III

(Actes préparatoires)

BANQUE CENTRALE EUROPÉENNE

AVIS DE LA BANQUE CENTRALE EUROPÉENNE

du 4 juin 2021

sur une proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier

(CON/2021/20)

(2021/C 343/01)

Introduction et fondement juridique

Les 22, 23 et 29 décembre 2020, la Banque centrale européenne (BCE) a reçu des demandes de consultation, respectivement, de la part du Conseil de l'Union européenne et du Parlement européen, concernant une proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements n° 1060/2009/CE, (UE) n° 648/2012, (UE) n° 600/2014 et (UE) n° 909/2014 ([1]) (ci-après le « règlement proposé »), et sur une proposition de directive modifiant les directives 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 ([2]) (ci-après la « directive modificative proposée » ensemble avec le règlement proposé, les « actes proposés »).

La BCE a compétence pour émettre un avis en vertu de l'article 127, paragraphe 4, et de l'article 282, paragraphe 5, du traité sur le fonctionnement de l'Union européenne, étant donné que les actes proposés contiennent des dispositions relevant des domaines de compétence de la BCE, notamment la définition et la mise en œuvre de la politique monétaire, la promotion du bon fonctionnement des systèmes de paiement, la contribution à la bonne conduite des politiques menées par les autorités compétentes en ce qui concerne la stabilité du système financier et les missions de la BCE ayant trait à la surveillance prudentielle des établissements de crédit en vertu de l'article 127, paragraphe 2, premier et quatrième tirets, et de l'article 127, paragraphes 5 et 6, du traité. Conformément à l'article 17.5, première phrase, du règlement intérieur de la Banque centrale européenne, le présent avis a été adopté par le conseil des gouverneurs.

1. Observations générales

1.1 La BCE accueille favorablement le règlement proposé qui vise à renforcer la cybersécurité et la résilience opérationnelle du secteur financier. En particulier, la BCE est favorable à l'objectif du règlement proposé consistant à supprimer des obstacles à l'établissement et au fonctionnement du marché intérieur des services financiers et y apporte des améliorations en harmonisant les règles applicables en matière de gestion des risques informatiques, de notification, de tests et de risques liés aux tiers prestataires de services informatiques. La BCE est également favorable à l'objectif du règlement proposé consistant à rationaliser et à harmoniser toutes exigences réglementaires ou attentes en matière de surveillance qui s'avèrent redondantes et auxquelles les entités financières sont actuellement soumises en vertu du droit de l'Union.

1.2 La BCE comprend que le règlement proposé constitue, vis-à-vis des entités financières identifiées comme opérateurs de services essentiels ([3]), une législation spécifique à un secteur (*lex specialis*) au sens de l'article 7, paragraphe 1, de la directive (UE) 2016/1148 du Parlement européen et du Conseil ([4]) (ci-après la « directive SRI »), ce qui implique que les obligations prévues dans le règlement proposé prévaudront, en principe, sur la directive SRI. En pratique, les entités financières identifiées comme opérateurs de services essentiels ([5])

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Voir l'article 1, paragraphe 2, du règlement proposé.
([4]) 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).
([5]) Voir l'article 5 de la directive SRI.

signaleraient, entre autres, les incidents conformément au règlement au lieu de la directive SRI. Si la BCE est favorable à la réduction des exigences potentiellement redondantes vis-à-vis des entités financières dans le domaine de la notification des incidents, elle estime toutefois qu'il conviendrait d'examiner plus en profondeur l'interaction entre le règlement proposé et la directive SRI. Par exemple, en vertu du règlement proposé les tiers prestataires de services informatiques ([6]) sont susceptibles de faire l'objet de recommandations émises par le superviseur principal ([7]). Par conséquent, le même tiers prestataire de services informatiques pourrait se voir qualifier d'opérateur de services essentiels au sens de la directive SRI tout en faisant l'objet d'instructions contraignantes émises par l'autorité compétente ([8]). Dans ce cas, le tiers prestataire de services informatiques pourrait faire l'objet de recommandations contradictoires qui seraient émises en vertu du règlement proposé et des instructions contraignantes émises au titre de la directive SRI. La BCE suggère que les organes législatifs de l'Union approfondissent leur réflexion au sujet des éventuelles incohérences entre le règlement proposé et la directive SRI qui risqueraient d'entraver l'harmonisation et la réduction des exigences redondantes et contradictoires pour les entités financières.

1.3 La BCE comprend également que, en vertu de la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 ([9]) (ci-après la « directive SRI2 proposée »), les « incidents évités » ([10]) feront l'objet d'obligations de notification ([11]). Si le considérant 39 de la directive SIR2 proposée fait bien référence à la signification de l'expression « incidents évités », il n'est toutefois pas certain que l'intention soit d'exiger le signalement des incidents évités par les entités financières énumérées à l'article 2 du règlement proposé. À cet égard, et compte tenu également du fait que les incidents évités ne peuvent être identifiés comme tels qu'une fois qu'ils se sont produits, la BCE apprécierait de recevoir en temps utile une notification des incidents évités importants, comme c'est déjà le cas pour les cyberincidents. La BCE suggère de renforcer la coordination entre le règlement proposé et la directive SIR2 proposée afin de clarifier le périmètre exact du signalement auquel toute entité financière donnée est susceptible d'être soumise en vertu de ces deux actes législatifs, distincts mais liés, de l'Union. Dans le même temps, il conviendrait de définir les « incident évités » et d'établir des dispositions précisant leur importance.

1.4 La BCE accueille favorablement le fait d'encourager les entités financières à partager, de manière volontaire, des renseignements sur les cybermenaces afin d'améliorer et de renforcer leurs positions en matière de cyberrésilience. La BCE elle-même a contribué à l'initiative pour le partage des cyber-informations et des cyber-renseignements (*Cyber Information and Intelligence Sharing Initiative, CIISI-EU*) orientée vers le marché et a mis les projets de cette initiative à disposition de toute personne souhaitant mettre en place et développer une telle initiative ([12]).

1.5 La BCE soutient la coopération entre les autorités compétentes aux fins du règlement proposé, les autorités européennes de surveillance (AES) et les équipes d'intervention en cas d'incidents de sécurité informatique (CSIRTS) ([13]). L'échange d'informations est essentiel pour garantir la résilience opérationnelle de l'Union étant donné que le partage d'informations et la coopération entre les autorités peut contribuer à prévenir les cyberattaques et aider à réduire la propagation des menaces informatiques. Il convient de promouvoir une compréhension commune des risques informatiques et d'assurer une évaluation cohérente de ces risques dans l'ensemble de l'Union. Il est de la plus haute importance que les informations ne soient partagées avec le point de contact unique ([14]) par les autorités compétentes et les CSIRT nationales ([15]) que lorsqu'il existe des mécanismes de classification et d'échange d'informations clairement établis et assortis de garanties de confidentialité adéquates.

1.6 Enfin, la BCE accueillerait favorablement l'introduction, dans le cadre du règlement proposé, de règles relatives aux données à caractère personnel et à la conservation des données. Il conviendrait que la durée de la période de conservation tienne compte des enquêtes, inspections, demandes d'informations, communications, publications, évaluations, vérifications, examens et conceptions de plans de surveillance ou de contrôle que les autorités compétentes pourraient être amenées à effectuer dans le cadre des obligations et des missions respectives que le règlement proposé prévoit à leur égard. Une période de rétention de 15 ans serait adéquate en la matière. Cette durée de conservation des données pourrait être

([6]) Voir l'article 3, paragraphe 15, du règlement proposé.
([7]) Voir l'article 31, paragraphe 1, point d), du règlement proposé.
([8]) Voir l'article 15, paragraphe 3, de la directive SRI.
([9]) COM(2020) 823 final.
([10]) Événements qui auraient potentiellement pu causer des dommages, mais dont la réalisation totale a pu être empêchée ; voir le considérant 39 de la directive SIR2.
([11]) Voir l'article 11 de la directive SIR2.
([12]) L'initiative pour le partage des cyber-informations et des cyber-renseignements (CIISI-EU) est disponible sur le site internet de la BCE www.ecb.europa.eu.
([13]) Voir l'article 42 du règlement proposé.
([14]) Voir l'article 8, paragraphe 3, de la directive SRI.
([15]) Voir aussi les articles 26 et 27 de la directive SRI2.

raccourcie ou prolongée selon les besoins particuliers. À cet égard, la BCE suggère que les organes législatifs de l'Union, dans la rédaction des dispositions pertinentes relatives aux données à caractère personnel et à la conservation des données, tiennent également compte du principe de minimisation des données, ainsi que du traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ([16]).

2. **Observations spécifiques concernant la surveillance ainsi que la compensation et le règlement de titres**

2.1 *Compétences dans le domaine de la surveillance du SEBC et de l'Eurosystème*

2.1.1 En lien étroit avec les missions fondamentales de politique monétaire de l'Eurosystème, le traité et les statuts du Système européen de banques centrales et de la Banque centrale européenne (ci-après les « statuts du SEBC ») prévoient que l'Eurosystème assure la surveillance des systèmes de compensation et de paiement. Conformément à l'article 127, paragraphe 2, quatrième tiret, du traité, qui se retrouve à l'article 3, paragraphe 1, des statuts du SEBC, l'une des missions fondamentales du SEBC consiste à promouvoir le bon fonctionnement des systèmes de paiement. Dans l'exécution de cette mission fondamentale, « [l]a BCE et les banques centrales nationales peuvent accorder des facilités, et la BCE peut arrêter des règlements, en vue d'assurer l'efficacité et la solidité des systèmes de compensation et de paiements au sein de l'Union et avec les pays tiers » ([17]). En vertu de son rôle de surveillance, la BCE a adopté le règlement (UE) n° 795/2014 de la Banque centrale européenne (BCE/2014/28) (ci-après le « règlement SIPS ») ([18]). Le règlement SIPS met en œuvre, sous forme prescriptive, les principes pour les infrastructures de marchés financiers publiés par le Comité sur les systèmes de paiement et de règlement (CSPR) et l'Organisation internationale des commissions de valeurs (OICV) ([19]) qui sont juridiquement contraignants et couvrent à la fois les systèmes de paiement de montant élevé et les systèmes de paiement de faible montant, d'importance systémique, gérés soit par une banque centrale de l'Eurosystème, soit par une entité privée. Le cadre de surveillance de l'Eurosystème ([20]) mentionne les instruments de paiement comme « faisant partie intégrante des systèmes de paiement » et les inclut donc dans le champ de sa surveillance. Le cadre de surveillance des instruments de paiement est en cours de révision ([21]). Selon ce cadre, un instrument de paiement (par exemple, une carte, un virement, un prélèvement, un virement électronique ou un jeton de paiement numérique ([22])) est défini comme un dispositif (ou un ensemble de dispositifs) personnalisé(s) et/ou un ensemble de procédures convenu entre l'utilisateur de services de paiement et le prestataire de services de paiement qui est utilisé pour initier un transfert de valeur ([23]).

2.1.2 Compte tenu de ce qui précède, la BCE est favorable à ce que les opérateurs de système définis à l'article 2, point p), de la directive 98/26/EC du Parlement européen et du Conseil ([24]), ainsi que les systèmes de paiement (y compris ceux gérés par les banques centrales), les schémas de paiement et les dispositifs de paiement soient exclus de l'article relatif au champ d'application du règlement proposé eu égard à l'application des cadres de

([16]) Voir les articles 4, point b), et 13, du 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).

([17]) Voir l'article 22 des statuts du SEBC.

([18]) Règlement (UE) n° 795/2014 de la Banque centrale européenne du 3 juillet 2014 concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique (BCE/2014/28) (JO L 217 du 23.7.2014, p. 16).

([19]) Disponibles sur le site internet de la Banque des règlements internationaux à l'adresse suivante : www.bis.org.

([20]) Cadre de surveillance de l'Eurosystème, version révisée (juillet 2016), disponible sur le site internet de la BCE à l'adresse suivante : www.ecb.europa.eu.

([21]) Voir le cadre de surveillance de l'Eurosystème révisé et consolidé pour les instruments, systèmes et dispositifs de paiement électronique (cadre PISA), disponible sur le site internet de la BCE à l'adresse suivante : www.ecb.europa.eu.

([22]) Un jeton de paiement numérique est une représentation numérique de valeur adossée à des créances ou des actifs enregistrés ailleurs et permettant un transfert de valeur entre utilisateurs finaux. Selon la conception qui les sous-tend, les jetons de paiement numériques peuvent prévoir un transfert de valeur sans faire nécessairement intervenir un tiers central ou utiliser des comptes de paiement.

([23]) On entend par « transfert de valeur », un « acte, initié par le payeur (ou pour son compte) ou par le bénéficiaire, consistant à transférer des fonds ou des jetons de paiement numériques, ou à placer ou retirer des espèces sur/depuis un compte d'utilisateur, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire. Le transfert peut concerner un ou plusieurs prestataires de services de paiement. » Cette définition du terme « transfert de valeur » conformément au cadre PISA s'écarte de la définition d'un « transfert de fonds » au sens de la directive (EU) 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). Un « transfert de valeur » dans le contexte d'un « instrument de paiement », tel que défini dans cette directive, ne peut faire référence qu'à un transfert de « fonds ». Conformément à ladite directive, les « fonds » n'incluent pas les jetons de paiement numériques, à moins qu'ils ne puissent être classés comme monnaie électronique (ou, moins vraisemblablement, comme monnaie scripturale).

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

surveillance susmentionnés. Pour ces raisons, les compétences du SEBC en vertu du traité et celles de l'Eurosystème en vertu du règlement SIPS devraient être clairement précisées dans les considérants du règlement proposé.

2.1.3 De même, la BCE est favorable à ce que les tiers prestataires de services informatiques qui sont soumis à des cadres de surveillance établis en vue de soutenir les missions visées à l'article 127, paragraphe 2, du traité sur le fonctionnement de l'Union européenne soient exclus de l'application du cadre de supervision comme prévu dans le règlement proposé ([25]). À cet égard, la BCE tient à souligner que les banques centrales du SEBC agissant dans le cadre de leurs capacités monétaires ([26]) et de l'Eurosystème, lorsqu'elles fournissent des services via TARGET2, TARGET2-Titres (T2S) ([27]) et le règlement des paiements instantanés TARGET (TIPS) ([28]), ne sont pas concernées par l'article relatif au champ d'application du règlement proposé et ne peuvent pas non plus être considérées comme des tiers prestataires de services informatiques, ce qui fait qu'elles sont susceptibles d'être considérées comme des tiers prestataires critiques de services informatiques aux fins du règlement proposé. L'Eurosystème assure la supervision de T2S dans le cadre de son mandat consistant à garantir l'efficacité et la solidité des systèmes de compensation et de paiement. En outre, l'AEMF a précisé que T2S n'est pas un prestataire critique de services ([29])au sens du règlement (UE) n° 909/2014 du Parlement européen et du Conseil ([30]) (ci-après le « règlement DCT »). Par conséquent, la sécurité, l'efficacité et la résilience organisationnelles et opérationnelles de T2S sont garanties par le cadre juridique, réglementaire et opérationnel applicable ainsi que par les dispositifs de gouvernance de T2S, par opposition au règlement DCT.

2.1.4 En outre, le cadre de surveillance de l'Eurosystème ([31]) couvre les prestataires de services essentiels tels que la Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT est une société coopérative à responsabilité limitée établie en Belgique qui fournit des services de messagerie sécurisée à l'international. La Banque nationale de Belgique agit en qualité de superviseur principal de SWIFT et assure la surveillance de SWIFT, sur la base d'un dispositif de surveillance coopérative, en coopération avec les autres banques centrales du G10, y compris la BCE. Les superviseurs du G10 reconnaissent que la supervision vise principalement le risque opérationnel de SWIFT étant donné qu'il s'agit de la principale catégorie de risque au titre de laquelle SWIFT pourrait présenter un risque systémique pour le système financier de l'Union. À cet égard, le groupe de surveillance de SWIFT (*SWIFT Cooperative Oversight*) a élaboré un ensemble spécifique de principes et de préconisations de haut niveau applicables à SWIFT, notamment en matière d'identification et de gestion des risques, de sécurité de l'information, de fiabilité et résilience, de planification technologique et de communication avec les utilisateurs. Les superviseurs du G10 attendent de SWIFT qu'elle adhère aux lignes directrices concernant la cyberrésilience du Comité sur les paiements et les infrastructures de marché (CPIM) et de l'OICV ([32]), ainsi qu'à d'autres normes internationales en matière de sécurité informatique qui, prises ensemble, sont plus exigeantes que les obligations énoncées dans le règlement proposé.

2.1.5 Il est impossible d'avoir la certitude que SWIFT et d'éventuels autres prestataires de services soumis au cadre de surveillance de l'Eurosystème soient soumis au règlement proposé en tant que tiers prestataires de services informatiques s'ils venaient à fournir des services non couverts par l'article 127, paragraphe 2, du traité. Par conséquent, la BCE est résolument favorable à l'exclusion des prestataires de services déjà soumis au cadre de surveillance de l'Eurosystème, et notamment mais pas exclusivement de SWIFT, du champ d'application du cadre de supervision prévu dans le règlement proposé.

([25]) Voir l'article 28, paragraphe 5, du règlement proposé.

([26]) Voir le point 1.3 de l'avis de la Banque centrale européenne du 19 février 2021 sur une proposition de règlement sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937 (CON/2021/4). Tous les avis de la BCE sont publiés sur EUR-Lex.

([27]) Voir l'annexe IIa de l'orientation de la Banque centrale européenne du 5 décembre 2012 relative au système de transferts express automatisés transeuropéens à règlement brut en temps réel (TARGET2) (BCE/2012/27) (JO L 30 du 30.1.2013, p. 1). Orientation de la Banque centrale européenne du 18 juillet 2012 relative à TARGET2-Titres (BCE/2012/13) (JO L 215 du 11.8.2012, p. 19) ; et décision de la Banque centrale européenne du 16 novembre 2011 établissant les règles et procédures détaillées pour la mise en œuvre des critères d'accès des dépositaires centraux de titres aux services TARGET2-Titres (BCE/2011/20) (JO L 319 du 2.12.2011, p. 117). Voir également l'accord-cadre T2S et la convention collective.

([28]) Voir l'annexe IIb de l'orientation BCE/2012/27.

([29]) Voir l'article 30, paragraphe 5, du 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), et l'article 68 du règlement délégué (UE) 2017/392 de la Commission du 11 novembre 2016 complétant le règlement (UE) n° 909/2014 du Parlement européen et du Conseil par des normes techniques de réglementation sur les exigences opérationnelles, d'agrément et de surveillance applicables aux dépositaires centraux de titres (JO L 65 du 10.3.2017, p. 48).

([30]) 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).

([31]) Cadre de surveillance de l'Eurosystème, version révisée (juillet 2016), disponible sur le site internet de la BCE à l'adresse suivante : www.ecb.europa.eu.

([32]) Disponibles sur le site internet de la Banque des règlements internationaux à l'adresse suivante : www.bis.org.

2.2 *Compétences du SEBC dans le domaine du règlement des opérations sur titres*

2.2.1 Les dépositaires centraux de titres (DCT) sont des infrastructures de marché financier (IMF) strictement réglementées et surveillées par différentes autorités en vertu du règlement DCT, lequel établit des exigences en matière de règlement des instruments financiers ainsi que des règles relatives à l'organisation et à la conduite des DCT. Il convient par ailleurs que les DCT prennent en compte les lignes directrices concernant la cyberrésilience du CPIM et de l'OICV, lesquelles sont devenues opérationnelles dans le cadre des attentes en matière de surveillance de la cyberrésilience destinées aux infrastructures de marché financier (*Cyber resilience oversight expectations for financial market infrastructures*) (décembre 2018) ([33]). Outre les compétences de surveillance confiées aux autorités compétentes nationales (ACN) en vertu du règlement DCT, les membres du SEBC agissent en tant qu'« autorités concernées », en leur qualité d'autorités de surveillance des systèmes de règlement de titres exploités par les DCT, de banques centrales émettant les monnaies les plus pertinentes dans lesquelles le règlement est effectué et de banques centrales dans les livres desquelles le volet « espèces » des opérations est réglé ([34]). À cet égard, le considérant 8 du règlement DCT dispose que celui-ci s'applique sans préjudice des compétences de la BCE et des banques centrales nationales pour assurer l'efficacité et la solidité des systèmes de compensation et de paiement au sein de l'Union et d'autres pays. Le considérant 8 précise également que le règlement DCT ne devrait pas empêcher les membres du SEBC d'avoir accès aux informations utiles pour l'exercice de leurs missions ([35]), y compris pour ce qui est de la surveillance des DCT et d'autres IMF ([36]).

2.2.2 En outre, les membres du SEBC font souvent office d'agents de règlement pour le volet « espèces » des opérations sur titres et l'Eurosystème propose des services de règlement à travers T2S pour les DCT. La surveillance par l'Eurosystème de T2S relève de son mandat consistant à garantir l'efficacité et la solidité des systèmes de compensation et de paiement, tandis que les autorités compétentes et les autorités concernées des DCT s'efforcent d'assurer leur bon fonctionnement ainsi que la sécurité et l'efficacité du règlement et le bon fonctionnement des marchés financiers sur leurs territoires respectifs.

2.2.3 En vertu du règlement proposé ([37]), les banques centrales du SEBC ne participent pas à l'élaboration des normes techniques en ce qui concerne la spécification des risques informatiques. De même, en vertu du règlement proposé ([38]), les autorités compétentes ne sont aucunement informées des incidents informatiques. La banque centrale du SEBC devrait conserver le même niveau de participation que celui actuellement prévu par le règlement DCT et les autorités concernées devraient être informées des incidents informatiques. L'Eurosystème est l'autorité compétente pour tous les DCT de la zone euro et pour certains autres DCT de l'UE. Les banques centrales du SEBC auraient besoin d'être informées des incidents informatiques pertinents vis-à-vis de l'exécution de leurs missions, y compris en ce qui concerne la surveillance des DCT et des autres IMF. Les risques auxquels les DCT sont exposés, y compris les risques informatiques, sont susceptibles de menacer leur bon fonctionnement. Les risques informatiques sont donc importants pour les autorités compétentes et celles-ci devraient disposer d'une vue d'ensemble complète et détaillée de ces risques afin de les évaluer et d'influencer l'approche de gestion des risques des DCT. S'agissant des risques informatiques, le règlement proposé ne devrait pas prévoir d'exigences moins strictes que celles prévues par le règlement DCT et les normes techniques de réglementation en vigueur.

2.2.4 En outre, les organes législatifs de l'Union devraient clarifier l'interaction entre le règlement proposé ([39]) et les normes techniques de réglementation complétant le règlement DCT. En particulier, il n'est pas certain qu'un DCT doive être exempté de l'obligation d'avoir son propre site secondaire lorsque son fournisseur de services informatiques tiers maintien un tel site ([40]). À supposer qu'un DCT soit exempté de cette obligation de maintien d'un site secondaire, la valeur juridique de l'exigence en question reste floue. De la même manière, le règlement

([33]) Disponibles sur le site internet de la BCE à l'adresse suivante : www.ecb.europa.eu.

([34]) Voir l'article 12 du règlement (UE) n° 909/2014.

([35]) Voir également l'article 13, l'article 17, paragraphe 4, et l'article 22, paragraphe 6, du règlement (UE) n° 909/2014.

([36]) Voir le point 7.3 de l'avis de la BCE du 6 avril 2017 sur l'identification des infrastructures critiques aux fins de la sécurité informatique (CON/2017/10) ; le point 7.2 de l'avis de la BCE du 8 novembre 2018 sur la désignation des services essentiels et des opérateurs de services essentiels aux fins de la sécurité des réseaux et des systèmes d'information (CON/2018/47) ; le point 3.5.2 de l'avis de la BCE du 2 mai 2019 sur la sécurité des réseaux et des systèmes d'information (CON/2019/17) ; et le point 3.5.2 de l'avis de la BCE du 11 novembre 2019 sur la sécurité des réseaux et des systèmes d'information (CON/2019/38) .

([37]) Voir l'article 54, paragraphe 5, du règlement proposé et l'article 45, paragraphe 7, du règlement (UE) n° 909/2014.

([38]) Voir l'article 54, paragraphe 4, du règlement proposé et l'article 45, paragraphe 6, du règlement (UE) n° 909/2014.

([39]) Voir l'article 11, paragraphe 5, du règlement proposé.

([40]) Voir l'article 78, paragraphe 3, du règlement délégué (UE) n° 2017/392 de la Commission du 11 novembre 2016 complétant le règlement (UE) no 909/2014 du Parlement européen et du Conseil par des normes techniques de réglementation sur les exigences opérationnelles, d'agrément et de surveillance applicables aux dépositaires centraux de titres (JO L 65 du 10.3.2017, p. 48).

proposé ([41]) fait référence à un objectif en matière de délai et à des objectifs en matière de point de rétablissement pour chaque fonction ([42]) tandis que la norme technique de réglementation pertinente opère une distinction entre les fonctions critiques ([43]) et les opérations critiques ([44]) en lien avec le délai de rétablissement déterminé pour les opérations critiques des DCT. Il convient que les organes législatifs de l'Union approfondissent leur réflexion et apportent des éclaircissements supplémentaires en rapport avec l'interaction entre le règlement proposé et les normes techniques de réglementation complétant le règlement DCT afin d'éviter le risque d'exigences contradictoires. Enfin, il convient de préciser que les dérogations accordées aux DCT exploités par certaines entités publiques en vertu du règlement DCT ([45]) sont étendues en vertu du règlement proposé.

2.3 *Compétences du SEBC dans le domaine de la compensation de titres*

2.3.1 Les banques centrales du SEBC sont investies de compétences de surveillance relatives aux contreparties centrales. À cet égard, les banques centrales nationales de l'Eurosystème coopèrent souvent avec les autorités compétentes nationales concernées dans le cadre des fonctions de surveillance et de supervision des contreparties centrales et participent au collège des contreparties centrales correspondant établi en vertu du règlement (UE) n° 648/2012 du Parlement européen et du Conseil ([46]) (ci-après le « règlement EMIR »). Les membres concernés de l'Eurosystème ([47]) font partie des collèges EMIR au titre de leur fonction de surveillance et représentent l'Eurosystème en tant que banque centrale d'émission pour les contreparties centrales dont l'euro est l'une des monnaies les plus pertinentes pour les instruments financiers compensés (et pour les contreparties centrales extraterritoriales compensant une part importante des instruments financiers en euros). La BCE est la banque centrale d'émission pour les contreparties centrales n'appartenant pas à la zone euro.

2.3.2 En vertu du règlement proposé ([48]), les banques centrales du SEBC ne participent pas à l'élaboration de normes techniques en ce qui concerne la spécification des risques informatiques. En outre, dans le règlement proposé ([49]), il manque une référence aux exigences concernant l'objectif de délai de rétablissement et l'objectif de point de rétablissement conformément au règlement EMIR ([50]). Le cadre réglementaire proposé ne devrait pas prévoir d'exigences relatives aux risques informatiques qui seraient moins strictes que celles en vigueur. Il est donc essentiel de fixer des objectifs clairs concernant les délais et points de rétablissement pour disposer d'un cadre solide de gestion de la continuité des activités. Le maintien d'objectifs spécifiques en matière de délais et de points de rétablissement fait également partie des principes du CPIL-OICV pour les infrastructures de marchés financiers ([51]). Il convient de conserver les dispositions en vigueur conformément au règlement EMIR et d'adapter le règlement proposé en conséquence. Les banques centrales du SEBC devraient être associées à l'élaboration de toute législation dérivée ainsi qu'à la clarification et à la réflexion à effectuer par les organes législatifs de l'Union concernant l'interaction entre le règlement proposé et les normes techniques de réglementation complémentaires, de manière à éviter le risque d'exigences contradictoires ou redondantes.

3. **Observations spécifiques sur les aspects liés à la surveillance prudentielle**

3.1 Le règlement (UE) n° 1024/2013 ([52]) du Conseil confie à la BCE des missions spécifiques en matière de surveillance prudentielle des établissements de crédit au sein de la zone euro et la charge également de veiller au fonctionnement efficace et cohérent du mécanisme de surveillance unique (MSU) au sein duquel des responsabilités spécifiques de surveillance sont réparties entre la BCE et les ACN participantes. En particulier, la BCE a pour mission d'accorder et de retirer des agréments à l'ensemble des établissements de crédit. La BCE a également pour mission, entre autres, de veiller au respect des dispositions législatives pertinentes de l'Union imposant des exigences prudentielles aux établissements de crédit, y compris l'obligation de disposer de dispositifs solides en matière de gouvernance, tels que des processus de gestion des risques et des mécanismes de contrôle interne fiables ([53]). À cette

([41]) Voir l'article 11, paragraphe 6, du règlement proposé.
([42]) Voir l'article 3, paragraphe 17, du règlement proposé.
([43]) Voir l'article 76, paragraphe 2, points d) et e), du règlement délégué (UE) n° 2017/392 de la Commission.
([44]) Voir l'article 78, paragraphes 2 et 3, du règlement délégué (UE) n° 2017/392 de la Commission.
([45]) Voir l'article 1, paragraphe 4, du règlement (UE) n° 909/2014.
([46]) 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).
([47]) Voir l'article 18, paragraphe 2, points g) et h), du règlement EMIR.
([48]) Voir l'article 53, paragraphe 2, point b), et paragraphe 3), du règlement proposé, et l'article 34, paragraphe 3, du règlement EMIR.
([49]) Voir l'article 53, paragraphe 2, point a), du règlement proposé.
([50]) Voir l'article 34 du règlement EMIR.
([51]) Voir les principes du CPIL-OICV pour les infrastructures de marchés financiers disponibles sur le site internet de la Banque des règlements internationaux : www.bis.org.
([52]) Règlement (UE) nº 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit (JO L 287 du 29.10.2013, p. 63).
([53]) Voir l'article 4, paragraphe 1, point e), et l'article 6, paragraphe 4, du règlement (UE) n° 1024/2013.

fin, la BCE dispose de tous les pouvoirs de surveillance pour intervenir dans l'activité des établissements de crédit qui sont nécessaires à l'exercice de ses fonctions. La BCE et les ACN concernées sont donc les autorités compétentes qui exercent des pouvoirs de surveillance prudentielle spécifiques en vertu du règlement 2013/575/UE du Parlement européen et du Conseil ([54]) (ci-après le « règlement sur les exigences de fonds propres ») et de la directive n° 2013/36/UE du Parlement européen et du Conseil ([55]) (ci-après la « directive sur les exigences de fonds propres »).

3.2 Le règlement proposé prévoit que le corpus réglementaire unique et le système de surveillance devraient continuer à être développés pour couvrir la résilience opérationnelle numérique et la sécurité informatique au moyen de l'élargissement des mandats des autorités de surveillance financière chargées de surveiller et de protéger la stabilité financière et l'intégrité du marché ([56]). L'objectif est de promouvoir un cadre exhaustif applicable aux risques informatiques ou opérationnels à travers l'harmonisation des exigences clés en matière de résilience opérationnelle numérique pour toutes les entités financières ([57]). En particulier, le règlement proposé vise à consolider et à mettre à niveau les exigences en matière de risques informatiques qui sont, jusqu'à présent, scindées dans différents actes législatifs ([58])

3.3 Les exigences liées au risque informatique pour le secteur financier sont actuellement réparties dans un certain nombre d'actes législatifs de l'Union, notamment la directive sur les exigences de fonds propres, et d'instruments juridiques non contraignants (tels que les orientations de l'ABE), qui s'avèrent inégaux et parfois incomplets. Dans certains cas, le risque informatique n'a été traité que de manière implicite, dans le cadre du risque opérationnel, tandis que dans d'autres, il n'a pas été traité du tout. Il convient d'y remédier en procédant à un alignement entre le règlement proposé et ces actes. À cette fin, la directive modificative proposée prévoit une série de modifications qui semblent nécessaires pour apporter une clarté et une cohérence juridiques eu égard à l'application des différentes exigences en matière de résilience opérationnelle numérique. Toutefois, les modifications de la directive sur les exigences de fonds propres actuellement suggérées par la directive modificative proposée ([59]) ne concernent que les dispositions relatives aux plans d'urgence et de poursuite de l'activité ([60]), étant donné que celles-ci sont implicitement censées servir de base à la gestion des risques informatiques.

3.4 En outre, le règlement proposé ([61]) prévoit que les entités financières, y compris les établissements de crédit, disposent de cadres de gouvernance et de contrôle internes qui garantissent une gestion efficace et prudente de tous les risques informatiques. Le règlement proposé ([62]) prévoit l'application, au niveau individuel et consolidé, des exigences qui y sont énoncées, mais sans coordination suffisante avec la législation sectorielle concernée. Enfin, le règlement proposé ([63]) prévoit que, sans préjudice des dispositions relatives au cadre de supervision des tiers prestataires critiques de services informatiques visés dans le règlement proposé ([64]), le respect des obligations énoncées dans celui-ci est assuré, pour les établissements de crédit, par les autorités compétentes désignées conformément à l'article 4 de la directive sur les exigences de fonds propres, sans préjudice des missions spécifiques confiées à la BCE par le règlement MSU.

3.5 Compte tenu de ce qui précède, la BCE comprend que, en ce qui concerne les établissements de crédit, et à l'exception des dispositions du règlement proposé relatives au cadre de supervision applicable aux tiers prestataires critiques de services informatiques ([65]), le règlement proposé vise à établir un cadre général de gouvernance interne pour la gestion du risque informatique qui sera intégré dans le cadre de gouvernance interne générale conformément à la directive sur les exigences de fonds propres. En outre, compte tenu de la nature prudentielle du cadre proposé, les autorités compétentes chargées de la surveillance du respect des obligations énoncées dans le cadre proposé, y compris la BCE, seront celles chargées de la surveillance bancaire conformément au règlement MSU.

([54]) 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 aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1).

([55]) 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 et des entreprises d'investissement, 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).

([56]) Voir le considérant 8 du règlement proposé.

([57]) Voir le considérant 11 du règlement proposé.

([58]) Voir le considérant 12 du règlement proposé.

([59]) Voir les considérants 4 et 5 de la directive modificative proposée.

([60]) Voir l'article 85 de la directive concernant les exigences de fonds propres.

([61]) Voir l'article 4, paragraphe 1, du règlement proposé.

([62]) Voir l'article 25, paragraphes 3 et 4, du règlement proposé.

([63]) Voir l'article 41 du règlement proposé.

([64]) Voir la section II du chapitre V du règlement proposé.

([65]) Voir la section II du chapitre V du règlement proposé.

3.6 Les organes législatifs de l'Union pourraient donc souhaiter prendre en considération les suggestions suivantes pour accroître la clarté et la coordination entre le règlement proposé et la directive sur les exigences de fonds propres. Premièrement, les exigences prévues par le règlement proposé peuvent être expressément qualifiées de prudentielles, comme cela est déjà le cas, entre autres, dans le règlement DCT ([66]). Deuxièmement, les considérants de la directive modificative proposée ([67]) pourraient donner lieu à une formulation plus large étant donné que les exigences du règlement proposé vont au-delà de la seule phase des plans d'urgence et de poursuite de l'activité. Les mesures de gouvernance des risques informatiques relèvent, dans l'ensemble, du champ d'application plus général des dispositifs solides de gouvernance prévus à l'article 74 de la directive sur les exigences de fonds propres ([68]). Troisièmement, le règlement proposé ([69]) devrait être modifié de manière à rappeler, dans ses considérants, la compétence de la BCE en matière de surveillance prudentielle des établissements de crédit en vertu du traité et du règlement MSU. Quatrièmement, la référence à l'application au niveau individuel et consolidé des exigences qu'il contient ([70]) devrait être revue étant donné que les niveaux sous-consolidés et consolidés ne sont pas définis dans le règlement proposé et que certains types d'intermédiaires ne font pas l'objet d'une surveillance consolidée en vertu de la législation applicable (par exemple, les établissements de paiement). En outre, le niveau d'application des exigences prévues par le règlement proposé ne devrait résulter que de la législation applicable à chaque type d'entité financière. Dans le cas des établissements de crédit, un lien clair est prévu entre la directive sur les exigences de fonds propres et le règlement proposé, si bien que les exigences prévues par le règlement proposé s'appliqueraient automatiquement au niveau individuel, sous-consolidé ou consolidé ([71]), selon le cas. Enfin, les organes législatifs de l'Union pourraient envisager d'établir un régime transitoire pour gérer la période comprise entre l'entrée en vigueur du règlement proposé et celle des normes techniques de réglementation prévues dans le règlement proposé, étant donné que certains intermédiaires, y compris les établissements de crédit, sont déjà soumis à des règles en matière de risques informatiques qui s'appliquent à des secteurs spécifiques et sont plus détaillées que les dispositions générales du règlement proposé.

3.7 Conformément au règlement MSU, la BCE a été investie de la mission de veiller au respect, par les établissements de crédit, des exigences du droit de l'Union exigeant de ceux-ci qu'ils disposent de processus solides de gestion des risques et de mécanismes de contrôle interne ([72]). Cela signifie que la BCE doit veiller à ce que les établissements de crédit mettent en œuvre des politiques et processus pour évaluer et gérer leur exposition au risque opérationnel, y compris au risque de modèle, et pour couvrir les événements à faible fréquence mais à fort impact. Il est exigé des établissements qu'ils précisent, aux fins de ces politiques et procédures, ce qui constitue un risque opérationnel ([73]).

3.8 En juillet 2017, le conseil des gouverneurs de la Banque centrale européenne (BCE) a adopté le dispositif de déclaration des cyberincidents du MSU (*SSM Cyber Incident Reporting Framework*) (ci-après le « dispositif de déclaration »), sur la base d'un projet de proposition du conseil de surveillance prudentielle, conformément à l'article 26, paragraphe 8, et l'article 6, paragraphe 2, du règlement MSU, et à l'article 21, paragraphe 1, du règlement (UE) n° 468/2014 de la Banque centrale européenne (ECB/2014/17) ([74]). Le dispositif de déclaration consiste en une demande contraignante (décisions individuelles adressées aux établissements de crédit) d'information ou de déclaration sur la base de l'article 10 du règlement MSU ([75]). Certains pays ont déjà mis en place un processus de notification des incidents au titre duquel les établissements de crédit doivent signaler tous les incidents informatiques importants à leurs ACN. Dans ces pays, les établissements de crédit importants continueront à signaler les incidents aux ACN, lesquelles en feront part à la BCE, dans les meilleurs délais, pour le

([66]) Voir le titre du chapitre II, section 4, « Exigences prudentielles », du règlement DCT.

([67]) Voir le considérant 4 de la directive modificative proposée.

([68]) L'article 85 de la directive 2013/36/UE est une simple spécification. À cet égard, voir également les pages 4, 11 et 37 des orientations de l'Autorité bancaire européenne sur la gestion des risques liés aux TIC et à la sécurité du 29 novembre 2019 (ci-après les « orientations de l'ABE »), dont la base juridique générale figure expressément à l'article 74 de la directive 2013/36/UE.

([69]) Voir l'article 41, paragraphe 1, du règlement proposé.

([70]) Voir l'article 25, paragraphes 3 et 4, du règlement proposé.

([71]) Voir également l'article 109 de la directive concernant les exigences de fonds propres.

([72]) Voir l'article 4, paragraphe 1, point e), du règlement MSU.

([73]) Voir l'article 85 de la directive concernant les exigences de fonds propres.

([74]) Règlement (UE) n° 468/2014 de la Banque centrale européenne du 16 avril 2014 établissant le cadre de la coopération au sein du mécanisme de surveillance unique entre la Banque centrale européenne, les autorités compétentes nationales et les autorités désignées nationales (le « règlement-cadre MSU ») (BCE/2014/17) (JO L 141 du 14.5.2014, p. 1).

([75]) En particulier, un cyberincident (à savoir une éventuelle violation identifiée de la sécurité de l'information, qu'elle soit malveillante ou accidentelle) doit être notifié à la BCE si au moins une des conditions suivantes est remplie : 1) l'impact financier potentiel est de 5 millions d'EUR ou représente 0,1 % des fonds propres de base de catégorie 1 ; 2) l'incident est signalé publiquement ou porte atteinte à une réputation ; 3) l'incident a été remonté au directeur des systèmes d'information en dehors des notifications régulières ; 4) la banque a notifié l'incident au CERT/CSIRT, à une agence de sécurité ou à la police ; 5) des procédures de rétablissement après sinistre ou de poursuite de l'activité ont été déclenchées ou une réclamation de cyberassurance a été déposée ; 6) il y a eu une violation des exigences légales ou réglementaires ; 7) la banque utilise des critères internes et des avis d'experts (y compris concernant l'effet systémique potentiel) et décide d'en informer la BCE.

compte des entités soumises à la surveillance prudentielle. Par conséquent, les décisions susmentionnées concernent également ces ACN qui doivent transmettre les informations en question à la BCE conformément au dispositif de déclaration. La BCE soutient les efforts déployés par les organes législatifs de l'Union pour promouvoir l'harmonisation et la rationalisation, notamment en ce qui concerne l'ensemble des règles et obligations applicables aux établissements de crédit en matière de notification des incidents. Compte tenu de ce qui précède, la BCE est disposée à modifier (et éventuellement à abroger) le dispositif de déclaration, le cas échéant, en vue de l'adoption éventuelle du règlement proposé.

4. **Observations spécifiques concernant la gestion du risque informatique, la notification des incidents, les tests de résilience opérationnelle et les risques liés aux tiers prestataires de services informatiques**

4.1 *Gestion des risques informatiques*

4.1.1 La BCE se félicite de l'introduction par le règlement proposé d'un cadre solide et complet de gestion des risques informatiques qui englobe les lignes directrices concernant la cyberrésilience du CPIM et de l'OICV et est en étroite conformité avec les meilleures pratiques, y compris avec les attentes en matière de surveillance de la cyberrésilience de l'Eurosystème (*Eurosystem Cyber Resilience Oversight Expectations*) concernant les IMF.

4.1.2 La BCE soutient l'idée selon laquelle les entités financières devraient procéder à des évaluations des risques lors de chaque « modification majeure » de l'infrastructure du réseau et du système d'information ([76]). Cela étant, le règlement proposé ne contient aucune définition de la notion de « modification majeure », ce qui laisse place à des interprétations divergentes par les entités financières et pourrait in fine faire obstacle aux objectifs d'harmonisation du règlement proposé. Dans un souci de sécurité juridique, les organes législatifs de l'Union pourraient envisager d'introduire une définition de la notion de « modification majeure » dans le règlement proposé.

4.1.3 De manière générale, la BCE soutient l'idée de la notification aux autorités compétentes, par les entités financières autres que les microentreprises, des coûts et pertes pertinents causés par les perturbations et incidents informatiques ([77]). Toutefois, pour garantir l'efficacité globale du système et écarter le risque que les autorités compétentes et les entités financières soient débordées par un nombre excessif de notifications, la piste de l'introduction de seuils pertinents, probablement de nature quantitative, mériterait d'être explorée par les organes législatifs de l'Union.

4.1.4 La BCE reconnaît la possibilité pour les entités financières de déléguer à des entreprises intragroupe ou externes les tâches de vérification du respect des exigences en matière de gestion des risques informatiques après approbation par les autorités compétentes ([78]). Dans le même temps, il importe que les organes législatifs de l'Union précisent les modalités d'octroi de l'approbation par les autorités compétentes dans le cas où une entité financière est soumise à plusieurs autorités compétentes. Cette situation pourrait se produire lorsqu'une entité financière est un établissement de crédit, un prestataire de services sur crypto-actifs ou un prestataire de services de paiement. Enfin, en ce qui concerne l'identification et la classification à effectuer par les entités financières conformément au règlement proposé ([79]), la BCE considère qu'il serait prudent, aux fins de la classification des actifs, que le règlement proposé leur impose également de tenir compte du caractère critique de ces actifs (déterminé en fonction des fonctions critiques ou non de ces actifs).

4.2 *Notification des incidents*

4.2.1 La BCE se félicite des efforts déployés dans le règlement proposé pour harmoniser le paysage en ce qui concerne la notification des incidents informatiques au sein de l'Union et œuvrer à une notification centralisée des incidents informatiques majeurs ([80]). L'introduction d'un cadre harmonisé de notification des incidents informatiques majeurs ([81]) aux autorités compétentes concernées permettrait, en principe, de rationaliser et d'harmoniser la charge de déclaration incombant aux entités financières, y compris les établissements de crédit. Les autorités compétentes tireraient profit du champ d'application élargi des incidents couverts, lequel s'étendrait au-delà des cyberincidents actuellement couverts par les cadres existants ([82]). L'adoption future du règlement proposé nécessiterait de revoir et, éventuellement, d'abroger les cadres existants, y compris le dispositif de déclaration des cyberincidents du MSU. Cela étant, afin de parvenir à une véritable rationalisation et à un alignement complet de tous les cadres, il est essentiel de veiller à ce que le champ d'application des dispositions relatives à la notification des incidents contenues dans le règlement proposé, y compris l'ensemble des définitions, seuils et paramètres de notification pertinents, soit

([76]) Voir l'article 7, paragraphe 3, du règlement proposé.
([77]) Voir l'article 10, paragraphe 9, du règlement proposé.
([78]) Voir l'article 5, paragraphe 10, du règlement proposé.
([79]) Voir l'article 7 du règlement proposé.
([80]) Voir l'article 19 du règlement proposé.
([81]) Voir l'article 3, paragraphe 7, et les articles 17 et 18 du règlement proposé.
([82]) Voir, par exemple, le dispositif de déclaration.

pleinement aligné sur les cadres pertinents. En particulier, il est de la plus haute importance d'assurer l'alignement entre, d'une part, le règlement proposé et, d'autre part, la directive (UE) 2015/2366 du Parlement européen et du Conseil ([83]) (ci-après la « DSP2 ») et les orientations de l'ABE sur la notification des incidents majeurs (ci-après les « orientations de l'ABE »). La directive modificative proposée ([84]) apporte des modifications à la DSP2 qui concernent la délimitation de la notification des incidents entre le règlement proposé et la DSP2, ce qui affecterait principalement les prestataires de services de paiement susceptibles d'être également agréés en tant qu'établissements de crédit, ainsi que les autorités compétentes. Le processus de notification des incidents manque de clarté et il risque d'y avoir un chevauchement entre certains des incidents nécessitant une notification au titre du règlement proposé et au titre des orientations de l'ABE.

4.2.2 Les processus de notification des incidents majeurs au titre, respectivement, du règlement proposé ([85]), de la DSP2 et des orientations correspondantes de l'ABE, obligeraient les prestataires de services de paiement à remettre un rapport d'incident à leur autorité compétente respective une fois que l'incident a donné lieu à une classification. Dans les faits, les rapports initiaux ne rendent pas compte de l'essence, de la cause ou de la zone fonctionnelle affectée par l'incident et les prestataires de services de paiement pourraient n'être en mesure d'opérer ces distinctions qu'à un stade ultérieur, lorsque des informations plus détaillées sur l'incident deviennent disponibles. Par conséquent, des rapports initiaux d'incidents pourraient être fournis à la fois au titre du règlement proposé et des orientations de l'ABE, ou les prestataires de services de paiement pourraient convenir d'un cadre de notification unique et rectifier leurs observations à une date ultérieure. La même incertitude (en ce qui concerne, par exemple, les causes profondes de tout incident) risque de se retrouver dans les rapports intermédiaires et finaux. Cela augmenterait encore la probabilité d'une fourniture parallèle de rapports aux autorités compétentes au titre du règlement proposé et au titre de la DSP2.

4.2.3 Il se peut également que certains incidents susceptibles d'être qualifiés d'incidents informatiques aient des effets dans d'autres domaines et devraient, par conséquent, être notifiés en vertu des orientations de l'ABE. Cela pourrait être le cas lorsqu'un incident a des effets sur le plan informatique tout en affectant également la prestation de services de paiement de manière directe ou d'autres domaines ou canaux fonctionnels qui ne relèvent pas du domaine informatique. Il se peut en outre qu'il y ait des cas où il n'est pas possible de faire la distinction entre les incidents opérationnels et les incidents informatiques. Par ailleurs, lorsque la même entité financière est à la fois un établissement de crédit important et un prestataire de services de paiement, celle-ci devrait, en vertu du règlement proposé, déclarer deux fois l'incident informatique étant donné qu'elle est soumise à deux autorités compétentes. Compte tenu de ce qui précède, le règlement proposé devrait préciser plus clairement comment la DSP2 et les orientations de l'ABE sont censées interagir en pratique. Plus significativement, il serait important, dans un souci d'harmonisation et de rationalisation des obligations de notification, que les organes législatifs de l'Union réfléchissent aux questions résiduelles de double notification et précisent si, d'une part, le règlement proposé, et, d'autre part, la DSP2 et les orientations de l'ABE peuvent coexister ou s'il conviendrait de prévoir un ensemble unique d'exigences en matière de notification des incidents.

4.2.4. Le règlement proposé introduit une exigence pour les autorités compétentes ([86]) au titre de laquelle ces dernières doivent, dès réception d'un rapport, en accuser réception et fournir le plus rapidement possible à l'entité financière tout retour d'information ou toute orientation nécessaire, notamment pour examiner les mesures correctives au niveau de l'entité ou les moyens de réduire au maximum les effets préjudiciables dans les différents secteurs. Cela signifierait que les autorités compétentes devraient contribuer activement à la gestion et à la résolution des incidents tout en évaluant également la réaction d'une entité soumise à la surveillance prudentielle aux incidents critiques. La BCE souligne que la responsabilité de la résolution et des conséquences d'un incident devrait exclusivement et clairement incomber à l'entité financière concernée. La BCE propose donc de limiter les retours d'information et les orientations aux seuls retours d'informations et orientations prudentiels de haut niveau. Des retours d'information plus vastes nécessiteraient des professionnels spécialisés, ayant des connaissances techniques très importantes, qui ne sont généralement pas disponibles dans la réserve des talents mis à disposition des autorités prudentielles.

4.3 *Tests de résilience opérationnelle numérique*

4.3.1 La BCE est favorable aux exigences prévues dans le règlement proposé ([87]) concernant des tests de résistance opérationnelle numérique dans toutes les entités financières et la nécessité pour chaque établissement de disposer de son propre programme de test. Le règlement proposé ([88]) décrit, à titre indicatif, différents types de tests

([83]) 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).
([84]) Voir l'article 7, paragraphe 9, de la directive modificative proposée.
([85]) Voir l'article 17, paragraphe 3, du règlement proposé.
([86]) Voir l'article 20 du règlement proposé.
([87]) Voir les articles 21 et 22 du règlement proposé.
([88]) Voir l'article 22, paragraphe 1, du règlement proposé.

s'adressant aux entités financières. Les types de tests manquent de clarté et certains tests, tels que les tests de compatibilité, les questionnaires ou les tests fondés sur des scénarios, peuvent être interprétés librement par les AES, les autorités compétentes et les entités financières. En outre, aucune orientation n'est fournie au sujet de la fréquence de chaque test. Il serait possible de retenir une approche consistant à ce que le règlement proposé définisse des exigences générales concernant les tests et soit accompagné d'une description plus précise des types de tests fournie dans les normes techniques de réglementation et d'exécution.

4.3.2 Les tests de pénétration fondés sur la menace sont un outil puissant pour tester les protections et l'état de préparation en matière de sécurité. La BCE encourage les entités financières à utiliser ce type de tests. Cet outil permet non seulement de tester les mesures techniques mais également le personnel et les processus. Les résultats de ces tests peuvent considérablement accroître la sensibilisation à la sécurité de la direction générale des entités testées. Le cadre européen de tests pour un cyberpiratage éthique fondé sur les renseignements sur les menaces (*Framework for Threat Intelligence Based Ethical Red-teaming*, TIBER-UE) ([89]), de même que d'autres outils du type « test de pénétration fondés sur la menace » qui sont déjà disponibles, en dehors de l'Union, sont des instruments essentiels pour permettre aux entités d'évaluer, de tester, de mettre en pratique et d'améliorer elles-mêmes leur position et leur défense en matière de cyberrésilience.

4.3.3 Dans la plupart des États membres où le TIBER-UE a été mis en œuvre, les superviseurs et les autorités de contrôle ne jouent pas un rôle actif dans la mise en œuvre d'un programme TIBER-XX localisé et l'équipe de cybersécurité TIBER est établie, dans presque tous les cas, indépendamment de ces fonctions. C'est la raison pour laquelle les tests avancés prévus par le règlement proposé ([90]), sous la forme des tests de pénétration fondés sur la menace, devraient être mis en œuvre comme des outils de renforcement de l'écosystème financier et d'accroissement de la stabilité financière plutôt que comme un outil purement prudentiel. En outre, il n'est pas nécessaire de mettre au point un nouveau cadre avancé de tests de cyberrésilience, étant donné que les États membres ont déjà largement adopté le cadre TIBER-UE, seul cadre de ce type à l'heure actuelle dans l'UE.

4.3.4 Les exigences applicables aux testeurs ne devraient pas figurer dans le corps du règlement proposé, car le secteur lié aux tests de pénétration fondés sur la menace est toujours en train en cours de développement et l'innovation pourrait être entravée par l'imposition d'exigences spécifiques. Cela étant, la BCE estime que, pour garantir un degré élevé d'indépendance lors de la réalisation des tests, les entités financières ne devraient pas employer ou sous-traiter des testeurs qui sont employés ou contractés par des entités financières de leur propre groupe ou qui sont détenus ou contrôlés d'une autre manière par les entités financières à tester.

4.3.5 Afin de réduire le risque de fragmentation et de garantir une harmonisation, le règlement proposé devrait imposer un cadre de tests de pénétration fondés sur la menace s'appliquant au secteur financier dans l'ensemble de l'Union. Une fragmentation pourrait entraîner une augmentation des coûts et des besoins en ressources techniques, opérationnelles et financières, tant pour les autorités compétentes que pour les établissements financiers. Ces coûts et besoins accrus pourraient, in fine, avoir une incidence négative sur la reconnaissance mutuelle des tests. Ce manque d'harmonisation et les problèmes qui en résultent en termes de reconnaissance mutuelle sont particulièrement importants pour les entités financières, étant donné qu'il est possible qu'elles détiennent plusieurs licences ou exercent leurs activités dans plusieurs juridictions de l'Union. Les normes techniques de réglementation et d'exécution à élaborer pour les tests de pénétration fondés sur la menace en vertu du règlement proposé, devraient être conformes au cadre TIBER-UE. En outre, la BCE est favorable à la possibilité de participer à l'élaboration de ces normes techniques de réglementation et d'exécution en coopération avec les AES.

4.3.6 La participation active des autorités compétentes aux tests risque de générer un conflit d'intérêts avec leur autre fonction, à savoir l'évaluation du cadre de test de l'entité financière. Dans ce contexte, la BCE propose de supprimer du règlement proposé toute obligation incombant aux autorités compétentes concernant la validation des documents et la délivrance d'une attestation pour un test de pénétration fondé sur la menace.

4.4 Risques liés aux tiers prestataires de services informatiques

4.4.1 La BCE est favorable à l'introduction d'un ensemble complet de principes clés et d'un cadre de supervision solide pour identifier et gérer les risques informatiques découlant de tiers prestataires de services informatiques, que ceux-ci appartiennent ou non au même groupe d'entités financières. Cela étant, pour parvenir à une identification et une gestion efficaces des risques informatiques, il est important d'identifier et de classer correctement, entre autres, les tiers prestataires critiques de services informatiques. À cet égard, si la BCE est favorable à l'introduction d'actes délégués ([91]) qui compléteront les critères à utiliser à des fins de classification ([92]), elle devrait néanmoins être consultée avant l'adoption de tels actes.

([89]) Disponible sur le site internet de la BCE à l'adresse suivante : www.ecb.europa.eu.
([90]) Articles 23 et 24 du règlement proposé.
([91]) Voir l'article 28, paragraphe 3, du règlement proposé.
([92]) Voir l'article 28, paragraphe 2, du règlement proposé.

4.4.2 Concernant la structure du cadre de supervision ([93]), des précisions supplémentaires sont nécessaires au sujet du rôle que doit jouer le comité mixte. Dans le même temps, la BCE se félicite de son inclusion dans le forum de supervision en tant qu'observateur, car ce rôle lui donnera le même accès que les membres votants à la documentation et aux informations ([94]). La BCE souhaite attirer l'attention des organes législatifs de l'Union sur le fait qu'au titre de son rôle d'observateur, elle contribuerait aux travaux du forum de supervision, tant en sa qualité de banque centrale d'émission, chargée de la surveillance des infrastructures de marché, qu'en tant qu'autorité de surveillance prudentielle des établissements de crédit. En outre, la BCE fait observer que, en plus de son rôle d'observateur du forum de supervision, elle ferait également partie, en tant qu'autorité compétente, de l'équipe d'examen conjoint. À cet égard, la composition des équipes d'examen conjoint ([95]) pourrait faire l'objet d'une réflexion plus approfondie de la part des organes législatifs de l'Union afin de garantir une implication suffisamment importante des autorités compétentes concernées. De même, la BCE estime que le nombre maximal de participants aux équipes communes d'examen devrait être revu à la hausse, en tenant compte du caractère critique, de la complexité et du périmètre des services fournis par les tiers prestataires.

4.4.3 La BCE fait remarquer qu'en vertu du règlement proposé, le superviseur principal peut empêcher des tiers prestataires critiques de services informatiques de conclure d'autres accords de sous-traitance lorsque i) le sous-traitant envisagé est un tiers prestataire de services informatiques ou un sous-traitant informatique établi dans un pays tiers, et ii) la sous-traitance concerne une fonction critique de l'entité financière. La BCE tient à souligner que ces pouvoirs ne peuvent être exercés par le superviseur principal que dans le cadre d'accords de sous-traitance lorsqu'un tiers prestataire critique de services informatiques sous-traite une fonction essentielle ou importante à une entité juridique distincte établie dans un pays tiers. La BCE comprend que le superviseur principal ne pourrait pas exercer des pouvoirs semblables pour empêcher un tiers prestataire critique de services informatiques d'externaliser des fonctions critiques ou importantes de l'entité financière vers des installations du prestataire en question situées dans un pays tiers. Il se pourrait, par exemple, que, d'un point de vue opérationnel, les données ou informations critiques soient stockées ou traitées par des installations situées en dehors de l'Espace économique européen (EEE). Dans un tel cas, les pouvoirs du superviseur principal pourraient ne pas permettre aux autorités compétentes de disposer des pouvoirs appropriés pour accéder à l'ensemble des informations, des locaux, des infrastructures et du personnel nécessaires à l'exercice de toutes les fonctions critiques ou importantes de l'entité financière. Afin de garantir la capacité des autorités compétentes à s'acquitter sans entrave de leurs missions, la BCE suggère que le superviseur principal soit habilité à limiter également l'utilisation d'installations situées en dehors de l'EEE par les tiers prestataires critiques de services informatiques. Ce pouvoir pourrait être exercé dans les cas spécifiques où les accords administratifs avec les autorités compétentes du pays tiers, comme prévu par règlement proposé ([96]), ou les représentants des tiers prestataires critiques de services informatiques ne présentent pas de garanties suffisantes, compte tenu du cadre du pays tiers concerné, en rapport avec l'accès aux informations, aux locaux, à l'infrastructure et au personnel nécessaires pour mener des missions de surveillance ou de supervision.

4.4.4 Enfin, exiger des autorités compétentes qu'elles assurent le suivi des recommandations du superviseur principal ([97]) risquerait de s'avérer inefficace étant donné que les autorités compétentes pourraient ne pas avoir une vision globale des risques générés par chaque tiers prestataire critique de services informatiques. En outre, les autorités compétentes pourraient être tenues de prendre des mesures à l'encontre de leurs entités financières soumises à la surveillance prudentielle lorsque les recommandations ne sont pas prises en compte par les tiers prestataire critiques de services informatiques. En vertu du règlement proposé ([98]), les autorités compétentes pourraient exiger de leurs entités financières soumises à la surveillance prudentielle qu'elles suspendent temporairement le tiers prestataire critique de services informatiques ou qu'elles résilient les accords contractuels en vigueur conclus avec les tiers prestataires critiques de services informatiques. Il est difficile de traduire le processus de suivi envisagé en actions concrètes. En particulier, la possibilité pour une entité financière soumise à la surveillance prudentielle d'être en mesure de suspendre ou de résilier un contrat avec un tiers prestataire critique de services informatiques reste floue. Cela tient au fait que le tiers prestataire critique de services informatiques pourrait être un prestataire important pour cette entité financière, ou qu'une telle suspension ou résiliation pourrait engendrer des coûts et dommages, contractuels ou autres, pour l'entité financière. En outre, cette approche n'est pas favorable à la convergence en matière de surveillance étant donné que les autorités compétentes pourraient interpréter différemment la même recommandation. À terme, cela pourrait faire obstacle à l'harmonisation envisagée et à une approche cohérente en matière de suivi des risques informatiques critiques pour les tiers au niveau de l'Union. Compte tenu de ce qui précède, les organes législatifs de l'Union pourraient envisager d'accorder aux autorités de surveillance juridiques des pouvoirs d'exécution spécifiques à l'égard des tiers prestataires critiques de services informatiques, en tenant compte des limites imposées par la doctrine *Meroni*, telles que la Cour de justice les a partiellement atténuées dans son arrêt rendu dans l'affaire AEMF ([99]).

([93]) Voir l'article 29 du règlement proposé.
([94]) Voir l'article 29, paragraphe 3, du règlement proposé.
([95]) Voir l'article 35 du règlement proposé.
([96]) Voir l'article 39, paragraphe 1, du règlement proposé.
([97]) Voir l'article 29, paragraphe 4, et l'article 37 du règlement proposé.
([98]) Voir l'article 37, paragraphe 3, du règlement proposé.
([99]) Arrêt du 22 janvier 2014, Royaume-Uni/Parlement et Conseil, C-270/12, ECLI:EU:C:2014:18.

Lorsque la BCE recommande de modifier le règlement proposé, des suggestions de rédaction particulières, accompagnées d'une explication, figurent dans un document de travail technique séparé. Le document de travail technique peut être consulté en anglais sur le site internet EUR-Lex.

Fait à Francfort-sur-le-Main, le 4 juin 2021.

La présidente de la BCE
Christine LAGARDE