DIRECTIVE (UE) 2022/2556 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 14 décembre 2022

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

(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 53, paragraphe 1, et 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]),

considérant ce qui suit:

(1) L'Union doit traiter de manière adéquate et globale les risques numériques auxquels sont exposées toutes les entités financières et qui découlent d'un recours accru aux technologies de l'information et de la communication (TIC) dans le cadre de la fourniture et de la consommation de services financiers, ce qui contribuera à exploiter le potentiel que recèle la finance numérique en matière de stimulation de l'innovation et de promotion de la concurrence dans un environnement numérique sûr.

(2) Les entités financières sont fortement tributaires de l'utilisation des technologies numériques dans leurs activités quotidiennes. Il est dès lors primordial d'assurer la résilience opérationnelle de leurs opérations numériques face au risque lié aux TIC. Ce besoin est devenu encore plus pressant en raison de la croissance des technologies de pointe sur le marché, notamment les technologies qui permettent de transférer et de stocker de manière électronique des représentations numériques de valeurs ou de droits, en utilisant la technologie des registres distribués ou une technologie similaire (crypto-actifs), et des services liés à ces actifs.

([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 28 novembre 2022.

(3) Au niveau de l'Union, les exigences liées à la gestion du risque lié aux TIC auquel est exposé le secteur financier sont actuellement prévues par les directives 2009/65/CE ([4]), 2009/138/CE ([5]), 2011/61/UE ([6]), 2013/36/UE ([7]), 2014/59/UE ([8]), 2014/65/UE ([9]), (UE) 2015/2366 ([10]) et (UE) 2016/2341 ([11]) du Parlement européen et du Conseil.

Ces exigences sont diverses et parfois incomplètes. Dans certains cas, le risque lié aux TIC n'est abordé qu'implicitement dans le cadre du risque opérationnel et, dans d'autres cas, il n'est tout simplement pas abordé. Il est remédié à ces problèmes par l'adoption du règlement (UE) 2022/2554 du Parlement européen et du Conseil ([12]). Il y a donc lieu de modifier ces directives afin d'assurer la cohérence avec ledit règlement. La présente directive prévoit une série de modifications qui sont nécessaires pour apporter la clarté et la cohérence juridiques en ce qui concerne l'application, par les entités financières agréées et soumises à une surveillance conformément auxdites directives, de diverses exigences en matière de résilience opérationnelle numérique qui sont nécessaires à l'exercice de leurs activités et à la prestation de services, assurant ainsi le bon fonctionnement du marché intérieur. Il est nécessaire de veiller à ce que ces exigences soient en adéquation avec les évolutions du marché, tout en encourageant la proportionnalité au regard notamment de la taille des entités financières et des régimes spécifiques auxquels elles sont soumises, en vue de réduire les coûts de mise en conformité.

(4) Dans le domaine des services bancaires, la directive 2013/36/UE n'énonce actuellement que des règles générales de gouvernance interne et des dispositions relatives au risque opérationnel définissant des exigences en matière de plans d'urgence et de poursuite de l'activité qui servent implicitement de base pour traiter le risque lié aux TIC. Toutefois, afin de traiter le risque lié aux TIC explicitement et clairement, les exigences en matière de plans d'urgence et de poursuite de l'activité devraient être modifiées de manière à inclure également les plans de continuité des activités et les plans de réponse et de rétablissement en ce qui concerne le risque lié aux TIC, conformément aux exigences fixées dans le règlement (UE) 22022/2554 En outre, le risque lié aux TIC n'est inclus que de façon implicite, dans le cadre du risque opérationnel, dans le processus de contrôle et d'évaluation prudentiels (SREP) mené par les autorités compétentes et ses critères d'évaluation sont actuellement définis dans les orientations sur l'évaluation du risque lié aux TIC dans le cadre du processus de contrôle et d'évaluation prudentiels (SREP), émises par l'Autorité européenne de surveillance (Autorité bancaire européenne) (ABE), instituée par le règlement (UE) nº 1093/2010 du Parlement européen et du Conseil ([13]). Dans un souci de clarté juridique et pour veiller à ce que les autorités de surveillance du secteur bancaire cernent efficacement le risque lié aux TIC et contrôlent sa gestion par les

([4]) 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).

([5]) 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).

([6]) 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) nº 1060/2009 et (UE) nº 1095/2010 (JO L 174 du 1.7.2011, p. 1).

([7]) 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).

([8]) 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) nº 1093/2010 et (UE) nº 648/2012 (JO L 173 du 12.6.2014, p. 190).

([9]) 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).

([10]) 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) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

([11]) 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).

([12]) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (voir page 1 du présent Journal officiel).

([13]) Règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12).

entités financières conformément au nouveau cadre sur la résilience opérationnelle numérique, le champ d'application du SREP devrait également être modifié pour se référer explicitement aux exigences fixées dans le règlement (UE) 2022/2554 et couvrir en particulier les risques mis en évidence par les rapports sur les incidents majeurs liés aux TIC et par les résultats des tests de résilience opérationnelle numérique effectués par les entités financières conformément audit règlement.

(5) La résilience opérationnelle numérique est essentielle pour préserver les fonctions critiques et les activités fondamentales d'une entité financière en cas de résolution et éviter ainsi de perturber l'économie réelle et le système financier. Les incidents opérationnels majeurs peuvent entraver la capacité d'une entité financière à poursuivre ses activités et peuvent compromettre les objectifs de la résolution. Certains accords contractuels relatifs à l'utilisation de services TIC sont essentiels pour assurer la continuité opérationnelle et fournir les données nécessaires en cas de résolution. Afin qu'elle corresponde aux objectifs du cadre de l'Union en matière de résilience opérationnelle, la directive 2014/59/UE devrait être modifiée en conséquence, en vue de garantir que les informations relatives à la résilience opérationnelle sont prises en compte dans le contexte de la planification de la résolution et de l'évaluation de la résolvabilité des entités financières.

(6) La directive 2014/65/UE fixe des règles plus strictes en matière de risque lié aux TIC pour les entreprises d'investissement et les plateformes de négociation qui recourent au trading algorithmique. Des exigences moins détaillées s'appliquent aux services de communication de données et aux référentiels centraux. En outre, la directive 2014/65/UE ne fait référence que de manière limitée aux dispositifs de contrôle et de sauvegarde des systèmes informatiques et à l'utilisation de systèmes, de ressources et de procédures appropriés pour garantir la continuité et la régularité des services. De plus, cette directive devrait être alignée sur le règlement (UE) 2022/2554 en ce qui concerne la continuité et la régularité de la fourniture de services d'investissement et de l'exercice d'activités d'investissement, la résilience opérationnelle, la capacité des systèmes de négociation, et l'efficacité des mécanismes de continuité des activités et de la gestion des risques.

(7) La directive (UE) 2015/2366 énonce des règles spécifiques relatives à des éléments de maîtrise et d'atténuation des risques en matière de sécurité des TIC aux fins d'obtenir un agrément pour la prestation de services de paiement. Ces règles d'agrément devraient être modifiées afin d'être alignées sur le règlement (UE) 2022/2554. En outre, afin de réduire la charge administrative et d'éviter la complexité et la répétition des obligations de notification, les règles relatives à la notification des incidents contenues dans ladite directive devraient cesser de s'appliquer aux prestataires de services de paiement qui sont régis par ladite directive et qui relèvent également du règlement (UE) 2022/2554, leur permettant ainsi de bénéficier d'un mécanisme de notification des incidents unique et entièrement harmonisé, applicable à tous les incidents opérationnels ou de sécurité liés au paiement, que ces incidents soient liés ou non aux TIC.

(8) Les directives 2009/138/CE et (UE) 2016/2341 couvrent en partie le risque lié aux TIC dans leurs dispositions générales sur la gouvernance et la gestion des risques, certaines exigences devant être précisées par des actes délégués avec ou sans référence spécifique au risque lié aux TIC. De même, seules des règles très générales s'appliquent aux gestionnaires de fonds d'investissement alternatifs relevant de la directive 2011/61/UE et aux sociétés de gestion relevant de la directive 2009/65/CE. Ces directives devraient dès lors être alignées sur les exigences fixées dans le règlement (UE) 2022/2554 en ce qui concerne la gestion des systèmes et outils de TIC.

(9) Dans de nombreux cas, des exigences supplémentaires en matière de risque lié aux TIC ont déjà été établies dans des actes délégués et d'exécution, adoptés sur la base de projets de normes techniques de réglementation et de projets de normes techniques d'exécution élaborés par l'autorité européenne de surveillance compétente. Étant donné que les dispositions du règlement (UE) 2022/2554 constituent désormais le cadre juridique du risque lié aux TIC dans le secteur financier, certaines habilitations en vue de l'adoption d'actes délégués et d'exécution contenues dans les directives 2009/65/CE, 2009/138/CE, 2011/61/UE et 2014/65/UE devraient être modifiées afin de retirer les dispositions relatives au risque lié aux TIC du champ d'application de ces habilitations.

(10) Pour assurer une mise en œuvre cohérente du nouveau cadre en matière de résilience opérationnelle numérique du secteur financier, les États membres devraient appliquer les dispositions de droit national transposant la présente directive à partir de la date d'application du règlement (UE) 2022/2554

(11) 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 ont été adoptées sur la base de l'article 53, paragraphe 1, ou de l'article 114 du traité sur le fonctionnement de l'Union européenne, ou de ces deux dispositions. Les modifications contenues dans la présente directive ont été incluses dans un acte législatif unique en raison de l'interdépendance de l'objet et des objectifs de ces modifications. En conséquence, la présente directive devrait être adoptée sur la base à la fois de l'article 53, paragraphe 1, et de l'article 114 du traité sur le fonctionnement de l'Union européenne.

(12) Étant donné que les objectifs de la présente directive ne peuvent pas être atteints de manière suffisante par les États membres, parce qu'ils supposent l'harmonisation d'exigences déjà contenues dans des directives, mais peuvent, en raison des dimensions et des effets de l'action, 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 énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(13) Conformément à la déclaration politique commune des États membres et de la Commission du 28 septembre 2011 sur les documents explicatifs ([14]), les États membres se sont engagés à joindre à la notification de leurs mesures de transposition, dans les cas où cela se justifie, un ou plusieurs documents expliquant le lien entre les éléments d'une directive et les parties correspondantes des instruments nationaux de transposition. En ce qui concerne la présente directive, le législateur estime que la transmission de ces documents est justifiée,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Modifications de la directive 2009/65/CE

L'article 12 de la directive 2009/65/CE est modifié comme suit:

1) Au paragraphe 1, deuxième alinéa, le point a) est remplacé par le texte suivant:

«a) ait des procédures administratives et comptables saines, des dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des données, y compris en ce qui concerne les réseaux et les systèmes d'information qui sont mis en place et gérés conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil (*), ainsi que des mécanismes de contrôle interne adéquats incluant, notamment, des règles concernant les opérations personnelles de ses salariés ou la détention ou la gestion de placements dans des instruments financiers en vue d'investir pour son propre compte, et garantissant, au minimum, que chaque transaction concernant l'OPCVM peut être reconstituée quant à son origine, aux parties concernées, à sa nature, ainsi qu'au moment et au lieu où elle a été effectuée, et que les actifs des OPCVM gérés par la société de gestion sont placés conformément au règlement du fonds ou aux documents constitutifs et aux dispositions légales en vigueur;

(*) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).».

2) Le paragraphe 3 est remplacé par le texte suivant:

«3. Sans préjudice de l'article 116, la Commission adopte, par voie d'actes délégués en conformité avec l'article 112 *bis*, des mesures précisant:

a) les procédures et les dispositifs visés au paragraphe 1, deuxième alinéa, point a), autres que les procédures et les dispositifs relatifs aux réseaux et aux systèmes d'information;

b) les structures et les conditions d'organisation destinées à réduire au minimum les conflits d'intérêts, visées au paragraphe 1, deuxième alinéa, point b).».

([14]) JO C 369 du 17.12.2011, p. 14.

Article 2

Modifications de la directive 2009/138/CE

La directive 2009/138/CE est modifiée comme suit:

1) À l'article 41, le paragraphe 4 est remplacé par le texte suivant:

«4. Les entreprises d'assurance et de réassurance prennent des mesures raisonnables afin de veiller à la continuité et à la régularité dans l'accomplissement de leurs activités, y compris par l'élaboration de plans d'urgence. À cette fin, elles utilisent des systèmes, des ressources et des procédures appropriés et proportionnés et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil (*).

(*) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).».

2) À l'article 50, paragraphe 1, les points a) et b) sont remplacés par le texte suivant:

«a) les éléments des systèmes visés à l'article 41, à l'article 44, en particulier les domaines énumérés à l'article 44, paragraphe 2, et aux articles 46 et 47, autres que les éléments concernant la gestion des risques liés aux technologies de l'information et de la communication;

b) les fonctions prévues aux articles 44, 46, 47 et 48, autres que les fonctions relatives à la gestion des risques liés aux technologies de l'information et de la communication.».

Article 3

Modification de la directive 2011/61/UE

L'article 18 de la directive 2011/61/UE est remplacé par le texte suivant:

«*Article 18*

Principes généraux

1. Les États membres exigent des gestionnaires qu'ils utilisent à tout moment les ressources humaines et techniques adaptées et appropriées nécessaires pour la bonne gestion des FIA.

En particulier, les autorités compétentes de l'État membre d'origine du gestionnaire, compte tenu aussi de la nature des FIA gérés par le gestionnaire, exigent que celui-ci ait de solides procédures administratives et comptables, des dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des données, y compris en ce qui concerne les réseaux et les systèmes d'information qui sont mis en place et gérés conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil (*), ainsi que des mécanismes de contrôle interne adéquats incluant, notamment, des règles concernant les transactions personnelles de ses employés ou la détention ou la gestion d'investissements en vue d'investir pour son propre compte et garantissant, au minimum, que chaque transaction concernant les FIA peut être reconstituée quant à son origine, aux parties concernées, à sa nature, ainsi qu'au moment et au lieu où elle a été effectuée, et que les actifs des FIA gérés par le gestionnaire sont placés conformément au règlement du FIA ou à ses documents constitutifs et aux dispositions légales en vigueur.

2. La Commission adopte par voie d'actes délégués, en conformité avec l'article 56 et dans le respect des conditions fixées par les articles 57 et 58, des mesures précisant les procédures et les dispositifs visés au paragraphe 1 du présent article, autres que les procédures et les dispositifs relatifs aux réseaux et aux systèmes d'information.

(*) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).».

Article 4

Modifications de la directive 2013/36/UE

La directive 2013/36/UE est modifiée comme suit:

1) À l'article 65, paragraphe 3, point a), le point vi) est remplacé par le texte suivant:

«vi) les tiers auprès desquels les entités visées aux points i) à iv) ont externalisé des fonctions ou des activités, y compris les prestataires tiers de services TIC visés au chapitre V du règlement (UE) 2022/2554 du Parlement européen et du Conseil (*);

(*) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).».

2) À l'article 74, paragraphe 1, le premier alinéa est remplacé par le texte suivant:

«Les établissements disposent d'un dispositif solide de gouvernance d'entreprise, comprenant notamment une structure organisationnelle claire avec un partage des responsabilités bien défini, transparent et cohérent, des processus efficaces de détection, de gestion, de suivi et de déclaration des risques auxquels ils sont ou pourraient être exposés, des mécanismes adéquats de contrôle interne, y compris des procédures administratives et comptables saines, des réseaux et des systèmes d'information qui sont mis en place et gérés conformément au règlement (UE) 2022/2554 et des politiques et pratiques de rémunération permettant et favorisant une gestion saine et efficace des risques.».

3) À l'article 85, le paragraphe 2 est remplacé par le texte suivant:

«2. Les autorités compétentes veillent à ce que les établissements disposent de politiques et de plans d'urgence et de poursuite de l'activité adéquats, y compris des politiques et des plans en matière de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC concernant les technologies qu'ils utilisent pour la communication d'informations, et que ces plans soient établis, gérés et testés conformément à l'article 11 du règlement (UE) 2022/2554, afin que les établissements puissent poursuivre leurs activités en cas de grave perturbation de celles-ci et limiter les pertes subies à la suite d'une telle perturbation.».

4) À l'article 97, paragraphe 1, le point suivant est ajouté:

«d) les risques mis en évidence par des tests de résilience opérationnelle numérique conformément au chapitre IV du règlement (UE) 2022/2554.».

Article 5

Modifications de la directive 2014/59/UE

La directive 2014/59/UE est modifiée comme suit:

1) L'article 10 est modifié comme suit:

a) au paragraphe 7, le point c) est remplacé par le texte suivant:

«c) une démonstration de la façon dont les fonctions critiques et les activités fondamentales pourraient être juridiquement et économiquement séparées des autres fonctions, dans la mesure nécessaire pour assurer leur continuité et la résilience opérationnelle numérique en cas de défaillance de l'établissement;»;

b) au paragraphe 7, le point q) est remplacé par le texte suivant:

«q) une description des principaux systèmes et opérations permettant de maintenir en permanence le fonctionnement des processus opérationnels de l'établissement, y compris des réseaux et des systèmes d'information visés dans le règlement (UE) 2022/2554 du Parlement européen et du Conseil (*);

(*) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).»;

c) au paragraphe 9, l'alinéa suivant est ajouté:

«Conformément à l'article 10 du règlement (UE) nº 1093/2010, l'ABE réexamine et, le cas échéant, met à jour les normes techniques de réglementation, afin entre autres de tenir compte des dispositions du chapitre II du règlement (UE) 2022/2554.».

2) L'annexe est modifiée comme suit:

a) à la section A, le point 16 est remplacé par le texte suivant:

«16. les dispositions et les mesures nécessaires pour assurer la continuité des processus opérationnels de l'établissement, y compris les réseaux et les systèmes d'information qui sont mis en place et gérés conformément au règlement (UE) 2022/2554;»;

b) la section B est modifiée comme suit:

i) le point 14 est remplacé par le texte suivant:

«14. l'identification des propriétaires des systèmes visés au point 13, les accords sur le niveau de service qui s'y rattachent, et tous les logiciels, systèmes ou licences, y compris une mise en correspondance avec leurs personnes morales, les opérations critiques et les activités fondamentales, ainsi que l'identification des prestataires tiers critiques de services TIC, tels qu'ils sont définis à l'article 3, point 23), du règlement (UE) 2022/2554;»;

ii) le point suivant est inséré:

«14 bis. les résultats des tests de résilience opérationnelle numérique des établissements en vertu du règlement (UE) 2022/2554;»;

c) la section C est modifiée comme suit:

i) le point 4 est remplacé par le texte suivant:

«4. la mesure dans laquelle les contrats de service, y compris les accords contractuels relatifs à l'utilisation de services TIC, que l'établissement a conclus sont solides et pleinement applicables en cas de résolution de l'établissement;»;

ii) le point suivant est inséré:

«4 bis. la résilience opérationnelle numérique des réseaux et des systèmes d'information qui soutiennent les fonctions critiques et les activités fondamentales de l'établissement, compte tenu des rapports sur les incidents majeurs liés aux TIC et des résultats des tests de résilience opérationnelle numérique en vertu du règlement (UE) 2022/2554;».

Article 6

Modifications de la directive 2014/65/UE

La directive 2014/65/UE est modifiée comme suit:

1) L'article 16 est modifié comme suit:

a) le paragraphe 4 est remplacé par le texte suivant:

«4. Toute entreprise d'investissement prend des mesures raisonnables pour garantir la continuité et la régularité de la fourniture de ses services d'investissement et de l'exercice de ses activités d'investissement. À cette fin, elle utilise des systèmes appropriés et proportionnés, y compris des systèmes de technologies de l'information et de la communication (TIC) mis en place et gérés conformément à l'article 7 du règlement (UE) 2022/2554 du Parlement européen et du Conseil (*), ainsi que des ressources et des procédures appropriées et proportionnées.

(*) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).»;

b) au paragraphe 5, les deuxième et troisième alinéas sont remplacés par le texte suivant:

«Toute entreprise d'investissement dispose de procédures administratives et comptables saines, de mécanismes de contrôle interne et de techniques efficaces d'évaluation des risques.

Sans préjudice de la capacité des autorités compétentes d'exiger l'accès aux communications conformément à la présente directive et au règlement (UE) n° 600/2014, toute entreprise d'investissement dispose de mécanismes de sécurité solides pour assurer, conformément aux exigences fixées dans le règlement (UE) 2022/2554, la sécurité et l'authentification des moyens de transfert de l'information, pour réduire au minimum le risque de corruption des données et d'accès non autorisé et pour empêcher les fuites d'informations afin de maintenir ainsi en permanence la confidentialité des données.».

2) L'article 17 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. Une entreprise d'investissement recourant au trading algorithmique dispose de systèmes et contrôles des risques efficaces et adaptés à son activité pour garantir que ses systèmes de négociation sont résilients et ont une capacité suffisante conformément aux exigences fixées au chapitre II du règlement (UE) 2022/2554, qu'ils sont soumis à des seuils et limites de négociation appropriés et qu'ils préviennent l'envoi d'ordres erronés ou tout autre fonctionnement des systèmes susceptible de donner naissance ou de contribuer à une perturbation du marché.

Elle dispose également de systèmes et contrôles des risques efficaces pour garantir que ses systèmes de négociation ne peuvent être utilisés à aucune fin contraire au règlement (UE) n° 596/2014 ou aux règles d'une plate-forme de négociation à laquelle elle est connectée.

Elle dispose de mécanismes de continuité des activités efficaces pour faire face à toute défaillance de ses systèmes de négociation, y compris d'une politique et de plans en matière de continuité des activités de TIC et de plans de réponse et de rétablissement des TIC mis en place conformément à l'article 11 du règlement (UE) 2022/2554, et elle veille à ce que ses systèmes soient entièrement testés et convenablement suivis de manière à garantir qu'ils satisfont aux exigences générales fixées au présent paragraphe et aux exigences spécifiques fixées aux chapitres II et IV du règlement (UE) 2022/2554.»;

b) au paragraphe 7, le point a) est remplacé par le texte suivant:

«a) le détail des exigences organisationnelles prévues aux paragraphes 1 à 6, autres que celles liées à la gestion des risques liés aux TIC, qu'il convient d'imposer aux entreprises d'investissement fournissant différents services d'investissement et services auxiliaires ou exerçant différentes activités d'investissement ou offrant une combinaison de ces services, selon lequel les précisions relatives aux exigences organisationnelles visées au paragraphe 5 comportent, pour l'accès direct au marché et l'accès sponsorisé, des exigences particulières propres à permettre que les contrôles appliqués à l'accès sponsorisé soient au minimum équivalents à ceux appliqués à l'accès direct au marché;».

3) À l'article 47, le paragraphe 1 est modifié comme suit:

a) le point b) est remplacé par le texte suivant:

«b) qu'ils soient adéquatement équipés pour gérer les risques auxquels ils sont exposés, y compris le risque lié aux TIC conformément au chapitre II du règlement (UE) 2022/2554, qu'ils mettent en œuvre des dispositifs et des systèmes appropriés leur permettant de cerner les risques significatifs pouvant compromettre leur bon fonctionnement, et qu'ils instaurent des mesures effectives pour atténuer ces risques;»;

b) le point c) est supprimé.

4) L'article 48 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. Les États membres exigent d'un marché réglementé qu'il mette en place et maintienne sa résilience opérationnelle conformément aux exigences fixées au chapitre II du règlement (UE) 2022/2554 pour garantir que ses systèmes de négociation sont résilients, possèdent une capacité suffisante pour gérer les volumes les plus élevés d'ordres et de messages, sont en mesure d'assurer un processus de négociation ordonné en période de graves tensions sur les marchés, sont soumis à des tests exhaustifs afin de confirmer que ces conditions sont réunies et sont régis par des mécanismes de continuité des activités, y compris une politique et des plans en matière de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC mis en place conformément à l'article 11 du règlement (UE) 2022/2554, afin d'assurer le maintien de ses services en cas de défaillance de ses systèmes de négociation.»;

b) le paragraphe 6 est remplacé par le texte suivant:

«6. Les États membres exigent d'un marché réglementé qu'il dispose de systèmes, de procédures et de mécanismes efficaces, y compris qu'il exige de ses membres ou de ses participants qu'ils procèdent à des essais appropriés d'algorithmes et mettent à disposition les environnements facilitant ces essais conformément aux exigences fixées aux chapitres II et IV du règlement (UE) 2022/2554, pour garantir que les systèmes de trading algorithmique ne donnent pas naissance ou ne contribuent pas à des conditions de négociation de nature à perturber le bon ordre du marché, et pour gérer les conditions de négociation de nature à perturber le bon ordre du marché qui découlent de ces systèmes de trading algorithmique, y compris de systèmes permettant de limiter la proportion d'ordres non exécutés par rapport aux transactions susceptibles d'être introduites dans le système par un membre ou un participant, afin de ralentir le flux d'ordres si le système risque d'atteindre sa capacité maximale ainsi que de limiter le pas minimal de cotation sur le marché et de veiller à son respect.»;

c) le paragraphe 12 est modifié comme suit:

i) le point a) est remplacé par le texte suivant:

«a) les exigences pour s'assurer que les systèmes de négociation des marchés réglementés sont résilients et disposent de capacités adéquates, à l'exception des exigences relatives à la résilience opérationnelle numérique;»;

ii) le point g) est remplacé par le texte suivant:

«g) les exigences pour veiller à l'essai approprié des algorithmes, autres que les tests de résilience opérationnelle numérique, de manière à garantir que les systèmes de trading algorithmique, y compris les systèmes de trading algorithmique de haute fréquence, ne donnent pas naissance ou ne contribuent pas à des conditions de négociation de nature à perturber le bon ordre du marché.».

Article 7

Modifications de la directive (UE) 2015/2366

La directive (UE) 2015/2366 est modifiée comme suit:

1) À l'article 3, le point j) et remplacé par le texte suivant:

«j) aux services fournis par des prestataires de services techniques à l'appui de la fourniture de services de paiement, sans qu'ils entrent, à aucun moment, en possession des fonds à transférer et consistant notamment dans le traitement et l'enregistrement des données, les services de protection de la confiance et de la vie privée, l'authentification des données et des entités, la fourniture de technologies de l'information et de la communication (TIC) et la fourniture de réseaux de communication, ainsi que la fourniture et la maintenance des terminaux et dispositifs utilisés aux fins des services de paiement, à l'exception des services d'initiation de paiement et des services d'information sur les comptes;».

2) À l'article 5, le paragraphe 1 est modifié comme suit:

a) le premier alinéa est modifié comme suit:

i) le point e) est remplacé par le texte suivant:

«e) une description du dispositif de gouvernance d'entreprise et des mécanismes de contrôle interne, notamment des procédures administratives, de gestion des risques et comptables du demandeur, ainsi que des dispositions relatives à l'utilisation des services TIC conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil (*), qui démontre que ce dispositif de gouvernance d'entreprise et ces mécanismes de contrôle interne sont proportionnés, adaptés, sains et adéquats;

(*) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).»;

ii) le point f) est remplacé par le texte suivant:

«f) une description de la procédure en place pour assurer la surveillance, le traitement et le suivi des incidents de sécurité et des réclamations de clients liées à la sécurité, y compris un mécanisme de signalement des incidents qui tient compte des obligations de notification incombant à l'établissement de paiement fixées au chapitre III du règlement (UE) 2022/2554;»;

iii) le point h) est remplacé par le texte suivant:

«h) une description des dispositions en matière de continuité des activités, y compris une désignation claire des opérations critiques, une politique et des plans en matière de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC efficaces, ainsi qu'une procédure prévoyant de tester et de réexaminer régulièrement le caractère adéquat et l'efficacité de ces plans conformément au règlement (UE) 2022/2554;»;

b) le troisième alinéa est remplacé par le texte suivant:

«La description des mesures de maîtrise et d'atténuation des risques en matière de sécurité visée au premier alinéa, point j), indique comment ces mesures garantissent un niveau élevé de résilience opérationnelle numérique conformément au chapitre II du règlement (UE) 2022/2554, notamment en ce qui concerne la sécurité technique et la protection des données, y compris pour les logiciels et les systèmes de TIC utilisés par le demandeur ou par les entreprises vers lesquelles il externalise la totalité ou une partie de ses activités. Ces mesures incluent également les mesures de sécurité prévues à l'article 95, paragraphe 1, de la présente directive. Elles tiennent compte des orientations de l'ABE relatives aux mesures de sécurité, visées à l'article 95, paragraphe 3, de la présente directive, une fois celles-ci établies.».

3) À l'article 19, paragraphe 6, le deuxième alinéa est remplacé par le texte suivant:

«L'externalisation de fonctions opérationnelles importantes, y compris les systèmes de TIC, ne peut être faite d'une manière qui nuise sérieusement à la qualité du contrôle interne de l'établissement de paiement et à la capacité des autorités compétentes de contrôler et d'établir que cet établissement respecte bien l'ensemble des obligations fixées par la présente directive.».

4) À l'article 95, paragraphe 1, l'alinéa suivant est ajouté:

«Le premier alinéa est sans préjudice de l'application du chapitre II du règlement (UE) 2022/2554 aux:

a) prestataires de services de paiement visés à l'article 1er, paragraphe 1, points a), b) et d), de la présente directive;

b) prestataires de services d'information sur les comptes visés à l'article 33, paragraphe 1, de la présente directe;

c) établissements de paiement exemptés en vertu de l'article 32, paragraphe 1, de la présente directive;

d) établissements de monnaie électronique bénéficiant d'une exemption visés à l'article 9, paragraphe 1, de la directive 2009/110/CE.».

5) À l'article 96, le paragraphe suivant est ajouté:

«7. Les États membres veillent à ce que les paragraphes 1 à 5 du présent article ne s'appliquent pas aux:

a) prestataires de services de paiement visés à l'article 1er, paragraphe 1, points a), b) et d), de la présente directive:

b) prestataires de services d'information sur les comptes visés à l'article 33, paragraphe 1, de la présente directive;

c) établissements de paiement exemptés en vertu de l'article 32, paragraphe 1, de la présente directive;

d) établissements de monnaie électronique bénéficiant d'une exemption visés à l'article 9, paragraphe 1, de la directive 2009/110/CE.».

6) À l'article 98, le paragraphe 5 est remplacé par le texte suivant:

«5. Conformément à l'article 10 du règlement (UE) no 1093/2010, l'ABE réexamine et, le cas échéant, met à jour les normes techniques de réglementation à intervalles réguliers, afin notamment de tenir compte de l'innovation et des progrès technologiques, ainsi que des dispositions du chapitre II du règlement (UE) 2022/2554.».

Article 8

Modification de la directive (UE) 2016/2341

L'article 21, paragraphe 5, de la directive (UE) 2016/2341, est remplacé par le texte suivant:

«5. Les États membres veillent à ce que les IRP prennent des mesures raisonnables afin de veiller à la continuité et à la régularité dans l'accomplissement de leurs activités, y compris par l'élaboration de plans d'urgence. À cette fin, les IRP

utilisent des systèmes, des ressources et des procédures appropriés et proportionnés et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil (*), le cas échéant.

(*) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).».

Article 9

Transposition

1. Les États membres adoptent et publient, au plus tard le 17 janvier 2025, les dispositions nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission.

Ils appliquent ces dispositions à partir du 17 janvier 2025.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 10

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 11

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Strasbourg, le 14 décembre 2022.

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
R. METSOLA	M. BEK