I

(Résolutions, recommandations et avis)

RECOMMANDATIONS

COMITÉ EUROPÉEN DU RISQUE SYSTÉMIQUE

RECOMMANDATION DU COMITE EUROPEEN DU RISQUE SYSTEMIQUE

N madu 2 décembre 2021

sur un cadre paneuropéen de coordination des cyberincidents systémiques pour les autorités concernées

(CERS/2021/17)

(2022/C 134/01)

LE CONSEIL GÉNÉRAL DU COMITÉ EUROPÉEN DU RISQUE SYSTÉMIQUE,

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

vu l'accord sur l'Espace économique européen ([1]), et notamment son annexe IX,

vu le règlement (UE) n° 1092/2010 du Parlement européen et du Conseil du 24 novembre 2010 relatif à la surveillance macroprudentielle du système financier dans l'Union européenne et instituant un Comité européen du risque systémique ([2]), et notamment son article 3, paragraphe 2, points b) et d), et ses articles 16 et 18,

vu la décision CERS/2011/1 du Comité européen du risque systémique du 20 janvier 2011 portant adoption du règlement intérieur du Comité européen du risque systémique ([3]), et notamment ses articles 18 à 20,

considérant ce qui suit :

(1) Comme indiqué au considérant 4 de la recommandation CERS/2013/1 du Comité européen du risque systémique ([4]), l'objectif ultime de la politique macroprudentielle est de contribuer au maintien de la stabilité du système financier dans son ensemble, y compris en renforçant la résilience du système financier et en diminuant l'accumulation de risques systémiques, et d'assurer ainsi une contribution durable du secteur financier à la croissance économique. Le Comité européen du risque systémique (CERS) est responsable de la surveillance macroprudentielle du système financier au sein de l'Union. Dans l'accomplissement de son mandat, le CERS devrait contribuer à la prévention et à l'atténuation des risques systémiques pour la stabilité financière, y compris ceux liés aux cyberincidents, et proposer des moyens d'atténuer ces risques.

(2) Les cyberincidents majeurs peuvent présenter un risque systémique pour le système financier en raison de leur capacité à perturber les opérations et services financiers essentiels. L'amplification d'un choc initial peut se produire soit par contagion opérationnelle ou financière, soit par une érosion de la confiance dans le système financier. Si le système financier n'est pas en mesure d'absorber ces chocs, la stabilité financière sera menacée et cette situation peut donner lieu à une cybercrise systémique ([5]).

([1]) JO L 1 du 3.1.1994, p. 3.
([2]) JO L 331 du 15.12.2010, p. 1.
([3]) JO C 58 du 24.2.2011, p. 4.
([4]) Recommandation CERS/2013/1 du Comité européen du risque systémique du 4 avril 2013 sur les objectifs intermédiaires et les instruments de la politique macroprudentielle (JO C 170 du 15.6.2013, p. 1).
([5]) Voir *Systemic cyber risk*, CERS, février 2020, disponible en anglais sur le site internet du CERS à l'adresse suivante : www.esrb.europa.eu

(3) L'évolution constante du paysage des cybermenaces et l'augmentation récente de cyberincidents majeurs sont des indicateurs d'un risque accru pour la stabilité financière de l'Union. La pandémie de COVID-19 a mis en évidence l'importance du rôle joué par la technologie pour permettre au système financier de fonctionner. Les autorités et institutions concernées ont dû adapter leur infrastructure technique et leurs cadres de gestion des risques à une soudaine augmentation du travail à distance, ce qui a augmenté l'exposition globale du système financier global aux cybermenaces et permis aux criminels de concevoir de nouveaux modes opératoires et d'adapter ceux existants pour tirer parti de la situation ([6]). Dans ce contexte, le nombre de cyberincidents signalés à la surveillance bancaire de la BCE en 2020 a augmenté de 54 % par rapport à 2019 ([7]).

(4) L'ampleur, la rapidité et le rythme de propagation potentiels d'un cyberincident majeur appellent une réponse efficace des autorités concernées afin d'atténuer les effets négatifs éventuels sur la stabilité financière. Une coordination et une communication rapides entre les autorités concernées au niveau de l'Union peuvent faciliter l'évaluation précoce de l'incidence d'un cyberincident majeur sur la stabilité financière, maintenir la confiance dans le système financier et limiter la contagion à d'autres établissements financiers, et contribuer ainsi à empêcher qu'un cyberincident majeur ne devienne un risque pour la stabilité financière.

(5) Le choc sous-jacent naît de manière inédite par rapport aux crises financières et de liquidité traditionnelles auxquelles les autorités concernées sont habituellement confrontées. Outre les aspects financiers, l'évaluation globale des risques doit inclure l'ampleur et l'incidence des perturbations opérationnelles étant donné que celles-ci pourraient influencer le choix des outils macroprudentiels. De même, la stabilité financière pourrait également influencer le choix des mesures d'atténuation opérationnelles par les experts en cybersécurité. Cela nécessite une coordination étroite et rapide et une communication ouverte afin, notamment, de développer la connaissance de la situation.

(6) Le risque d'un manque de coordination de la part des autorités existe et doit être traité. Les autorités concernées de l'Union devront se coordonner entre elles et avec d'autres autorités, telles que l'Agence de l'Union européenne pour la cybersécurité (ENISA), avec lesquelles elles pourraient ne pas interagir habituellement. Étant donné qu'un nombre important d'établissements financiers de l'Union opèrent à l'échelle mondiale, un cyberincident majeur ne se limitera probablement pas à l'Union ou pourrait être déclenché en dehors de l'Union et pourrait nécessiter une coordination mondiale de la réponse.

(7) Les autorités concernées doivent être préparées à ces interactions. Dans le cas contraire, elles risqueraient de prendre des mesures incohérentes qui contredisent ou compromettent les réponses d'autres autorités. Un tel manque de coordination pourrait amplifier le choc pour le système financier en entraînant une érosion de la confiance dans le fonctionnement du système financier, ce qui, dans le pire des cas, représenterait un risque pour la stabilité financière ([8]). Il convient donc de prendre les mesures nécessaires pour faire face au risque pour la stabilité financière découlant d'un manque de coordination en cas de cyberincident majeur.

(8) Le rapport du CERS (2021) intitulé *Mitigating systemic cyber risk* ([9]) met en évidence la nécessité d'établir un cadre paneuropéen de coordination des cyberincidents systémiques (EU-SCICF) pour les autorités concernées de l'Union. L'objectif de l'EU-SCICF serait d'augmenter le niveau de préparation des autorités concernées pour faciliter une réponse coordonnée à un cyberincident potentiellement majeur. Le rapport du CERS (2021) intitulé *Mitigating systemic cyber risk* présente l'évaluation du CERS concernant les caractéristiques du cadre qui seraient nécessaires, à première vue, afin de faire face à un risque de manque de coordination.

(9) L'objectif principal de la présente recommandation est de tirer parti de l'un des rôles envisagés pour les autorités européennes de surveillance (AES) dans le cadre de la proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier ([10]) (ci-après « DORA »), à savoir favoriser la mise en place progressive d'une réponse efficace et coordonnée au niveau de l'Union en cas d'incident transfrontalier majeur lié aux technologies de l'information et de la communication (TIC) ou de menace connexe ayant une incidence systémique sur l'ensemble du secteur financier de l'Union. Ce processus conduira à la création de l'EU-SCICF pour les autorités concernées.

([6]) Voir *Internet Organised Crime Threat Assessment*, Europol, 2020, disponible en anglais sur le site internet d'Europol à l'adresse suivante : www.europol.europa.eu

([7]) Voir *IT and cyber risk: a constant challenge*, BCE, 2021, disponible en anglais sur le site internet de la BCE consacré à la supervision bancaire à l'adresse suivante : www.bankingsupervision.europa.eu

([8]) Voir *Systemic cyber risk*, CERS, février 2020, disponible en anglais sur le site internet du CERS à l'adresse suivante : www.esrb.europa.eu

([9]) Voir *Mitigating systemic cyber risk*, CERS, 2021, à paraître.

([10]) COM(2020) 595 final.

(10) L'EU-SCICF ne devrait pas viser à remplacer les cadres existants, mais à combler toute lacune en matière de coordination et de communication entre les autorités concernées elles-mêmes et avec d'autres autorités de l'Union et d'autres acteurs clés au niveau international. À cet égard, il convient de tenir compte du positionnement de l'EU-SCICF dans le paysage des cadres existants en matière de crise financière et de cyberincidents de l'Union. En ce qui concerne la coordination entre les autorités concernées elles-mêmes, il convient de tenir compte, sans s'y limiter, des rôles et activités du groupe de coopération sur les réseaux et systèmes d'information (SRI) pour les entités financières au titre de la directive (UE) 2016/1148 du Parlement européen et du Conseil ([11]), et des mécanismes de coordination envisagés par la création de l'unité conjointe de cybersécurité parallèlement à la participation de l'ENISA.

(11) En particulier, la proposition de lancer la préparation de l'EU-SCICF vise à approuver les rôles potentiels des AES, comme le prévoit la proposition DORA. DORA propose que « [l]es AES, par l'intermédiaire du comité mixte et en collaboration avec les autorités compétentes, la BCE [(Banque centrale européenne)] et le CERS, [puissent] mettre en place des mécanismes qui permettent le partage de pratiques efficaces entre les secteurs financiers afin d'améliorer la perception de chaque situation et de détecter les cybervulnérabilités et les cyberrisques communs aux différents secteurs » et qu'elles « [puissent] mettre au point des exercices de gestion de crise et d'urgence reposant sur des scénarios de cyberattaques, en vue de développer les canaux de communication et de favoriser la mise en place progressive d'une réponse efficace et coordonnée au niveau de l'Union, en cas d'incident transfrontière majeur lié à l'informatique ou de menace connexe ayant une incidence systémique sur l'ensemble du secteur financier de l'Union » ([12]). Un cadre paneuropéen tel que l'EU-SCICF n'existe pas encore et devrait être établi et développé dans le cadre de DORA.

(12) Compte tenu du risque que représente le cyberrisque pour la stabilité financière de l'Union, les travaux préparatoires en vue de la mise en place progressive de l'EU-SCICF devraient, dans la mesure du possible, commencer avant même que le cadre juridique et politique requis pour sa mise en place ne soit pleinement applicable. Ce cadre juridique et politique serait entièrement achevé et finalisé une fois que les dispositions pertinentes de DORA et de ses actes délégués deviennent applicables.

(13) Une communication efficace contribue à la connaissance de la situation par les autorités concernées et constitue donc une condition préalable indispensable à la coordination à l'échelle de l'Union lors de cyberincidents majeurs. À cet égard, il convient de définir l'infrastructure de communication nécessaire pour coordonner la réponse à un cyberincident majeur. Cela supposerait de préciser le type d'informations qui doivent être partagées, les canaux réguliers à utiliser pour partager ces informations et les points de contact avec lesquels les informations devraient être partagées. Le partage d'informations doit respecter les exigences juridiques existantes. En outre, il se peut que les autorités concernées doivent définir un plan d'action clair et les protocoles à suivre afin d'assurer une bonne coordination entre les autorités intervenant dans la planification d'une réponse coordonnée à un cyberincident majeur.

(14) Une cybercrise systémique nécessitera la mise en œuvre d'une coopération pleine et entière au niveau national et au niveau de l'Union. Par conséquent, la désignation de points de contact pour les AES, la BCE et chaque État membre – pour ces derniers, choisis parmi leurs autorités nationales concernées –, qui devrait être communiquée aux AES, peut être envisagée pour déterminer les principaux interlocuteurs du mécanisme de coordination de l'EU-SCICF à informer en cas de cyberincident majeur. Il convient d'évaluer la nécessité de désigner des points de contact au cours de l'élaboration de l'EU-SCICF, en tenant compte du point de contact unique que les États membres ont désigné, en vertu de la directive (UE) 2016/1148, aux fins de la sécurité des réseaux et des systèmes d'information pour assurer la coopération transfrontalière avec d'autres États membres et avec le groupe de coopération SRI ([13]).

(15) La conduite d'exercices de gestion de crise et d'urgence pourrait faciliter la mise en œuvre de l'EU-SCICF et permettre aux autorités d'évaluer leur degré de réactivité et de préparation à une cybercrise systémique au niveau de l'Union. Les autorités tireraient des enseignements de ces exercices, ce qui permettrait d'améliorer et de faire évoluer en continu l'EU-SCICF.

([11]) 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).

([12]) Voir le projet d'article 43 de la proposition de DORA.

([13]) Voir Commission européenne, groupe de coopération SRI, disponible sur le site internet de la Commission européenne à l'adresse suivante : www.ec.europa.eu

(16) Pour l'élaboration de l'EU-SCICF, il est essentiel que les AES mènent conjointement les travaux préparatoires appropriés afin d'examiner les éléments clés possibles du cadre ainsi que les ressources et besoins nécessaires en vue de son élaboration. Ensuite, les AES pourraient commencer à procéder à une analyse préliminaire de tout obstacle qui serait susceptible d'entraver la capacité des AES et des autorités concernées à établir l'EU-SCICF et à partager les informations pertinentes par les canaux de communication en cas de cyberincident majeur. Une telle analyse constituerait une étape importante pour éclairer toute action ultérieure, que celle-ci soit de nature législative ou qu'il s'agisse d'autres initiatives de soutien que la Commission européenne pourrait prendre dans la phase de mise en œuvre post-DORA,

A ADOPTÉ LA PRÉSENTE RECOMMANDATION :

SECTION 1

RECOMMANDATIONS

Recommandation A – Création d'un cadre paneuropéen de coordination des cyberincidents systémiques (EU-SCICF)

1. Il est recommandé que, comme le prévoit la proposition de la Commission d'un règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (ci-après « DORA »), les autorités européennes de surveillance (AES), conjointement par l'intermédiaire du comité mixte et conjointement avec la Banque centrale européenne (BCE), le Comité européen du risque systémique (CERS) et les autorités nationales concernées, commencent à préparer la mise au place progressive d'une réponse efficace et coordonnée au niveau de l'Union en cas de cyberincident transfrontalier majeur ou de menace connexe qui pourrait avoir une incidence systémique sur le secteur financier de l'Union. Les travaux préparatoires en vue d'une réponse coordonnée au niveau de l'Union devraient impliquer la mise en place progressive de l'EU-SCICF pour les AES, la BCE, le CERS et les autorités nationales concernées. Les travaux préparatoires devraient également inclure une évaluation des ressources nécessaires pour une mise en place efficace de l'EU-SCICF.

2. Il est recommandé que les AES entreprennent, compte tenu de la sous-recommandation A, paragraphe 1, en concertation avec la BCE et le CERS, une cartographie et une analyse ultérieure des obstacles actuels, juridiques et des autres obstacles opérationnels à la mise en place efficace de l'EU-SCICF.

Recommandation B – Mise en place des points de contact de l'EU-SCICF

Il est recommandé que les AES, la BCE et chaque État membre – pour ces derniers, parmi leurs autorités nationales concernées –, désignent un point de contact principal qui devrait être communiqué aux AES. Cette liste de contacts facilitera l'élaboration du cadre et, une fois que l'EU-SCICF est en place, les points de contact et le CERS devraient être informés en cas de cyberincident majeur. Une coordination devrait également être envisagée entre l'EU-SCICF et le point de contact unique que les États membres ont désigné, en vertu de la directive (UE) 2016/1148, aux fins de la sécurité des réseaux et des systèmes d'information pour assurer la coopération transfrontalière avec d'autres États membres et avec le groupe de coopération sur les réseaux et systèmes d'information.

Recommandation C – Mesures appropriées au niveau de l'Union

Il est recommandé que, sur la base des résultats des analyses effectuées conformément à la recommandation A, la Commission examine les mesures appropriées nécessaires pour assurer une coordination efficace des réponses aux cyberincidents systémiques.

SECTION 2

MISE EN ŒUVRE

1. **Définitions**

Aux fins de la présente recommandation, on entend par :

a) « cyber », se rapportant à, au sein de, ou par l'intermédiaire de l'infrastructure d'information interconnectée des interactions entre les personnes, les processus, les données et les systèmes d'information ([14]) ;

([14]) Voir *Cyber Lexicon*, CSF, 12 novembre 2018, disponible en anglais sur le site internet du CSF à l'adresse suivante : www.fsb.org

b) « cyberincident majeur », un incident majeur lié aux technologies de l'information et de la communication (TIC) ayant une incidence négative potentiellement élevée sur les réseaux et les systèmes d'information qui sous-tendent les fonctions critiques des entités financières ([15]) ;

c) « cybercrise systémique », un cyberincident majeur qui cause un niveau de perturbation du système financier de l'Union susceptible d'entraîner de graves conséquences négatives sur le bon fonctionnement du marché intérieur et le fonctionnement de l'économie réelle. Une telle crise pourrait découler d'un cyberincident majeur provoquant des chocs dans un certain nombre de canaux, y compris opérationnels, financiers et de confiance ;

d) « autorités européennes de surveillance » ou « AES », l'Autorité européenne de surveillance (Autorité bancaire européenne) instituée par le règlement (UE) n° 1093/2010 du Parlement européen et du Conseil ([16]), l'Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles) instituée par le règlement (UE) n° 1094/2010 du Parlement européen et du Conseil ([17]) et l'Autorité européenne de surveillance (Autorité européenne des marchés financier) instituée par le règlement (UE) n° 1095/2010 du Parlement européen et du Conseil ([18]) ;

e) « comité mixte », le comité mixte des autorités européennes de surveillance institué par l'article 54 du règlement (UE) n° 1093/2010, du règlement (UE) n° 1094/2010 et du règlement (UE) n° 1095/2010 ;

f) « autorité nationale concernée »,

1. une autorité compétente ou une autorité de surveillance d'un État membre, telle que précisée dans les actes de l'Union visés à l'article 1er, paragraphe 2, du règlement (UE) n° 1093/2010, du règlement (UE) n° 1094/2010 et du règlement (UE) n° 1095/2010, et toute autre autorité compétente nationale telle que précisée dans les actes de l'Union qui confient des missions aux AES ;

2. une autorité compétente d'un État membre désignée conformément à :

i. l'article 4 de la directive 2013/36/UE du Parlement européen et du Conseil ([19]), sans préjudice des missions spécifiques confiées à la BCE par le règlement (UE) n° 1024/2013 du Conseil ([20]) ;

ii. l'article 22 de la directive (UE) 2015/2366 du Parlement européen et du Conseil ([21]) ;

iii. l'article 37 de la directive 2009/110/UE du Parlement européen et du Conseil ([22]) ;

iv. l'article 4 de la directive (UE) n° 2019/2034 du Parlement européen et du Conseil ([23]) ;

([15]) Voir article 3, point 7, de la proposition de DORA.

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

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

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

([19]) 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).

([20]) Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit (JO L 287 du 29.10.2013, p. 63).

([21]) 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).

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

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

v. l'article 3, paragraphe 1, point ee), premier tiret, de la proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937 ([24]) ;

vi. l'article 11 du règlement (UE) n° 909/2014 du Parlement européen et du Conseil ([25]) ;

vii. l'article 22 du règlement (UE) n° 648/2012 du Parlement européen et du Conseil ([26]) ;

viii. l'article 67 de la directive 2014/65/UE du Parlement européen et du Conseil ([27]) ;

ix. l'article 22 du règlement (UE) n° 648/2012 ;

x. l'article 44 de la directive 2011/61/UE du Parlement européen et du Conseil ([28]) ;

xi. l'article 97 de la directive 2009/65/CE du Parlement européen et du Conseil ([29]) ;

xii. l'article 30 de la directive 2009/138/CE du Parlement européen et du Conseil ([30]) ;

xiii. l'article 12 de la directive (UE) 2016/97 du Parlement européen et du Conseil ([31]) ;

xiv. l'article 47 de la directive (UE) 2016/2341 du Parlement européen et du Conseil ([32]) ;

xv. l'article 22 du règlement (CE) n° 1060/2009 du Parlement européen et du Conseil ([33]) ;

xvi. l'article 3, paragraphe 2, et l'article 32 de la directive 2006/43/CE du Parlement européen et du Conseil ([34]) ;

xvii. l'article 40 du règlement (UE) 2016/1011 du Parlement européen et du Conseil ([35]) ;

xviii. l'article 29 du règlement (UE) 2020/1503 du Parlement européen et du Conseil ([36]) ;

([24]) COM(2020) 593 final.

([25]) 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).

([26]) 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).

([27]) 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).

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

([29]) 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).

([30]) 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).

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

([32]) 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).

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

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

([35]) Règlement (UE) 2016/1011 du Parlement européen et du Conseil du 8 juin 2016 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement et modifiant les directives 2008/48/CE et 2014/17/UE et le règlement (UE) n° 596/2014 (JO L 171 du 29.6.2016, p. 1).

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

3. une autorité à laquelle est confiée l'adoption ou l'activation de mesures de politique macroprudentielle ou d'autres missions en matière de stabilité financière, telles que des analyses complémentaires connexes, notamment :

   i. une autorité désignée en vertu du titre VII, chapitre 4, de la directive 2013/36/UE ou de l'article 458, paragraphe 1, du règlement (UE) n° 575/2013 du Parlement européen et du Conseil ([37]);

   ii. une autorité macroprudentielle dont les objectifs, accords, missions, pouvoirs, instruments, exigences de responsabilité et autres caractéristiques sont définis dans la recommandation CERS/2011/3 du Comité européen du risque systémique ([38]).

g) « autorité concernée »,

   1. une AES ;

   2. la BCE pour les missions qui lui sont confiées conformément à l'article 4, paragraphes 1 et 2, et à l'article 5, paragraphe 2, du règlement (UE) n° 1024/2013 ;

   3. une autorité nationale concernée.

2. **Critères de mise en œuvre**

La mise en œuvre de la présente recommandation satisfait aux critères suivants :

a) il convient de tenir dûment compte du principe du « besoin d'en connaître » et du principe de proportionnalité, en considérant l'objectif et le contenu de chaque recommandation ;

b) il convient de respecter les critères de conformité particuliers énoncés en annexe concernant chaque recommandation.

3. **Calendrier du suivi**

Conformément à l'article 17, paragraphe 1, du règlement (UE) n° 1092/2010, les destinataires doivent communiquer au Parlement européen, au Conseil, à la Commission et au CERS les mesures prises en réponse à la présente recommandation ou fournit une justification en cas d'inaction. Les destinataires sont invités à communiquer ces informations conformément au calendrier suivant :

1. Recommandation A

   a) Au plus tard le 30 juin 2023, mais au plus tôt six mois après l'entrée en vigueur de DORA, les AES sont invitées à présenter au Parlement européen, au Conseil, à la Commission et au CERS un rapport intermédiaire sur la mise en œuvre de la sous-recommandation A, paragraphe 1.

   b) Au plus tard le 30 juin 2024, mais au plus tôt dix-huit mois après l'entrée en vigueur de DORA, les AES sont invitées à présenter au Parlement européen, au Conseil, à la Commission et au CERS un rapport final sur la mise en œuvre de la sous-recommandation A, paragraphe 1.

   c) Au plus tard le 30 juin 2025, mais au plus tôt trente mois après l'entrée en vigueur de DORA, les AES sont invitées à présenter au Parlement européen, au Conseil, à la Commission et au CERS un rapport sur la mise en œuvre de la sous-recommandation A, paragraphe 2.

2. Recommandation B

   Au plus tard le 30 juin 2023, mais au plus tôt six mois après l'entrée en vigueur de DORA, les AES, la BCE et les États membres sont invités à présenter au Parlement européen, au Conseil, à la Commission et au CERS un rapport sur la mise en œuvre de la recommandation B.

3. Recommandation C

   a) Au plus tard le 31 décembre 2023, mais au plus tôt douze mois après l'entrée en vigueur de DORA, la Commission est invitée à présenter au Parlement européen, au Conseil et au CERS un rapport sur la mise en œuvre de la recommandation C, compte tenu du rapport intermédiaire des AES prévu dans la sous-recommandation A, paragraphe 1.

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

([38]) Recommandation CERS/2011/3 du Comité européen du risque systémique du 22 décembre 2011 concernant le mandat macroprudentiel des autorités nationales (JO C 41 du 14.2.2012, p. 1).

b) Au plus tard le 31 décembre 2025, mais au plus tôt trente-six mois après l'entrée en vigueur de DORA, la Commission est invitée à présenter au Parlement européen, au Conseil et au CERS un rapport sur la mise en œuvre de la recommandation C, compte tenu des rapports des AES prévu dans la recommandation A.

4. **Suivi et évaluation**

1. Le secrétariat du CERS :

a) aidera les destinataires, en assurant la coordination des rapports et en fournissant les modèles adéquats, et en donnant, le cas échéant, des précisions sur la procédure et le calendrier du suivi ;

b) vérifiera le suivi effectué par les destinataires, leur prêtera assistance sur demande, et soumettra les rapports de suivi au conseil général. Les évaluations seront entreprises comme suit :

i) dans les douze mois suivant l'entrée en vigueur de DORA, en ce qui concerne la mise en œuvre des recommandations A et B ;

ii) dans les dix-huit mois suivant l'entrée en vigueur de DORA, en ce qui concerne la mise en œuvre de la recommandation C ;

iii) dans les vingt-quatre mois suivant l'entrée en vigueur de DORA, en ce qui concerne la mise en œuvre de la recommandation A ;

iv) dans les trente-six mois suivant l'entrée en vigueur de DORA, en ce qui concerne la mise en œuvre de la recommandation A ;

v) dans les quarante-deux mois suivant l'entrée en vigueur de DORA, en ce qui concerne la mise en œuvre de la recommandation C.

2. Le conseil général évaluera les mesures et les justifications communiquées par les destinataires et, le cas échéant, pourra décider que la présente recommandation n'a pas été suivie et qu'un destinataire n'a pas justifié son inaction de façon appropriée.

Fait à Francfort-sur-le-Main, le 2 décembre 2021.

Le chef du secrétariat du CERS,
au nom du conseil général du CERS,
Francesco MAZZAFERRO

ANNEXE

PRÉCISION DES CRITÈRES DE CONFORMITÉ APPLICABLES AUX RECOMMANDATIONS

Recommandation A – Création d'un cadre paneuropéen de coordination des cyberincidents systémiques (EU-SCICF)

Pour la sous-recommandation A, paragraphe 1, les critères de conformité suivants sont précisés.

1. Lorsqu'elles préparent une réponse efficace et coordonnée au niveau de l'Union qui devrait impliquer la mise en place progressive de l'EU-SCICF en exerçant le pouvoir prévu dans le futur règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (ci-après « DORA »), les autorités européennes de surveillance (AES), agissant par l'intermédiaire du comité mixte et conjointement avec la Banque centrale européenne (BCE), le Comité européen du risque systémique (CERS) et les autorités nationales concernées, et en concertation avec l'Agence de l'Union européenne pour la cybersécurité et la Commission lorsque cela est jugé nécessaire, devraient envisager d'inclure dans la préparation envisagée pour l'EU-SCICF au moins les aspects suivants :

   a. analyse des ressources nécessaires pour une mise en place efficace de l'EU-SCICF ;

   b. mise au point d'exercices de gestion de crise et d'urgence impliquant des scénarios de cyberattaques en vue de développer des canaux de communication ;

   c. élaboration d'un vocabulaire commun ;

   d. élaboration d'une classification cohérente des cyberincidents ;

   e. mise en place de canaux de partage d'informations sûrs et fiables, y compris des systèmes de sauvegarde ;

   f. mise en place des points de contact ;

   g. traitement de la question de la confidentialité dans le partage d'informations ;

   h. initiatives de collaboration et de partage d'informations avec les services de cyberrenseignement du secteur financier ;

   i. élaboration de processus d'activation et de remontée de l'information efficaces par la connaissance de la situation ;

   j. clarification des responsabilités des participants au cadre ;

   k. élaboration d'interfaces pour la coordination intersectorielle et, le cas échéant, pour la coordination avec des pays tiers ;

   l. garantie d'une communication cohérente des autorités concernées avec le public afin de préserver la confiance ;

   m. mise en place de lignes de communication prédéfinies pour une communication en temps utile ;

   n. réalisation d'exercices appropriés afin de tester le cadre, y compris des tests interjuridictionnels et la coordination avec des pays tiers, et d'évaluations qui permettent de tirer des enseignements et de faire évoluer le cadre ;

   o. garantie d'une communication efficace et de contre-mesures contre la désinformation.

Recommandation B – Mise en place des points de contact de l'EU-SCICF

Pour la recommandation B, les critères de conformité suivants sont précisés.

1. Les AES, la BCE et chaque État membre – pour ces derniers, parmi leurs autorités nationales concernées – devraient convenir d'une approche commune pour partager et tenir à jour la liste des points de contact désignés de l'EU-SCICF.

2. La désignation du point de contact devrait être évaluée en tenant compte du point de contact unique que les États membres ont désigné, en vertu de la directive (UE) 2016/1148, aux fins de la sécurité des réseaux et des systèmes d'information pour assurer la coopération transfrontalière avec d'autres États membres et avec le groupe de coopération sur les réseaux et systèmes d'information (SRI).

Recommandation C – Modifications du cadre juridique de l'Union

Pour la recommandation C, le critère de conformité suivant est précisé.

La Commission devrait examiner si des mesures, y compris des modifications de la législation pertinente de l'Union, sont nécessaires à la suite de l'analyse effectuée conformément à la recommandation A afin de veiller à ce que les AES, par l'intermédiaire du comité mixte et conjointement avec la BCE, le CERS et les autorités nationales concernées, puissent mettre en place l'EU-SCICF conformément à la sous-recommandation A, paragraphe1, et que les AES, la BCE, le CERS et les autorités nationales concernées, ainsi que d'autres autorités, puissent prendre des mesures de coordination et échanger des informations suffisamment détaillées et cohérentes pour soutenir un EU-SCICF efficace.