

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

5. Les entités financières ne peuvent conclure des accords contractuels qu'avec des prestataires tiers de services TIC qui respectent des normesadéquates en matière de sécurité de l'information. Lorsque ces accords contractuels portent sur des fonctions critiques ou importantes, les entités financières prennent en considération, avant la conclusion des accords, l'utilisation par les prestataires tiers de services TIC des normes les plus actualisées et les plus élevées en matière de sécurité de l'information.

6. Lorsqu'elles exercent leurs droits d'accès, d'inspection et d'audit à l'égard d'un prestataire tiers de services TIC, les entités financières déterminent au préalable, sur la base d'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.

Lorsque des accords contractuels conclus avec des prestataires tiers de services TIC impliquent un niveau élevé de complexité technique, l'entité financière vérifie que les auditeurs, qu'il s'agisse d'auditeurs internes ou externes ou d'un groupe d'auditeurs, possèdent les compétences et les connaissances requises pour réaliser efficacement les évaluations et les audits pertinents.

7. Les entités financières veillent à ce que les accords contractuels relatifs à l'utilisation de services TIC puissent être résiliés dans l'une des circonstances suivantes:

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

b) le suivi des risques liés aux prestataires tiers de services TIC 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 prestataire tiers de services TIC;

c) le prestataire tiers de services TIC présente des faiblesses avérées liées à sa gestion globale du risque lié aux TIC et, en particulier, dans la manière dont il assure la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, qu'il s'agisse de données personnelles ou autrement sensibles, ou de données non personnelles;

d) l'autorité compétente ne peut plus surveiller efficacement l'entité financière en raison des conditions de l'accord contractuel en question, ou des circonstances qui y sont liées.

8. Pour les services TIC qui soutiennent des fonctions critiques ou importantes, les entités financières mettent en place des stratégies de sortie. Les stratégies de sortie tiennent compte des risques susceptibles d'apparaître au niveau des prestataires tiers de services TIC, en particulier une éventuelle défaillance de leur part, une détérioration de la qualité des services TIC fournis, toute perturbation de l'activité due à une fourniture inappropriée ou défaillante de services TIC ou tout risque significatif découlant du déploiement approprié et continu du service TIC concerné, ou la résiliation d'accords contractuels conclus avec un prestataire tiers de services TIC dans l'une des circonstances énumérées au paragraphe 7.

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

a) perturber leurs activités;

b) restreindre le respect des exigences réglementaires;

c) porter atteinte à la continuité et à la qualité des services fournis aux clients.

Les plans de sortie sont complets, documentés et, conformément aux critères énoncés à l'article 4, paragraphe 2, sont soumis à des tests suffisants et réexaminés périodiquement.

Les entités financières définissent des solutions alternatives et élaborent des plans de transition leur permettant de supprimer les services TIC visés par le contrat et les données pertinentes détenues par le prestataire tiers de services TIC, et de les transférer en toute sécurité et intégralement à des prestataires alternatifs ou de les réincorporer en interne.

Les entités financières disposent des mesures d'urgence qui s'imposent pour maintenir la continuité des activités au cas où les circonstances visées au premier alinéa se présenteraient.

9. Les AES élaborent, agissant 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 3, y compris les informations communes à tous les accord contractuels relatifs à l'utilisation de services TIC. Les AES soumettent ces projets de normes techniques d'exécution à la Commission au plus tard le ... [12 mois à compter de 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) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

10. Les AES élaborent, agissant par l'intermédiaire du comité mixte, des projets de normes techniques de réglementation pour préciser davantage le contenu détaillé de la stratégie visée au paragraphe 2 en ce qui concerne les accords contractuels relatifs à l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC.

Lorsqu'elles élaborent ces projets de normes techniques de réglementation, les AES tiennent compte de la taille et du profil de risque global de l'entité financière, ainsi que de la nature, de l'ampleur et de la complexité de ses services, activités et opérations. Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le ... [12 mois à compter de la date d'entrée en vigueur du présent règlement].

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) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

Article 29

Évaluation préliminaire du risque de concentration de TIC au niveau de l'entité

1. Lorsqu'elles procèdent à l'identification et à l'évaluation des risques visés à l'article 28, paragraphe 4, point c), les entités financières déterminent également si la conclusion envisagée d'un accord contractuel portant sur des services TIC qui soutiennent des fonctions critiques ou importantes déboucherait sur l'une des situations suivantes:

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

   b) la mise en place de plusieurs accords contractuels relatifs à la fourniture de services TIC qui soutiennent des fonctions critiques ou importantes avec le même prestataire tiers de services TIC ou avec des prestataires tiers de services TIC étroitement liés.

   Les entités financières évaluent les avantages et les coûts des solutions alternatives, telles que le recours à différents prestataires tiers de services TIC, en tenant compte de la compatibilité éventuelle des solutions envisagées avec leurs besoins et leurs objectifs définis dans leur stratégie de résilience numérique, et de la manière de garantir cette compatibilité.

2. Lorsque les accords contractuels relatifs à l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes prévoient la possibilité qu'un prestataire tiers de services TIC sous-traite des services TIC qui soutiennent une fonction critique ou importante à d'autres prestataires tiers de services TIC, les entités financières évaluent les avantages et les risques qui peuvent découler de cette sous-traitance, en particulier dans le cas d'un sous-traitant de services TIC établi dans un pays tiers.

Lorsque des accords contractuels concernent des services TIC qui soutiennent des fonctions critiques ou importantes, les entités financières tiennent dûment compte des dispositions de la législation en matière d'insolvabilité qui s'appliqueraient en cas de faillite du prestataire tiers de services TIC, ainsi que de toute contrainte qui pourrait survenir relativement à la récupération urgente des données de l'entité financière.

Lorsque des accords contractuels relatifs à l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes sont conclus avec un prestataire tiers de services TIC établi dans un pays tiers, les entités financières tiennent également compte, en plus des considérations visées au deuxième alinéa, du respect des règles de l'Union en matière de protection des données et de l'application effective de la législation dans ce pays tiers.

Lorsque les accords contractuels relatifs à l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes prévoient une sous-traitance, 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 30

Principales dispositions contractuelles

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

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

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

   b) les lieux, notamment les régions ou les pays, où les services TIC 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 prestataire tiers de services TIC d'informer au préalable l'entité financière si celui-ci envisage de changer ces lieux;

c) des dispositions sur la disponibilité, l'authenticité, l'intégrité et la confidentialité en ce qui concerne la protection des données, y compris les données à caractère personnel;

d) des dispositions 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, de cessation des activités du prestataire tiers de services TIC ou de résiliation des accords contractuels;

e) des descriptions des niveaux de service, y compris leurs mises à jour et révisions;

f) l'obligation pour le prestataire tiers de services TIC de fournir à l'entité financière, sans frais supplémentaires ou à un coût déterminé ex ante, une assistance en cas d'incident lié aux TIC en rapport avec le service TIC fourni à l'entité financière;

g) l'obligation pour le prestataire tiers de services TIC de coopérer pleinement avec les autorités compétentes et les autorités de résolution de l'entité financière, y compris les personnes nommées par eux;

h) les droits de résiliation et les délais de préavis minimaux correspondant pour la résiliation des accords contractuels, conformément aux attentes des autorités compétentes et des autorités de résolution;

i) les conditions de participation des prestataires tiers de services TIC aux programmes de sensibilisation à la sécurité des TIC et aux formations à la résilience opérationnelle numérique élaborés par les entités financières, conformément à l'article 13, paragraphe 6.

3. Les accords contractuels relatifs à l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes comportent au moins les éléments suivants, en plus de ceux qui figurent au paragraphe 2:

a) des descriptions complètes des niveaux de service, y compris leurs mises à jour et révisions, assorties d'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 des services TIC, et de prendre, sans retard injustifié, des mesures correctives appropriées lorsque les niveaux de service convenus ne sont pas atteints;

b) les délais de préavis et les obligations de notification du prestataire tiers de services TIC à l'entité financière, y compris la notification de tout développement susceptible d'avoir une incidence significative sur la capacité du prestataire tiers de services TIC à fournir les services TIC qui soutiennent des fonctions critiques ou importantes de manière efficace conformément aux niveaux de service convenus;

c) l'obligation pour le prestataire tiers de services TIC 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 des TIC qui fournissent un niveau approprié de sécurité en vue de la prestation de services par l'entité financière, conformément à son cadre réglementaire;

d) l'obligation pour le prestataire tiers de services TIC de participer et de coopérer pleinement au test de pénétration fondé sur la menace effectué par l'entité financière visé aux articles 26 et 27;

e) le droit d'assurer un suivi permanent des performances du prestataire tiers de services TIC, qui comprend les éléments suivants:

i) les droits illimités d'accès, d'inspection et d'audit par l'entité financière ou par une tierce partie désignée, et par l'autorité compétente, et le droit de prendre des copies des documents pertinents sur place s'ils sont essentiels aux activités du prestataire tiers de services TIC, dont l'exercice effectif n'est pas entravé ou limité par d'autres accords contractuels ou politiques d'exécution;

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

iii) l'obligation pour le prestataires tiers de services TIC de coopérer pleinement lors des inspections sur place et des audits effectués par les autorités compétentes, le superviseur principal, l'entité financière ou une tierce partie désignée; et

iv) l'obligation de fournir des précisions sur la portée, les procédures à suivre et la fréquence de ces inspections et audits;

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

i) au cours de laquelle le prestataire tiers de services TIC continuera à fournir les fonctions ou services TIC concernés en vue de réduire le risque de perturbation au niveau de l'entité financière ou d'assurer sa résolution et sa restructuration efficaces;

ii) qui permet à l'entité financière de migrer vers un autre prestataire tiers de services TIC ou de recourir à des solutions en interne adaptées à la complexité du service fourni.

Par dérogation au point e), le prestataire tiers de services TIC et l'entité financière qui est une microentreprise peuvent convenir que les droits d'accès, d'inspection et d'audit de l'entité financière peuvent être délégués à une tierce partie indépendante, nommée par le prestataire tiers de services TIC, et que l'entité financière est habilitée à demander à la tierce partie, en tout temps, des informations ainsi qu'une garantie concernant la performance du prestataire tiers de services TIC.

4. Lors de la négociation d'accords contractuels, les entités financières et les prestataires tiers de services TIC envisagent l'utilisation de clauses contractuelles types élaborées par les autorités publiques pour des services particuliers.

5. Les AES élaborent, par l'intermédiaire du comité mixte, des projets de normes techniques de réglementation visant à préciser davantage les éléments visés au paragraphe 2, point a), qu'une entité financière doit déterminer et évaluer lorsqu'elle sous-traite des services TIC qui soutiennent des fonctions critiques ou importantes.

Lorsqu'elles élaborent ces projets de normes techniques de réglementation, les AES tiennent compte de la taille et du profil de risque global de l'entité financière, ainsi que de la nature, de l'ampleur et de la complexité de ses services, activités et opérations.

Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le ... [18 mois à compter de la date d'entrée en vigueur du présent règlement].

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) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

SECTION II

CADRE DE SUPERVISION

DES PRESTATAIRES TIERS CRITIQUES DE SERVICES TIC

Article 31

Désignation de prestataires tiers critiques de services TIC

1. Les AES, agissant par l'intermédiaire du comité mixte et sur recommandation du forum de supervision établi conformément à l'article 32, paragraphe 1:

   a) désignent les prestataires tiers de services TIC qui sont critiques pour les entités financières, à l'issue d'une évaluation tenant compte des critères précisés au paragraphe 2;

b) désignent comme superviseur principal pour chaque prestataire tiers critique de services TIC l'AES responsable, conformément aux règlements (UE) n° 1093/2010, (UE) n° 1094/2010 ou (UE) n° 1095/2010, des entités financières totalisant ensemble la plus grande part d'actifs de la valeur du total des actifs de toutes les entités financières qui utilisent les services du prestataire tiers critique de services TIC concerné, sur la base de la somme des bilans individuels de ces entités financières.

2. La désignation visée au paragraphe 1, point a), repose sur l'ensemble des critères suivants en ce qui concerne les services TIC fournis par le prestataire tiers de services TIC:

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

b) le caractère ou l'importance systémique des entités financières qui dépendent du prestataire tiers de services TIC 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 prestataire tiers de services TIC 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 prestataire tiers de services TIC concerné en ce qui concerne les fonctions critiques ou importantes des entités financières qui font en fin de compte intervenir le même prestataire tiers de services TIC, que les entités financières dépendent de ces services directement ou indirectement, par des accords de sous-traitance;

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

i) l'absence de réelles solutions de substitution, même partielles, en raison du nombre limité de prestataires tiers de services TIC actifs sur un marché donné, ou de la part de marché du prestataire tiers de services TIC 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 prestataire tiers de services TIC;

ii) des difficultés liées à la migration partielle ou totale des données et des charges de travail pertinentes du prestataire tiers de services TIC concerné vers un autre, en raison soit de coûts financiers importants, de contraintes de temps ou d'autres ressources que le processus de migration peut imposer, soit du risque lié aux TIC accru ou d'autres risques opérationnels auxquels l'entité financière est susceptible d'être exposée du fait de cette migration.

3. Lorsque le prestataire tiers de services TIC appartient à un groupe, les critères visés au paragraphe 2 sont considérés par rapport aux services TIC fournis par l'ensemble du groupe.

4. Les tiers critiques de services TIC qui font partie d'un groupe désignent une personne morale comme point de coordination afin de veiller à une représentation adéquate et à la communication avec le superviseur principal.

5. Le superviseur principal notifie au prestataire tiers de services TIC les résultats de l'évaluation menée en vue de la désignation visée au paragraphe 1, point a). Dans un délai de six semaines à compter de la notification, le prestataire tiers de services TIC peut adresser au superviseur principal une déclaration motivée contenant toute information pertinente aux fins de l'évaluation. Le superviseur principal tient compte de la déclaration motivée et peut demander que de plus amples informations soient transmises dans un délai de 30 jours civils à compter de la réception de cette déclaration.

Après avoir désigné un prestataire tiers de services TIC comme critique, les AES, agissant par l'intermédiaire du comité mixte, notifient au prestataire tiers de services TIC cette désignation ainsi que la date à partir de laquelle il fera effectivement l'objet d'activités de supervision. Cette date est fixée au plus tard un mois après la notification. Le prestataire tiers de services TIC notifie aux entités financières auxquelles il fournit des services la désignation le qualifiant de critique.

6. La Commission est habilitée à adopter un acte délégué conformément à l'article 57 pour compléter le présent règlement en précisant davantage les critères visés au paragraphe 2 du présent article, au plus tard le … [18 mois à compter de la date d'entrée en vigueur du présent règlement].

7. La désignation visée au paragraphe 1, point a), n'est pas employée tant que la Commission n'a pas adopté un acte délégué conformément au paragraphe 6.

8. La désignation visée au paragraphe 1, point a), ne s'applique pas:

   i) aux entités financières qui fournissent des services TIC à d'autres entités financières;

   ii) aux prestataires tiers de services TIC 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;

   iii) aux prestataires tiers de services TIC intra-groupe;

iv) aux prestataires tiers de services TIC qui fournissent des services TIC dans un seul État membre à des entités financières qui ne sont actives que dans cet État membre.

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

10. Aux fins du paragraphe 1, point a), les autorités compétentes transmettent, sur une base annuelle et agrégée, les rapports visés à l'article 28, paragraphe 3, troisième alinéa, au forum de supervision institué en vertu de l'article 32. Le forum de supervision évalue les relations de dépendance des entités financières à l'égard de prestataires tiers de services TIC sur la base des informations reçues des autorités compétentes.

11. Les prestataires tiers de services TIC qui ne figurent pas sur la liste visée au paragraphe 9 peuvent demander à être désignés comme critiques conformément au paragraphe 1, point a).

Aux fins du premier alinéa, le prestataire tiers de services TIC présente une demande motivée à l'ABE, à l'AEMF ou à l'AEAPP, lesquelles, par l'intermédiaire du comité mixte, décident de désigner ou non ce prestataire tiers de services TIC comme critique conformément au paragraphe 1, point a).

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

12. Les entités financières ne font appel aux services d'un prestataire tiers de services TIC établi dans un pays tiers et ayant été désigné comme critique en vertu du paragraphe 1, point a), que si ce dernier a établi une filiale dans l'Union dans un délai de 12 mois à compter de la désignation.

13. Le prestataire tiers critique de services TIC visé au paragraphe 12 notifie au superviseur principal toute modification de la structure de la direction de la filiale établie dans l'Union.

Article 32

Structure du cadre de supervision

1. Le comité mixte institue, conformément à l'article 57, paragraphe 1, des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 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 31, paragraphe 1, point b), dans le domaine des risques liés aux prestataires tiers de services TIC 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 des TIC et promeut une approche cohérente dans le suivi des risques liés aux prestataires tiers de services TIC au niveau 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 prestataires tiers critiques de services TIC 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 prestataires tiers critiques de services TIC, qui seront adoptés par le comité mixte en tant que positions communes des AES, conformément à l'article 56, paragraphe 1, des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

4. Le forum de supervision se compose:

a) des présidents des AES;

b) d'un représentant de haut niveau du personnel en poste de l'autorité compétente concernée de chaque État membre, visée à l'article 46;

c) des directeurs exécutifs de chaque AES et d'un représentant de la Commission, du CERS, de la BCE et de l'ENISA, en qualité d'observateurs;

d) s'il y a lieu, d'un représentant supplémentaire d'une autorité compétente visée à l'article 46, de chaque État membre, en qualité d'observateur;

e) le cas échéant, d'un représentant des autorités compétentes désignées ou établies conformément à la directive (UE) …/…[+], responsables de la supervision d'une entité essentielle ou importante relevant de ladite directive, qui a été désignée en tant que prestataire tiers critique de services TIC, en qualité d'observateur.

Le forum de supervision peut, le cas échéant, demander l'avis d'experts indépendants désignés conformément au paragraphe 6.

5. Chaque État membre désigne l'autorité compétente concernée dont le membre du personnel est le représentant de haut niveau visé au paragraphe 4, premier alinéa, point b), et en informe le superviseur principal.

Les AES publient sur leur site internet la liste des représentants de haut niveau désignés par les États membres au sein de l'actuel personnel de l'autorité compétente concernée.

6. Les experts indépendants visés au paragraphe 4, deuxième alinéa, sont désignés par le forum de supervision parmi un groupe d'experts sélectionnés à l'issue d'une procédure de candidature publique et transparente.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

Les experts indépendants sont désignés sur la base de leur expertise en matière de stabilité financière, de résilience opérationnelle numérique et de questions de sécurité des TIC. Ils agissent en toute indépendance et objectivité dans le seul intérêt de l'ensemble de l'Union et ne sollicitent ni ne suivent aucune instruction émanant des institutions ou organes de l'Union, des gouvernements des États membres ou d'autres entités publiques ou privées.

7. Conformément à l'article 16 des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010, les AES publient au plus tard le … [18 mois après la date d'entrée en vigueur du présent règlement], aux fins de la présente section, des orientations sur la coopération entre les AES et les autorités compétentes concernant les procédures et les conditions détaillées relatives à la répartition et à l'exécution des tâches entre les autorités compétentes et les AES, ainsi que les modalités des échanges d'informations qui sont nécessaires aux autorités compétentes pour assurer le suivi des recommandations, conformément à l'article 35, paragraphe 1, point d), adressées aux prestataires tiers critiques de services TIC.

8. Les exigences énoncées dans la présente section sont sans préjudice de l'application de la directive (UE) …/…[+] et des autres règles de l'Union en matière de supervision applicables aux fournisseurs de services d'informatique en nuage.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

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

Article 33

Tâches du superviseur principal

1. Le superviseur principal, désigné conformément à l'article 31, paragraphe 1, point b), assure la supervision des prestataires tiers critiques de services TIC assignés et est, aux fins de toutes les questions liées à la supervision, le premier point de contact de ces prestataires tiers critiques de services TIC.

2. Aux fins du paragraphe 1, le superviseur principal détermine si chaque prestataire tiers critique de services TIC a mis en place des règles, des procédures, des mécanismes et des dispositifs complets, solides et efficaces pour gérer le risque lié aux TIC qu'il est susceptible de faire peser sur les entités financières.

   L'évaluation visée au premier alinéa porte essentiellement sur les services TIC fournis par le prestataire tiers critique de services TIC qui soutient les fonctions critiques ou importantes des entités financières. Lorsque cela est nécessaire pour parer à tous les risques pertinents, cette évaluation s'étend aux services TIC qui soutiennent des fonctions autres que celles qui sont critiques ou importantes.

3. L'évaluation visée au paragraphe 2 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 prestataire tiers critique de services TIC fournit aux entités financières, ainsi que la capacité à maintenir à tout moment des normes élevées de disponibilité, d'authenticité, d'intégrité ou de confidentialité des données;

b) la sécurité physique qui contribue à assurer la sécurité des TIC, 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 du risque lié aux TIC, la politique de continuité des activités de TIC et les plans de réponse et de rétablissement des TIC;

d) les modalités de gouvernance, notamment une structure organisationnelle comportant des lignes de responsabilité et des règles d'imputabilité claires, transparentes et cohérentes permettant une gestion efficace du risque lié aux TIC;

e) le recensement et le suivi des incidents importants liés aux TIC, 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 de TIC;

h) les audits des TIC;

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

4. Sur la base de l'évaluation visée au paragraphe 2, et en coordination avec le réseau de supervision commun visé à l'article 34, paragraphe 1, le superviseur principal adopte un plan de supervision individuel clair, détaillé et motivé décrivant les objectifs annuels de supervision et les principales actions de supervision prévues pour chaque prestataire tiers critique de services TIC. Ce plan est communiqué chaque année au prestataire tiers critique de services TIC.

Avant l'adoption du plan de supervision, le superviseur principal communique le projet de plan de surveillance au prestataire tiers critique de services TIC.

Dès réception du projet de plan de supervision, le prestataire tiers critique de services TIC peut présenter, dans un délai de quinze jours civils, une déclaration motivée dans laquelle il démontre l'incidence attendue sur les clients qui sont des entités ne relevant pas du champ d'application du présent règlement et formule, le cas échéant, des solutions pour atténuer les risques.

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

Article 34

Coordination opérationnelle entre superviseurs principaux

1. Afin de garantir une approche cohérente en matière d'activités de supervision et en vue de permettre la coordination des stratégies générales de supervision ainsi que des approches opérationnelles et des méthodes de travail cohérentes, les trois superviseurs principaux désignés conformément à l'article 31, paragraphe 1, point b), mettent en place un réseau de supervision commun pour assurer la coordination de leurs activités au cours des phases préparatoires et durant l'exécution des activités de supervision de leurs prestataires tiers critiques de services TIC respectifs qui font l'objet d'une supervision, ainsi qu'au cours de toute action qui pourrait s'avérer nécessaire en vertu de l'article 42.

2. Aux fins du paragraphe 1, les superviseurs principaux élaborent un protocole de supervision commun précisant les procédures détaillées à suivre pour assurer la coordination quotidienne et permettre des échanges et des réactions rapides. Le protocole est révisé périodiquement pour tenir compte des besoins opérationnels, en particulier de l'évolution des modalités pratiques de supervision.

3. Les superviseurs principaux peuvent, sur une base ad hoc, demander à la BCE et à l'ENISA de fournir des conseils techniques, de partager leur expérience pratique ou de participer à des réunions de coordination spécifiques du réseau de supervision commun.

Article 35

Pouvoirs du superviseur principal

1. Aux fins de l'exécution des tâches prévues dans la présente section, le superviseur principal dispose des pouvoirs suivants en ce qui concerne les prestataires tiers critiques de services TIC:

a) demander l'ensemble des informations et des documents pertinents conformément à l'article 37;

b) mener des enquêtes et des inspections générales conformément à l'article 38 et à l'article 39, respectivement;

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 prestataires tiers critiques de services TIC en ce qui concerne les recommandations visées au point d) du présent paragraphe;

d) formuler des recommandations dans les domaines visés à l'article 33, paragraphe 3, 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, en particulier 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 en matière de TIC 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 prestataires tiers critiques de services TIC fournissent des services TIC 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) toute sous-traitance envisagée, lorsque le superviseur principal estime que la poursuite de la sous-traitance, y compris les accords d'externalisation que les prestataires tiers critiques de services TIC prévoient de conclure avec des prestataires tiers de services TIC ou avec des sous-traitants de TIC établis dans un pays tiers, peut entraîner des risques pour la fourniture de services par l'entité financière ou des risques pour la stabilité financière, sur la base de l'examen des informations recueillies conformément aux articles 37 et 38;

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

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

– la sous-traitance concerne des fonctions critiques ou importantes de l'entité financière; et

– le superviseur principal estime que le recours à la sous-traitance présente un risque clair et sérieux pour la stabilité financière de l'Union ou pour les entités financières, y compris en ce qui concerne la capacité des entités financières à se conformer aux exigences prudentielles.

Aux fins du point iv) du présent point, les prestataires tiers de services TIC transmettent au superviseur principal, en utilisant le modèle visé à l'article 41, paragraphe 1, point b), les informations relatives à la sous-traitance.

2. Lorsqu'il exerce les pouvoirs visés au présent article, le superviseur principal:

a) assure une coordination régulière au sein du réseau de supervision commun et, en particulier, s'efforce d'adopter des approches cohérentes, le cas échéant, en ce qui concerne la supervision des prestataires tiers critiques de services TIC;

b) tient dûment compte du cadre établi par la directive (UE) …/…[+] et, s'il y a lieu, consulte les autorités compétentes concernées désignées ou établies conformément à ladite directive, afin d'éviter la duplication des mesures techniques et organisationnelles qui pourraient s'appliquer aux prestataires tiers critiques de services TIC en vertu de ladite directive;

c) s'efforce de réduire au minimum, dans la mesure du possible, le risque de perturbation des services fournis par des prestataires tiers critiques de services TIC à des clients qui sont des entités ne relevant pas du champ d'application du présent règlement.

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

Avant de formuler des recommandations conformément au paragraphe 1, point d), le superviseur principal donne au prestataire tiers de services TIC la possibilité de fournir, dans un délai de trente jours civils, des informations pertinentes dans lesquelles il démontre l'incidence attendue sur les clients qui sont des entités ne relevant pas du champ d'application du présent règlement et, le cas échéant, formule des solutions pour atténuer les risques.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

4. Le superviseur principal informe le réseau de supervision commun du résultat de l'exercice des pouvoirs visés au paragraphe 1, points a) et b). Le superviseur principal transmet sans retard injustifié les rapports visés au paragraphe 1, point c), au réseau de supervision commun et aux autorités compétentes des entités financières qui utilisent les services TIC de ce prestataire tiers critique de services TIC.

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

6. En cas de non-respect total ou partiel des mesures à adopter en vertu de l'exercice des pouvoirs visés au paragraphe 1, points a), b) et c), et après l'expiration d'un délai d'au moins trente jours civils à compter de la date à laquelle le prestataire tiers critique de services TIC a reçu notification des mesures correspondantes, le superviseur principal adopte une décision imposant une astreinte pour obliger le prestataire tiers critique de services TIC à se conformer à ces mesures.

7. L'astreinte visée au paragraphe 6 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 prestataire tiers critique de services TIC de la décision d'imposer une astreinte.

8. Le montant de l'astreinte, calculé à partir de la date indiquée dans la décision d'astreinte, est égal à 1 % au maximum du chiffre d'affaires quotidien moyen réalisé au niveau mondial par le prestataire tiers critique de services TIC au cours de l'exercice précédent. Lorsqu'il détermine le montant de l'astreinte, le superviseur principal tient compte des critères suivants concernant le non-respect des mesures visées au paragraphe 6:

i) la gravité et la durée du non-respect;

ii) si le non-respect est délibéré ou résulte d'une négligence;

iii) le niveau de coopération du prestataire tiers de services TIC avec le superviseur principal.

Aux fins du premier alinéa, afin de garantir une approche cohérente, le superviseur principal procède à des consultations au sein du réseau de supervision commun.

9. 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.

10. Le superviseur principal rend 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.

11. Avant d'imposer une astreinte en vertu du paragraphe 6, le superviseur principal donne aux représentants du prestataire tiers critique de services TIC 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 prestataire tiers critique de services TIC 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. Le prestataire tiers critique de services TIC faisant l'objet de la procédure dispose 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 36

Exercice des pouvoirs du superviseur principal en dehors de l'Union

1. Lorsque les objectifs en matière de supervision ne peuvent être atteints en interagissant avec la filiale créée aux fins de l'article 31, paragraphe 12, ou en exerçant des activités de supervision dans des locaux situés dans l'Union, le superviseur principal peut exercer les pouvoirs visés ci-après dans tout local situé dans un pays tiers qui est détenu, ou utilisé de quelque manière que ce soit, aux fins de la fourniture de services à des entités financières de l'Union par un prestataire tiers critique de services TIC, dans le cadre de ses activités, de ses fonctions ou de ses services, y compris tout bureau administratif, commercial ou opérationnel, tout local, terrain, bâtiment ou autre bien immobilier:

a) à l'article 35, paragraphe 1, point a); et

b) à l'article 35, paragraphe 1, point b), conformément à l'article 38, paragraphe 2, points a), b) et d), et à l'article 39, paragraphe 1, et à l'article 39, paragraphe 2, point a).

Les pouvoirs visés au premier alinéa peuvent être exercés pour autant que l'ensemble des conditions suivantes soient remplies:

i) le superviseur principal juge qu'il est nécessaire de réaliser une inspection dans un pays tiers pour pouvoir s'acquitter pleinement et efficacement des tâches qui lui incombent en vertu du présent règlement;

ii) l'inspection dans un pays tiers est directement liée à la fourniture de services TIC à des entités financières dans l'Union;

iii) le prestataire tiers critique de services TIC concerné consent à la réalisation d'une inspection dans un pays tiers; et

iv) l'autorité compétente du pays tiers concerné a été officiellement informée par le superviseur principal et n'a soulevé aucune objection à cet égard.

2. Sans préjudice des compétences respectives des institutions de l'Union et des États membres, aux fins du paragraphe 1, l'ABE, l'AEMF ou l'AEAPP conclut des accords de coopération administrative avec l'autorité compétente du pays tiers afin de permettre le bon déroulement des inspections menées dans le pays tiers concerné par le superviseur principal et son équipe désignée pour sa mission dans ce pays tiers. Ces accords de coopération ne créent pas d'obligations juridiques à l'égard de l'Union et de ses États membres et n'empêchent pas les États membres et leurs autorités compétentes de conclure des accords bilatéraux ou multilatéraux avec ces pays tiers et leurs autorités concernées.

Ces accords de coopération précisent au moins les éléments suivants:

a) les procédures de coordination des activités de supervision menées au titre du présent règlement et tout contrôle analogue du risque lié aux prestataires tiers de services TIC dans le secteur financier exercé par l'autorité compétente du pays tiers concerné, y compris les modalités de transmission de l'accord de cette dernière visant à permettre au superviseur principal et à son équipe désignée de mener les enquêtes générales et les inspections sur place visées au paragraphe 1, premier alinéa, sur le territoire relevant de sa juridiction;

b) le mécanisme de transmission de toute information pertinente entre l'ABE, l'AEMF ou l'AEAPP et l'autorité concernée du pays tiers concerné, en particulier en ce qui concerne les informations qui peuvent être demandées par le superviseur principal en vertu de l'article 37;

c) les mécanismes de notification rapide, par l'autorité compétente du pays tiers concerné, à l'ABE, à l'AEMF ou à l'AEAPP des cas où un prestataire tiers de services TIC établi dans un pays tiers et désigné comme critique conformément à l'article 31, paragraphe 1, point a), est réputé avoir enfreint les exigences auxquelles il est tenu d'adhérer en vertu du droit applicable du pays tiers concerné lorsqu'il fournit des services à des établissements financiers dans ce pays tiers, ainsi que les voies de recours et les sanctions appliquées;

d) la transmission régulière d'informations actualisées sur l'évolution de la réglementation ou de la supervision en matière de suivi du risque lié aux prestataires tiers de services TIC des établissements financiers dans le pays tiers concerné;

e) les modalités permettant, si nécessaire, la participation d'un représentant de l'autorité compétente du pays tiers aux inspections menées par le superviseur principal et l'équipe désignée.

3. Lorsque le superviseur principal n'est pas en mesure de mener les activités de supervision, en dehors de l'Union, visées aux paragraphes 1 et 2, il:

a) exerce les pouvoirs qui lui sont conférés en vertu de l'article 35 sur la base de tous les faits et documents dont il dispose;

b) documente et explique toute conséquence résultant de son incapacité à mener les activités de supervision envisagées visées au présent article.

Les conséquences potentielles visées au point b) du présent paragraphe sont prises en considération dans les recommandations formulées par le superviseur principal conformément à l'article 35, paragraphe 1, point d).

Article 37

Demande d'informations

1. Le superviseur principal peut, sur simple demande ou par voie de décision, exiger des prestataires tiers critiques de services TIC 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 des TIC, rapports d'incidents liés aux TIC, ainsi que toute information relative aux parties auxquelles le prestataire tiers critique de services TIC 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 prestataire tiers critique de services TIC 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 35, paragraphe 6, pour le cas où les informations communiquées seraient incomplètes ou lorsque ces informations ne sont pas communiquées dans le délai fixé au point d) du présent paragraphe;

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 dénommée "Cour de justice") conformément aux articles 60 et 61 des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

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

5. Le superviseur principal transmet, sans retard, une copie de la décision portant sur la communication d'informations aux autorités compétentes des entités financières qui ont recours aux services pertinents des prestataires tiers critiques de services TIC ainsi qu'au réseau de supervision commun.

Article 38

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 conjoint visée à l'article 40, paragraphe 1, peut, si nécessaire, mener des enquêtes auprès des prestataires tiers critiques de services TIC.

2. Le superviseur principal a le pouvoir:

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

b) de prendre ou d'obtenir des copies certifiées conformes ou de prélever des extraits de ces dossiers, données, procédures documentées et tout autre document;

c) de convoquer les représentants du prestataire tiers critique de services TIC et de 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 d'enregistrer leurs réponses;

d) 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) de 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 35, paragraphe 6, lorsque les dossiers, données, procédures documentées ou autres documents requis, ou les réponses aux questions posées aux représentants du prestataire tiers de services TIC ne sont pas fournis ou sont incomplets.

4. Les représentants des prestataires tiers critiques de services TIC 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 35, paragraphe 6, les voies de recours existantes en vertu des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 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 le début de l'enquête, le superviseur principal informe les autorités compétentes des entités financières qui utilisent les services TIC de ce prestataire tiers critique de services TIC de l'enquête envisagée et de l'identité des personnes mandatées.

Le superviseur principal communique au réseau de supervision commun toutes les informations transmises en application du premier alinéa.

Article 39

Inspections

1. Afin d'exercer les fonctions qui lui incombent en vertu du présent règlement, le superviseur principal, assisté des équipes d'examen conjoint visées à l'article 40, paragraphe 1, peut pénétrer dans tout local professionnel, sur tout terrain ou sur toute propriété des prestataires tiers de services TIC, 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.

   Aux fins de l'exercice des pouvoirs visés au premier alinéa, le superviseur principal consulte le réseau de supervision commun.

2. Les agents et autres personnes mandatés par le superviseur principal pour effectuer une inspection sur place sont investis des pouvoirs suivants:

   a) pénétrer dans ces locaux professionnels, sur ces terrains ou sur ces propriétés; et

   b) sceller ces locaux professionnels, livres ou registres, pendant la durée de l'inspection et dans la mesure nécessaire à celle-ci.

Les agents et autres personnes mandatés par le superviseur principal 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 35, paragraphe 6, lorsque les représentants des prestataires tiers critiques de services TIC concernés ne se soumettent pas à l'inspection.

3. En temps utile avant le début de l'inspection, le superviseur principal informe les autorités compétentes des entités financières utilisant ce prestataire tiers de services TIC.

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

5. Avant toute inspection sur place prévue, le superviseur principal adresse un préavis raisonnable aux prestataires tiers critiques de services TIC, 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 prestataire tiers critique de services TIC se soumet aux inspections sur place ordonnées par décision du superviseur principal. La décision indique l'objet et le but de l'inspection, fixe la date à laquelle l'inspection commence et indique les astreintes prévues à l'article 35, paragraphe 6, les voies de recours existantes en vertu des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 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 prestataire tiers critique de services TIC s'oppose à une inspection ordonnée en vertu du présent article, le superviseur principal informe le prestataire tiers critique de services TIC des conséquences de cette opposition, et notamment de la possibilité qu'ont les autorités compétentes d'exiger des entités financières concernées de résilier les accords contractuels conclus avec ce prestataire tiers critique de services TIC.

Article 40

Supervision continue

1. Lorsqu'il mène des activités de supervision, en particulier des enquêtes générales ou des inspections, le superviseur principal est assisté par une équipe d'examen conjoint, constituée pour chaque prestataire tiers critique de services TIC.

2. L'équipe d'examen conjoint visée au paragraphe 1 se compose de membres du personnel:

   a) des AES;

   b) des autorités compétentes concernées qui assurent la surveillance des entités financières auxquelles le prestataire tiers critique de services TIC fournit des services TIC;

   c) de l'autorité nationale compétente visée à l'article 32, paragraphe 4, point e), à titre volontaire;

   d) d'une autorité nationale compétente de l'État membre dans lequel le prestataire tiers critique de services TIC est établi, à titre volontaire.

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 du superviseur principal (ci-après dénommé "coordonnateur du superviseur principal").

3. Dans les trois mois suivant la fin d'une enquête ou d'une inspection, le superviseur principal, après consultation du forum de supervision, adopte des recommandations qu'il adresse au prestataire tiers critique de services TIC en vertu des pouvoirs visés à l'article 35.

4. Les recommandations visées au paragraphe 3 sont immédiatement communiquées au prestataire tiers critique de services TIC et aux autorités compétentes des entités financières auxquelles il fournit des services TIC.

Aux fins de la réalisation des activités de supervision, le superviseur principal peut prendre en considération toute certification pertinente d'un tiers et tout rapport d'audit interne ou externe d'un prestataire tiers de services TIC mis à disposition par le prestataire tiers critique de services TIC.

Article 41

Harmonisation des conditions permettant l'exercice des activités de 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 prestataire tiers de services TIC dans la demande de désignation volontaire en tant que prestataire critique, en vertu de l'article 31, paragraphe 11;

   b) le contenu, la structure et le format des informations que les prestataires tiers de services TIC sont tenus de soumettre, de publier ou de fournir conformément à l'article 35, paragraphe 1, y compris le modèle destiné à la communication des informations relatives aux accords de sous-traitance;

   c) les critères pour déterminer la composition de l'équipe d'examen conjoint en vue de garantir une participation équilibrée des membres du personnel des AES et des autorités compétentes concernées, leur désignation, leurs tâches et leurs modalités de travail;

   d) les détails de l'évaluation, par les autorités compétentes, des mesures prises par des prestataires tiers critiques de services TIC sur la base des recommandations formulées par le superviseur principal conformément à l'article 42, paragraphe 3.

2. Les AES soumettent ces projets de normes techniques de réglementation à la Commission au plus tard le ... [18 mois à compter de la date d'entrée en vigueur du présent règlement].

Le pouvoir de compléter le présent règlement en adoptant les normes techniques de réglementation prévues au paragraphe 1 est délégué à la Commission conformément à la procédure prévue aux articles 10 à 14 des règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010.

Article 42

Suivi par les autorités compétentes

1. Dans les soixante jours civils suivant la réception des recommandations formulées par le superviseur principal conformément à l'article 35, paragraphe 1, point d), les prestataires tiers critiques de services TIC notifient au superviseur principal leur intention de suivre les recommandations ou fournissent une explication circonstanciée des raisons pour lesquelles elles ne suivront pas ces recommandations. Le superviseur principal transmet immédiatement ces informations aux autorités compétentes des entités financières concernées.

2. Le superviseur principal divulgue publiquement les cas où un prestataire tiers critique de services TIC ne présente pas au superviseur principal la notification prévue au paragraphe 1 ou ceux où l'explication fournie par le prestataire tiers critique de services TIC n'est pas jugée suffisante. Les informations publiées révèlent l'identité du prestataire tiers critique de services TIC et contiennent également des informations sur le type et la nature du non-respect. Ces informations sont limitées à ce qui est pertinent et proportionné aux fins de la sensibilisation du public, à moins que cette publication ne soit susceptible de causer un préjudice disproportionné aux parties concernées ou de compromettre gravement le bon fonctionnement et l'intégrité des marchés financiers ou la stabilité de tout ou partie du système financier de l'Union.

Le superviseur principal notifie cette divulgation publique au prestataire tiers de services TIC.

3. Les autorités compétentes informent les entités financières concernées des risques recensés dans les recommandations adressées aux prestataires tiers critiques de services TIC conformément à l'article 35, paragraphe 1, point d).

Lorsqu'elles gèrent le risque lié aux prestataires tiers de services TIC, les entités financières tiennent compte des risques visés au premier alinéa.

4. Lorsqu'une autorité compétente estime qu'une entité financière ne tient pas compte ou ne prend pas suffisamment en considération, dans le cadre de sa gestion du risque lié aux prestataires tiers de services TIC, des risques spécifiques recensés dans les recommandations, elle informe l'entité financière de la possibilité qu'une décision soit prise, dans un délai de soixante jours civils à compter de la réception d'une telle notification, conformément au paragraphe 6, en l'absence de dispositions contractuelles appropriées visant à parer à ces risques.

5. Dès qu'elles reçoivent les rapports visés à l'article 35, paragraphe 1, point c), et avant de prendre la décision visée au paragraphe 6 du présent article, les autorités compétentes peuvent, à titre volontaire, consulter les autorités compétentes désignées ou établies conformément à la directive (UE) .../...[+], responsables de la supervision d'une entité essentielle ou importante relevant de ladite directive, qui a été désignée comme un prestataire tiers critique de services TIC.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

6. Les autorités compétentes peuvent, en dernier recours, après la notification et, le cas échéant, la consultation visée aux paragraphes 4 et 5 du présent article, conformément à l'article 50, exiger des entités financières qu'elles suspendent temporairement, en partie ou en totalité, l'utilisation ou le déploiement d'un service fourni par le prestataire tiers critique de services TIC, jusqu'à ce que les risques identifiés dans les recommandations adressées aux prestataires tiers critiques de services TIC 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 prestataires tiers critiques de services TIC.

7. Lorsqu'un prestataire tiers critique de services TIC refuse d'approuver des recommandations, en se fondant sur une approche qui diverge de celle recommandée par le superviseur principal, et que cette approche divergente pourrait avoir une incidence négative sur un grand nombre d'entités financières, ou sur une partie importante du secteur financier, et que les alertes individuelles émises par les autorités compétentes n'ont pas abouti à des approches cohérentes permettant d'atténuer le risque potentiel pour la stabilité financière, le superviseur principal peut, après avoir consulté le forum de supervision, émettre des avis non contraignants et non publics à l'intention des autorités compétentes, afin de promouvoir des mesures de suivi cohérentes et convergentes en matière de supervision, s'il y a lieu.

8. Dès réception des rapports visés à l'article 35, paragraphe 1, point c), les autorités compétentes, lorsqu'elles prennent la décision visée au paragraphe 6 du présent article, tiennent compte du type et de l'ampleur des risques qui n'ont pas été écartés par le prestataire tiers critique de services TIC, 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 prestataire tiers critique de services TIC;

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;

e) si la suspension ou la résiliation des accords contractuels entraîne un risque pour la continuité des activités de l'entité financière, en dépit des efforts déployés par l'entité financière pour éviter toute perturbation dans la fourniture de ses services;

f) le cas échéant, l'avis, sollicité à titre volontaire conformément au paragraphe 5 du présent article, des autorités compétentes désignées ou établies conformément à la directive (UE) …/…[+], responsables de la supervision d'une entité essentielle ou importante relevant de ladite directive, qui a été désignée en tant que prestataire tiers critique de services TIC.

Les autorités compétentes accordent aux entités financières le délai nécessaire pour leur permettre d'adapter les accords contractuels conclus avec des prestataires tiers critiques de services TIC, afin d'éviter des effets préjudiciables sur leur résilience opérationnelle numérique et de leur permettre de déployer les stratégies de sortie et les plans de transition visés à l'article 28.

9. La décision visée au paragraphe 6 du présent article est notifiée aux membres du forum de supervision visés à l'article 32, paragraphe 4, points a), b) et c), ainsi qu'au réseau de supervision commun.

Les prestataires tiers critiques de services TIC concernés par les décisions prévues au paragraphe 6 coopèrent pleinement avec les entités financières affectées, en particulier dans le cadre du processus de suspension ou de résiliation de leurs accords contractuels.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

10. Les autorités compétentes informent régulièrement le superviseur principal des approches suivies et des mesures prises dans le cadre de leurs tâches de surveillance des entités financières, ainsi que des accords contractuels conclus par les entités financières lorsque des prestataires tiers critiques de services TIC n'ont pas suivi, en partie ou en totalité, les recommandations qui leur ont été adressées par le superviseur principal.

11. Le superviseur principal peut, sur demande, fournir des précisions supplémentaires sur les recommandations émises afin de donner des orientations aux autorités compétentes concernant les mesures de suivi.

Article 43

Redevances de supervision

1. Conformément à l'acte délégué visé au paragraphe 2 du présent article, le superviseur principal perçoit, auprès des prestataires tiers critiques de services TIC, des redevances qui couvrent intégralement les dépenses que le superviseur principal doit engager pour exercer les tâches de supervision que lui assigne le présent règlement, y compris le remboursement de tous les coûts pouvant résulter des travaux effectués par l'équipe d'examen conjoint visée à l'article 40, ainsi que les coûts des conseils fournis par les experts indépendants visés à l'article 32, paragraphe 4, deuxième alinéa, en rapport avec les questions liées aux activités de supervision directes.

Le montant de la redevance perçue auprès d'un prestataire tiers critique de services TIC couvre tous les frais afférents à l'exécution des tâches exposées dans la présente section et est proportionnel à son chiffre d'affaires.

2. La Commission est habilitée à adopter un acte délégué conformément à l'article 57 pour compléter le présent règlement en déterminant le montant des redevances et leurs modalités de paiement au plus tard le … [18 mois à compter de la date d'entrée en vigueur du présent règlement].

Article 44

Coopération internationale

1. Sans préjudice de l'article 36, l'ABE, l'AEMF et l'AEAPP peuvent, conformément à l'article 33 des règlements (UE) n° 1093/2010, (UE) n° 1095/2010 et (UE) n° 1094/2010, 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 prestataires tiers de services TIC dans différents secteurs financiers, en particulier en élaborant des bonnes pratiques pour l'examen des pratiques et des contrôles en matière de gestion du risque lié aux TIC, 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 prestataires tiers de services TIC et sur ses implications pour la stabilité financière, l'intégrité du marché, la protection des investisseurs et le fonctionnement du marché intérieur.

Chapitre VI
Dispositifs de partage d'informations

Article 45

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 les capacités de défense, les techniques de détection des menaces et les stratégies d'atténuation ou les 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 conformément au règlement (UE) 2016/679 et des lignes directrices sur la politique de concurrence.

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, les modalités de la participation des prestataires tiers de services TIC, ainsi que les aspects opérationnels de ce partage, y compris de l'utilisation de plateformes de TIC 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 46

Autorités compétentes

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

a) pour les établissements de crédit et pour les établissements exemptés en vertu de la directive 2013/36/UE, l'autorité compétente désignée conformément à l'article 4 de ladite directive, et pour les établissements de crédit classés comme importants conformément à l'article 6, paragraphe 4, du règlement (UE) n° 1024/2013, la BCE conformément aux pouvoirs et missions conférés par ledit règlement;

b) pour les établissements de paiement, y compris les établissements de paiement exemptés en vertu de la directive (UE) 2015/2366, les établissements de monnaie électronique exemptés en vertu de la directive 2009/110/CE et les prestataires de services d'information sur les comptes visés à l'article 33, paragraphe 1, de la directive (UE) 2015/2366, l'autorité compétente désignée conformément à l'article 22 de la directive (UE) 2015/2366;

c) pour les entreprises d'investissement, l'autorité compétente désignée conformément à l'article 4 de la directive (UE) 2019/2034 du Parlement européen et du Conseil[1];

d) pour les prestataires de services sur crypto-actifs, agréés en vertu du règlement sur les marchés de crypto-actifs et les émetteurs de jetons se référant à un ou des actifs, l'autorité compétente désignée conformément à la disposition pertinente dudit règlement;

e) pour les dépositaires centraux de titres, l'autorité compétente désignée conformément à l'article 11 du règlement (UE) n° 909/2014;

f) pour les contreparties centrales, l'autorité compétente désignée conformément à l'article 22 du règlement (UE) n° 648/2012;

---

[1] Directive (UE) 2019/2034 du Parlement européen et du Conseil du 27 novembre 2019 concernant la surveillance prudentielle des entreprises d'investissement et modifiant les directives 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE et 2014/65/UE (JO L 314 du 5.12.2019, p. 64).

g) 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, et l'autorité compétente définie à l'article 2, paragraphe 1, point 18), du règlement (UE) n° 600/2014;

h) pour les référentiels centraux, l'autorité compétente désignée conformément à l'article 22 du règlement (UE) n° 648/2012;

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

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

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

l) 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;

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

n) pour les agences de notation de crédit, l'autorité compétente désignée conformément à l'article 21 du règlement (CE) n° 1060/2009;

o) pour les administrateurs d'indices de référence d'importance critique, l'autorité compétente désignée conformément aux articles 40 et 41 du règlement (UE) 2016/1011;

p) pour les prestataires de services de financement participatif, l'autorité compétente désignée conformément à l'article 29 du règlement(UE) 2020/1503;

q) pour les référentiels des titrisations, l'autorité compétente désignée conformément à l'article 10 et à l'article 14, paragraphe 1, du règlement (UE) n° 2017/2402.

Article 47

Coopération avec les structures et autorités établies par la directive (UE) .../...[+]

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 14 de la directive (UE) …/…[+], les AES et les autorités compétentes peuvent participer aux activités du groupe de coopération pour les questions qui concernent leurs activités de supervision liées aux entités financières. Les AES et les autorités compétentes peuvent demander à être invitées à participer aux activités du groupe de coopération pour les questions en lien avec les entités essentielles ou importantes relevant de la directive (UE) …/…[+] qui ont également été désignées comme des prestataires tiers critiques de services TIC en vertu de l'article 31 du présent règlement.

2. Le cas échéant, les autorités compétentes peuvent consulter les points de contact uniques et les CSIRT désignés ou établis conformément à la directive (UE) …/…[+] et partager des informations avec ceux-ci.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

3. Le cas échéant, les autorités compétentes peuvent demander tout conseil et assistance technique pertinents aux autorités compétentes désignées ou établies conformément à la directive (UE) …/…[+] et établir des accords de coopération permettant la mise en place de mécanismes de coordination efficaces et rapides.

4. Les accords visés au paragraphe 3 du présent article peuvent, entre autres, préciser les procédures relatives à la coordination des activités de surveillance et de supervision en ce qui concerne les entités essentielles ou importantes relevant de la directive (UE) …/…[+] qui ont été désignées comme prestataires tiers critiques de services TIC en vertu de l'article 31 du présent règlement, ainsi que les procédures relatives à la réalisation, conformément au droit national, d'enquêtes et d'inspections sur place, et les procédures régissant les mécanismes d'échange d'informations entre les autorités compétentes relevant du présent règlement et les autorités compétentes désignées ou établies conformément à ladite directive, y compris l'accès aux informations demandées par ces dernières.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

Article 48

Coopération entre autorités

1. Les autorités compétentes coopèrent étroitement entre elles et, le cas échéant, avec le superviseur principal.

2. Les autorités compétentes et le superviseur principal s'échangent mutuellement, en temps utile, toutes les informations pertinentes concernant les prestataires tiers critiques de services TIC qui leur sont nécessaires pour s'acquitter des missions qui leur incombent en vertu du présent règlement, en particulier en ce qui concerne les risques recensés, les approches et les mesures adoptées dans le cadre des tâches de supervision du superviseur principal.

Article 49

Exercices, communication et coopération entre secteurs financiers

1. Les AES, agissant par l'intermédiaire du comité mixte et en collaboration avec les autorités compétentes, les autorités de résolution visées à l'article 3 de la directive 2014/59/UE, la BCE, le Conseil de résolution unique en ce qui concerne les informations relatives aux entités relevant du champ d'application du règlement (UE) n° 806/2014, le CERS et l'ENISA, le cas échéant, 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 aux TIC ou de menace connexe ayant une incidence systémique sur l'ensemble du secteur financier de l'Union.

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

2. Les autorités compétentes, les AES et la BCE coopèrent étroitement entre elles et échangent des informations afin de s'acquitter de leurs missions conformément aux articles 47 à 54. 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 50

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 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, qui comprennent, sans s'y limiter, les actions suivantes:

i) convoquer les représentants des entités financières 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;

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

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 52, 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 effectives, 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 qui constitue une violation du présent règlement 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 le paragraphe 2, point c), et le 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 visées au paragraphe 2, point c), soit dûment motivée et puisse faire l'objet d'un recours.

Article 51

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 50 conformément à leurs cadres juridiques nationaux, et, selon le cas, comme suit:

   a) directement;

   b) en collaboration avec d'autres autorités;

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

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 50, tiennent compte de la mesure dans laquelle la violation est intentionnelle ou résulte d'une négligence ainsi que de toutes les autres circonstances pertinentes, et notamment, le cas échéant, des éléments suivants:

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

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

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

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

f) le 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 physique ou morale;

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

Article 52

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 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 53

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 … [24 mois à compter de la date d'entrée en vigueur du présent règlement]. Les États membres notifient à la Commission, à l'AEMF, à l'ABE et à l'AEAPP, sans retard injustifié, toute modification ultérieure desdites dispositions.

Article 54

Application de sanctions administratives

1. Les autorités compétentes publient sur leur site internet officiel, sans retard injustifié, 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, notamment en ce qui concerne les risques liés à la protection des données à caractère personnel, 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 internet officiel et y publient, ultérieurement, 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 ne demeure sur leur site internet officiel que pendant la période nécessaire aux fins de l'entrée en vigueur du présent article. Cette période n'excède pas cinq ans à compter de sa publication.

Article 55

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, y compris l'échange d'information entre les autorités compétentes relevant du présent règlement et les autorités compétentes désignées ou établies conformément à la directive (UE) …/…[+], 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.

[+] JO: veuillez insérer, dans le texte, le numéro du règlement figurant dans le document PE-CONS 32/22 (2020/0359 (COD)).

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.

Article 56

Protection des données

1. Les AES et les autorités compétentes ne sont autorisées à traiter des données à caractère personnel que lorsque cela est nécessaire à l'accomplissement de leurs obligations et missions respectives en vertu du présent règlement, en particulier en matière d'enquête, d'inspection, de demande d'informations, de communication, de publication, d'évaluation, de vérification, d'évaluation et d'élaboration de plans de supervision. Les données à caractère personnel sont traitées conformément au règlement (UE) 2016/679 ou au règlement (UE) 2018/1725, selon le cas.

2. Sauf disposition contraire dans d'autres actes sectoriels, les données à caractère personnel visées au paragraphe 1 sont conservées jusqu'à l'accomplissement des missions de contrôle applicables et, en tout état de cause, pendant une période maximale de quinze ans, sauf dans le cas de procédures judiciaires en cours nécessitant la conservation de ces données pendant une période plus longue.

Chapitre VIII
Actes délégués

Article 57

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 31, paragraphe 6, et à l'article 43, paragraphe 2, est conféré à la Commission pour une période de cinq ans à compter du ... [12 mois à compter de la date d'entrée en vigueur du présent règlement]. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 31, paragraphe 6, et à l'article 43, paragraphe 2, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. 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 qui est précisée dans ladite 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 au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 31, paragraphe 6, et de l'article 43, paragraphe 2, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois 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 trois mois à l'initiative du Parlement européen ou du Conseil.

Chapitre IX
Dispositions transitoires et finales

SECTION I

Article 58

Clause de réexamen

1. Au plus tard le … [5 ans après la date d'entrée en vigueur du présent règlement], la Commission, après avoir consulté les AES 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. Le réexamen porte au moins sur les points suivants:

   a) les critères de désignation des prestataires tiers critiques de services TIC conformément à l'article 31, paragraphe 2;

   b) le caractère volontaire de la notification des cybermenaces importantes, visé à l'article 19;

c) le régime visé à l'article 31, paragraphe 12, et les pouvoirs du superviseur principal prévus à l'article 35, paragraphe 1, point d) iv), premier tiret, en vue d'évaluer l'efficacité de ces dispositions pour assurer une supervision efficace des prestataires tiers critiques de services TIC établis dans un pays tiers, et la nécessité d'établir une filiale dans l'Union.

Aux fins du premier alinéa du présent point, le réexamen comprend une analyse du régime visé à l'article 31, paragraphe 12, y compris les conditions d'accès des entités financières de l'Union aux services de pays tiers et la disponibilité de services sur le marché de l'Union, et il tient compte de l'évolution des marchés des services couverts par le présent règlement, de l'expérience pratique des entités financières et des superviseurs financiers en ce qui concerne l'application et, respectivement, la supervision de ce régime, ainsi que de toute évolution pertinente en matière de réglementation et de supervision au niveau international;

d) l'opportunité d'inclure dans le champ d'application du présent règlement les entités financières visées à l'article 2, paragraphe 3, point e), qui font usage de systèmes de vente automatisés, compte tenu de l'évolution future du marché en ce qui concerne l'utilisation de ces systèmes;

e) le fonctionnement et l'efficacité du réseau de supervision commun pour ce qui est de soutenir la cohérence de la supervision et l'efficacité de l'échange d'informations au sein du cadre de supervision.

2. Dans le cadre du réexamen de la directive (UE) 2015/2366, la Commission évalue la nécessité de renforcer la cyberrésilience des systèmes de paiement et des activités de traitement de paiements, ainsi que l'opportunité d'étendre le champ d'application du présent règlement aux opérateurs de systèmes de paiement et aux entités participant aux activités de traitement de paiements. À la lumière de cette évaluation, la Commission soumet, dans le cadre du réexamen de la directive (UE) 2015/2366, un rapport au Parlement européen et au Conseil au plus tard le … [6 mois à compter de la date d'entrée en vigueur du présent règlement].

Sur la base de ce rapport de réexamen, et après avoir consulté les AES, la BCE et le CERS, la Commission peut présenter, le cas échéant et dans le cadre de la proposition législative qu'elle peut adopter en vertu de l'article 108, deuxième alinéa, de la directive (UE) 2015/2366, une proposition visant à faire en sorte que tous les opérateurs de systèmes de paiement et entités participant à des activités de traitement des paiements fassent l'objet d'une surveillance appropriée, tout en tenant compte de la supervision existante par la banque centrale.

3. Au plus tard le … [3 ans après la date d'entrée en vigueur du présent règlement], la Commission, après avoir consulté les AES et le comité des organes européens de supervision de l'audit, procède à un réexamen et remet au Parlement européen et au Conseil un rapport, accompagné, le cas échéant, d'une proposition législative sur l'opportunité de renforcer les exigences applicables aux contrôleurs légaux des comptes et aux cabinets d'audit en ce qui concerne la résilience opérationnelle numérique, au moyen de l'inclusion des contrôleurs légaux des comptes et des cabinets d'audit dans le champ d'application du présent règlement ou au moyen de modifications de la directive 2006/43/CE du Parlement européen et du Conseil[1].

[1] Directive 2006/43/CE du Parlement européen et du Conseil du 17 mai 2006 concernant les contrôles légaux des comptes annuels et des comptes consolidés et modifiant les directives 78/660/CEE et 83/349/CEE du Conseil, et abrogeant la directive 84/253/CEE du Conseil (JO L 157 du 9.6.2006, p. 87).

SECTION II

MODIFICATIONS

Article 59

Modifications du règlement (CE) n° 1060/2009

Le règlement (CE) n° 1060/2009 est modifié comme suit:

1) À l'annexe I, section A, 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 de TIC conforme au règlement (UE) .../... du Parlement européen et du Conseil*+".

---

* Règlement (UE) .../... du Parlement européen et du Conseil du ... sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L ... du …, p. ...).".

\+ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)) et insérer le numéro, la date et la référence au JO dudit règlement dans la note de bas de page.

2) À l'annexe III, le point 12 est remplacé par le texte suivant:

"12. L'agence de notation de crédit enfreint l'article 6, paragraphe 2, en liaison avec l'annexe I, section A, point 4, en ne disposant pas de procédures comptables ou administratives saines, de mécanismes de contrôle interne, de procédures efficaces d'évaluation des risques ou de dispositifs efficaces de contrôle ou de sauvegarde pour une gestion des systèmes de TIC conforme au règlement (UE) …/…[+]; ou en ne mettant pas en œuvre ou en ne maintenant pas les procédures de prise de décision ou les structures organisationnelles requises par ledit point.".

[+] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)).

Article 60

Modifications du règlement (UE) n° 648/2012

Le règlement (UE) n° 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. Elles utilisent des systèmes, des ressources et des procédures appropriés et proportionnés, dont des systèmes de TIC gérés conformément au règlement (UE) …/… du Parlement européen et du Conseil*+.

* Règlement (UE) .../... du Parlement européen et du Conseil du ... sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L ... du …, p. ...).";

+ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)) et insérer le numéro, la date et la référence au JO dudit règlement dans la note de bas de page.

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 une politique de continuité des activités de TIC et des plans de réponse et de rétablissement dans le domaine des TIC mis en place et appliqués conformément au règlement (UE) …/…[+], 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:

"3. 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 de la politique de continuité des activités de TIC et des plans de rétablissement après sinistre des TIC.".

[+] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)).

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 du risque lié aux TIC.".

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 de TIC gérés conformément au règlement (UE) .../...[+].

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 une politique de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC établis conformément au règlement (UE) .../...[+], 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.

[+] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)).

6) À l'annexe I, la section II est modifiée comme suit:

a) les points a) et b) sont remplacés par le texte suivant:

"a) un référentiel central enfreint l'article 79, paragraphe 1, en ne détectant pas les sources de risques opérationnels ou en ne les réduisant pas au minimum en mettant en place des systèmes, des moyens de contrôle et des procédures appropriés, y compris des systèmes de TIC gérés conformément au règlement (UE) .../...[+];

b) un référentiel central enfreint l'article 79, paragraphe 2, en n'établissant pas, en ne mettant pas en œuvre et en ne tenant pas à jour une politique adéquate de continuité des activités et un plan de rétablissement après sinistre établis conformément au règlement (UE) .../...[+], visant à assurer la poursuite de ses fonctions, la reprise rapide de ses activités et le respect de ses obligations;";

b) le point c) est supprimé.

[+] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)).

7) L'annexe III est modifiée comme suit:

a) la section II est modifiée comme suit:

i) le point c) est remplacé par le texte suivant:

"c) une contrepartie centrale de catégorie 2 enfreint l'article 26, paragraphe 3, si elle ne maintient pas ou n'exploite pas une structure organisationnelle qui assure la continuité et le bon fonctionnement de la fourniture de ses services et de l'exercice de ses activités ou si elle n'utilise pas des systèmes, des ressources ou des procédures appropriés et proportionnés, y compris des systèmes de TIC gérés conformément au règlement (UE) .../...[+];

ii) le point f) est supprimé;

b) à la section III, le point a) est remplacé par le texte suivant:

"a) une contrepartie centrale de catégorie 2 enfreint l'article 34, paragraphe 1, si elle n'établit pas, ne met pas en œuvre ou ne tient pas à jour une politique adéquate de continuité des activités et un plan de réponse et de rétablissement établis conformément au règlement (UE) .../...[+], visant à assurer la préservation de ses fonctions, la reprise rapide de ses activités et le respect de ses obligations, prévoyant au moins la reprise de toutes les transactions en cours lorsque le dysfonctionnement est survenu, pour lui permettre de continuer à fonctionner de manière sûre et d'achever le règlement à la date programmée;".

[+] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)).

Article 61

Modifications du règlement (UE) n° 909/2014

L'article 45 du règlement (UE) n° 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 de TIC appropriés, mis en place et gérés conformément au règlement (UE) .../... du Parlement européen et du Conseil[*+], 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) .../... du Parlement européen et du Conseil du ... sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L ... du …, p. ...).".

[+] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)) et insérer le numéro, la date et la référence au JO dudit règlement dans la note de bas de page.

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 une politique de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC, établis conformément au règlement (UE) .../....[+], pour garantir le maintien de ses services, la reprise rapide de ses activités et le respect de ses obligations en cas d'événements 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 de TIC critiques puissent reprendre les opérations à partir du moment où s'est produit le dysfonctionnement, comme prévu à l'article 12, paragraphes 5 et 7, du règlement (UE) .../...[+].".

[+] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)).

4) Le paragraphe 6 est remplacé par le texte suivant:

"6. 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 retard l'autorité compétente et les autorités concernées de tout incident opérationnel, autre qu'en lien avec un risque lié aux TIC, résultant de ces risques.".

5) Au paragraphe 7, le premier alinéa est remplacé par le texte suivant:

"7. L'AEMF élabore, en étroite coopération avec les membres du SEBC, des projets de normes techniques de réglementation pour préciser les risques opérationnels visés aux paragraphes 1 et 6, autres que le risque lié aux TIC, 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 62

Modifications du règlement (UE) n° 600/2014

Le règlement (UE) n° 600/2014 est modifié comme suit:

1) L'article 27 *octies* est modifié comme suit:

a) le paragraphe 4 est remplacé par le texte suivant:

4. "Un APA se conforme aux exigences relatives à la sécurité des réseaux et des systèmes d'information énoncées dans le règlement (UE) .../... du Parlement européen et du Conseil[*+].

---

[*] Règlement (UE) .../... du Parlement européen et du Conseil du ... sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L ... du …, p. ...).";

[+] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)) et insérer le numéro, la date et la référence au JO dudit règlement dans la note de bas de page.

b) au paragraphe 8, le point c) est remplacé par le texte suivant:

"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 remplacé par le texte suivant:

"5. Le CTP se conforme aux exigences relatives à la sécurité des réseaux et des systèmes d'information énoncées dans le règlement (UE) .../...[+].";

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 remplacé par le texte suivant:

"3. L'ARM se conforme aux exigences relatives à la sécurité des réseaux et des systèmes d'information énoncées dans le règlement (UE) .../...[+].";

[+] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)).

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 63

Modification du règlement (UE) 2016/1011

À l'article 6 du règlement (UE) 2016/1011, le paragraphe suivant est ajouté:

"6. En ce qui concerne les indices de référence d'importance critique, un administrateur 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 de TIC conforme au règlement (UE) .../... du Parlement européen et du Conseil*+.

---

* Règlement (UE) .../... du Parlement européen et du Conseil du ... sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L ... du …, p. ...).".

\+ JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 41/22 (2020/0266 (COD)) et insérer le numéro, la date et la référence au JO dudit règlement dans la note de bas de page.

Article 64

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 ... [24 mois à compter de 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 ..., le

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président / La présidente*