Conseil de
l'Union européenne

Bruxelles, le 11 mars 2026
(OR. en)

7240/26

EF 66
ECOFIN 329
FSC 6
ESMA
ESRB
ECB
EIOPA
SRB
EBA

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2026) 119 final
Objet:	RAPPORT DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN sur la préparation dans le secteur financier de l'UE

Les délégations trouveront ci-joint le document COM(2026) 119 final.

p.j.: COM(2026) 119 final

COMMISSION
EUROPÉENNE

Bruxelles, le 10.3.2026
COM(2026) 119 final

RAPPORT DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN

sur la préparation dans le secteur financier de l'UE

1. Introduction

L'Union européenne est confrontée à des risques croissants et à des menaces sans précédent dans de nombreux secteurs. Ces risques vont de l'incertitude accrue, des tensions et conflits géopolitiques, des risques en matière de cybersécurité et de manipulation de l'information au changement climatique en passant par les risques croissants de catastrophes naturelles. Afin de renforcer la capacité de l'UE à anticiper ces menaces, à les prévenir et à y réagir, la Commission et le Service européen pour l'action extérieure (SEAE) ont présenté conjointement, le 26 mars 2025, la stratégie pour une union de la préparation[1]. Le secteur financier de l'UE joue un rôle essentiel dans le maintien de fonctions sociétales vitales en toutes circonstances. C'est pourquoi, dans le cadre de la stratégie pour une union de la préparation et de la mise en œuvre de l'action 25 de l'annexe de ladite communication conjointe, la Commission procède actuellement à une évaluation complète du niveau de préparation dans le secteur financier. En particulier, elle évalue la capacité du secteur à continuer d'exercer ses fonctions critiques, notamment effectuer des paiements et financer l'économie, en toutes circonstances.

La législation de l'UE sur les services financiers repose sur une solide tradition de prudence, de précaution, de résilience et d'anticipation. Ses objectifs sont clairs: préserver la stabilité financière, la résolution ordonnée des défaillances des établissements financiers, la gestion des crises et la garantie des dépôts, la protection des investisseurs et l'intégrité du marché. L'UE a achevé la révision complète de ses règles prudentielles et de son architecture de surveillance bancaire à la suite de la grande crise financière, qui avait été entreprise dès 2007. Ces réformes ont renforcé les établissements financiers de l'UE, ses marchés des capitaux et ses prestataires d'infrastructures de marchés financiers.

Aujourd'hui, le secteur financier de l'UE a atteint un niveau élevé de résilience grâce à la consolidation de trois piliers: i) des exigences de fonds propres fondées sur le risque pour les banques et les établissements financiers, ii) des exigences en matière de gouvernance et de transparence et iii) des mécanismes de coopération en matière de surveillance entre les États membres et entre les secteurs. L'UE a mis en place des politiques et des principes qui produisent des évaluations continues des risques d'événements extrêmes, dans les cadres de risque opérationnel ainsi que les plans de continuité des activités et les plans d'urgence.

Le cadre de l'UE a été mis à l'épreuve par plusieurs épisodes de crise ces dernières années, tels que la pandémie de COVID-19, l'agression menée par la Russie contre l'Ukraine, la crise bancaire régionale aux États-Unis et la crise du Crédit Suisse en 2023, des pannes d'électricité, des cyberattaques et des incidents hybrides. Face à ces crises, le secteur financier de l'UE a fait preuve de robustesse et de résilience. Les autorités à l'échelon de l'UE et à l'échelon national ont agi rapidement et efficacement.

De manière générale, la préparation n'est pas statique; c'est un état dynamique et tourné vers l'avenir. Elle nécessite un cycle continu de planification, de formation, d'équipement, de tests, d'évaluation et d'amélioration. Elle requiert une volonté de faire face à tous les dangers en

[1] La Commission et le SEAE ont publié une communication conjointe sur la stratégie pour une union de la préparation.

anticipant les risques, en développant les capacités, en assurant la coordination entre les secteurs (gouvernemental, privé, public) et en tirant les enseignements des événements passés afin de construire des communautés résilientes capables de prévenir les crises, de s'en protéger et de s'en relever si elles surviennent. Cela vaut également pour le secteur financier.

Le présent rapport donne une vue d'ensemble de l'état actuel de préparation du secteur financier de l'UE, sur la base de discussions continues avec la Banque centrale européenne, les autorités européennes de surveillance, le comité européen du risque systémique, le Conseil de résolution unique, les États membres et le secteur des services financiers.

2. Préparation dans le marché unique de l'UE

À l'échelle de l'UE, la préparation dans le secteur financier s'est améliorée au cours des dernières années grâce à des mesures législatives et à la création de structures de gouvernance au niveau de l'Union qui reflètent la nature transfrontière du secteur financier de l'UE. La gouvernance repose sur deux piliers: une réglementation de l'UE et des autorités de l'UE. Cette structure est complétée par une série de mesures prises au niveau de la zone euro, au niveau régional (impliquant plusieurs États membres) et au niveau des États membres.

2.1 Législation de l'UE régissant le secteur financier

Le secteur financier est régi à la fois par une législation sectorielle et par une législation transversale.

Législation sectorielle

La législation sectorielle comprend la directive et le règlement sur les exigences de fonds propres (CRD/CRR)[2], Solvabilité II[3], la directive révisée sur les marchés d'instruments financiers (MiFID II)[4], le règlement sur l'infrastructure du marché européen (règlement EMIR)[5] et le règlement sur les dépositaires centraux de titres (règlement sur les DCT)[6]. Ces actes législatifs mettent en place des exigences prudentielles visant à assurer la résilience, la stabilité et le bon fonctionnement des établissements financiers, des infrastructures financières et du système financier.

---

2 Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (CRD);
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 modifiant le règlement (UE) nº 648/2012 (CRR).

3 Texte consolidé: 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).

4 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 (MiFID II).

5 Règlement (UE) nº 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 (règlement EMIR).

6 Règlement (UE) nº 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) nº 236/2012.

Du point de vue de la préparation, plusieurs actes législatifs sectoriels régissent la gestion des risques opérationnels, la résilience opérationnelle, la résilience des TIC, la continuité des activités et la gestion des crises. Par exemple, dans le secteur bancaire, le CRR/la CRD, la directive relative au redressement des banques et à la résolution de leurs défaillances (directive BRRD)[7], le règlement sur le mécanisme de résolution unique (règlement MRU)[8] et la directive relative aux systèmes de garantie des dépôts (directive DGSD)[9] garantissent que les banques ont la résilience nécessaire pour résister à un large éventail de risques potentiels, y compris des événements extrêmes. Il est attendu des banques qu'elles mettent en œuvre des cadres robustes de gouvernance et de gestion des risques, y compris des plans renforcés de continuité des activités, de communication et de redressement, afin de faire face efficacement à un large éventail de risques. Les principales caractéristiques des mesures pour faire face aux scénarios de risque, prévues tant à titre de précaution qu'à titre réactif, comprennent des exigences ex ante spécifiques pour les banques, telles que des plans de redressement et de résolution, conformément aux dispositions du règlement MRU et de la directive BRRD.

Outre les banques, les entreprises d'assurance au titre de Solvabilité II, les entreprises d'investissement au titre de MiFID II et les infrastructures de marchés telles que les contreparties centrales (CCP) et les dépositaires centraux de titres sont soumis à des exigences similaires pour assurer leur résilience opérationnelle, leur gestion des risques liés TIC, la continuité de leurs activités et leur gestion des crises. Celles-ci sont complétées par des exigences de renforcement, le cas échéant, de la planification du redressement et de la résolution. La gestion d'actifs et l'intermédiation financière non bancaire font également l'objet d'un cadre réglementaire de l'UE large et de plus en plus complet, comprenant la directive sur les organismes de placement collectif en valeurs mobilières (directive OPCVM), la directive sur les gestionnaires de fonds d'investissement alternatifs (directive GFIA) et le règlement sur les fonds monétaires (règlement MMF). Ces instruments imposent des exigences en matière de gestion des risques, de gestion de la liquidité, d'effet de levier, de valorisation et de transparence, afin de favoriser la stabilité du secteur. Les mesures visant à développer l'union de l'épargne et des investissements (UEI) en renforçant la capacité du secteur financier de l'UE à mettre en lien l'épargne avec les investissements productifs, améliorant ainsi le partage et la diversification des risques dans l'ensemble du secteur financier de l'UE, amélioreront sa résilience et sa préparation globales.

La Banque centrale européenne (BCE), qui est l'autorité de surveillance unique des banques dans 21 États membres, et les autorités nationales compétentes à l'intérieur et à l'extérieur de

---

7 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 (directive BRRD).

8 Règlement (UE) nº 806/2014 du Parlement européen et du Conseil du 15 juillet 2014 établissant des règles et une procédure uniformes pour la résolution des établissements de crédit et de certaines entreprises d'investissement dans le cadre d'un mécanisme de résolution unique et d'un Fonds de résolution bancaire unique, et modifiant le règlement (UE) nº 1093/2010 (règlement MRU).

9 Directive 2014/49/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux systèmes de garantie des dépôts (directive DGSD).

la zone euro placent la résilience financière et opérationnelle des banques au centre de leurs priorités en matière de surveillance. Les banques sont notamment encouragées à tenir dûment compte des risques géopolitiques et à les intégrer dans leurs processus de gestion des risques. Les expositions sur des contreparties de pays tiers, les incidences potentielles des sanctions étrangères sur les expositions et les dépendances à l'égard de prestataires de services et d'infrastructures externes devraient être prises en considération par les banques dans ce contexte. En outre, les banques devraient mettre en place un cadre de gouvernance robuste et une protection contre les cybermenaces et les autres menaces susceptibles de nuire à leur résilience opérationnelle. Il s'agit notamment de mesures visant à renforcer la sécurité et la protection contre les dommages physiques. Au-delà des mesures propres aux établissements, le cadre prudentiel bancaire de l'UE couvre également des canaux de risque plus larges, systémique et transfrontières.

Le cadre de gestion des crises crée une boîte à outils à utiliser lorsque la viabilité du prestataire d'une fonction critique est menacée. Le cadre révisé pour la gestion des crises bancaires et la garantie des dépôts, sur lequel un accord politique a été conclu en juin 2025, constitue une étape importante pour rendre le système de gestion des crises de l'UE encore plus efficace, en particulier pour les banques de petite et de moyenne taille.

Un aspect important de la préparation dans le secteur financier est la disponibilité d'instruments de paiement pour le public, qu'il s'agisse de paiements en espèces ou de paiements électroniques. Afin de garantir la disponibilité des **espèces** en toutes circonstances, au niveau de l'Eurosystème, une mesure essentielle consiste à maintenir des stocks stratégiques communs de billets en euros. La BCE est l'organe central de coordination et de décision et organise des exercices périodiques de gestion des crises, incluant la communication de crise potentielle. Au niveau national, les banques centrales nationales (BCN) maintiennent des plans de continuité des activités afin de garantir que les retraits d'espèces et les dépôts restent disponibles.

En parallèle, la proposition sur le cours légal des billets et pièces en euros, présentée par la Commission le 28 juin 2023, vise à faire en sorte que les espèces en euros restent largement acceptées comme moyen de paiement et soient faciles à obtenir pour les citoyens, les entreprises et les entités publiques dans l'ensemble de la zone euro. Les exigences visant à maintenir une infrastructure de gestion des espèces saine en temps normal favorisent la disponibilité d'espèces en situation d'urgence. La proposition de la Commission ne comportait pas de disposition sur la résilience, mais le Conseil l'a ajoutée dans son mandat de négociation, qui exige des États membres qu'ils mettent en place un plan de résilience en matière d'espèces ou une combinaison de mesures équivalentes.

En outre, la troisième directive sur les services de paiement (DSP3), sur laquelle un accord politique a été conclu en novembre 2025, vise à renforcer l'accès à l'argent liquide dans les magasins en permettant aux détaillants de proposer un service de retraits d'espèces sans achat (*cash-in-shop*), jusqu'à un certain montant. Cela rend l'utilisation des espèces plus pratique, en particulier dans les zones rurales, en clarifiant les règles applicables aux détaillants et aux opérateurs de distributeurs automatiques de billets.

Outre la disponibilité des espèces, il est essentiel de maintenir la continuité des **services de paiement**, y compris les paiements par carte, les paiements fondés sur des opérations de compte à compte (y compris par téléphone mobile), l'accès aux comptes de paiement et la possibilité d'effectuer des dépôts, afin de maintenir la confiance du public dans le système financier, de maintenir l'ordre public et d'assurer le fonctionnement de base de l'économie en cas de perturbation généralisée en fournissant au public un accès ininterrompu aux services de base.

La deuxième directive sur les services de paiement (DSP2), en vigueur, réglemente d'autres aspects, notamment la gestion des risques opérationnels et de sécurité et le signalement des incidents majeurs. L'objectif est de renforcer la sécurité et la résilience des systèmes de paiement dans l'ensemble de l'UE.

L'Eurosystème promeut la sécurité et l'efficacité des systèmes de paiement. Il a mis en place des exigences de supervision pour faire face aux principaux scénarios de risque recensés pour l'écosystème européen des paiements. Ces cadres définissent un ensemble exhaustif d'exigences en matière de gestion des risques opérationnels. Il s'agit notamment de mesures de gestion de la continuité des activités et de reprise rapide, ainsi que de dispositions spécifiques en matière de sécurité de l'information, de cyberrésilience, de sécurité physique, d'externalisation, de gestion des risques informatiques, ainsi que dans d'autres matières connexes. Le cadre couvre les instruments de paiement électronique (tels que les cartes, les prélèvements, les virements, la monnaie électronique et les portefeuilles numériques), ainsi que les systèmes (par exemple les réseaux de cartes) et les applications (par exemple les portefeuilles électroniques) qui permettent leur utilisation.

Afin de renforcer la protection, l'article 15 du règlement de la BCE sur les systèmes de paiement d'importance systémique (SPIS) énonce d'autres exigences. Par exemple, il exige que les systèmes reprennent leur fonctionnement normal dans un délai de deux heures (y compris grâce à l'utilisation de sites secondaires) et que les opérateurs de SPIS soient en mesure d'effectuer avant la fin du jour ouvrable l'intégralité des règlements dus le jour au cours duquel l'incident s'est produit.

Le projet de création d'un euro numérique – une forme numérique d'espèces, complétant les espèces physiques et les solutions de paiement privées – donnerait au public un mode de paiement supplémentaire, tout en favorisant l'inclusion numérique et financière. En tant que premier système de paiement paneuropéen unifié, l'euro numérique contribuerait également à préserver le rôle international de l'euro. En renforçant l'autonomie stratégique ouverte de l'UE et en élargissant l'éventail des instruments de paiement disponibles, le projet d'euro numérique vise à renforcer encore la résilience globale des services de paiement. En ce qui concerne la proposition relative au cours légal, le Conseil a ajouté des dispositions supplémentaires pour renforcer encore la résilience de l'euro numérique. Dans ce contexte, les portefeuilles européens

d'identité numérique (EUDI) seront interopérables avec les interfaces utilisateur de l'euro numérique, ce qui garantira une authentification sûre et fluide des utilisateurs[10].

Législation transsectorielle dans le secteur financier

Complétant la législation financière mise en évidence ci-dessus, le règlement sur la résilience opérationnelle numérique du secteur financier (règlement DORA) est un acte législatif sectoriel qui s'applique à l'ensemble du secteur financier de l'UE. Il couvre 20 types différents d'entités financières, dont les établissements de crédit, les prestataires de services de paiement, les infrastructures de marchés financiers, les entreprises d'assurance, les agences de notation de crédit et les gestionnaires d'actifs.

Le règlement DORA met fortement l'accent sur la résilience des entités financières, sur leur niveau de préparation pour faire face à d'éventuelles perturbations dans le domaine des TIC et sur la gestion des risques qui découlent de la dépendance des entités financières à l'égard des prestataires tiers de services TIC, dont les risques systémiques et les risques de concentration posés par les prestataires de services TIC critiques pour le secteur financier de l'UE. Le règlement DORA établit un cadre harmonisé et robuste pour renforcer la capacité du secteur financier de l'UE de prévenir les perturbations liées aux TIC, d'y résister, d'y réagir et de s'en remettre. Les entités financières doivent mettre en place un cadre global de gestion des risques liés aux TIC, incluant la gouvernance, l'inventaire des actifs, l'identification des risques, la protection, la détection, la réaction, le rétablissement et l'amélioration continue. Ainsi, les vulnérabilités et la résilience des systèmes et des processus seront gérés de manière proactive. Les entités financières sont également tenues de détecter les incidents majeurs liés aux TIC, de les classer et de les signaler aux autorités compétentes en utilisant des définitions, des seuils et des délais convenus, afin de permettre des réponses coordonnées entre les pays. Le règlement DORA impose des évaluations et des tests réguliers des processus, outils et dispositifs de résilience et de préparation des entités.

Les entités financières doivent également gérer les risques associés au recours à des prestataires tiers de services TIC, et en particulier à des prestataires tiers critiques. Le règlement DORA impose aux entités financières de faire preuve de la diligence requise en ce qui concerne le risque de concentration avant de conclure de nouveaux contrats avec des tiers prestataires de services TIC. Le règlement DORA inclut un cadre de supervision, en vertu duquel les trois autorités européennes de surveillance (AES)[11]sont le superviseur des prestataires tiers critiques de services TIC, à l'échelle paneuropéenne, renforçant ainsi la résilience opérationnelle numérique globale dans l'ensemble du secteur financier de l'UE. En novembre 2025, les AES

[10] Le cadre européen relatif à une identité numérique établit un écosystème sûr et fiable pour l'identification et l'authentification numériques ainsi que l'utilisation de preuves numériques, qui sera mis à la disposition de tous les citoyens de l'UE d'ici à la fin de 2026. Les portefeuilles européens d'identité numérique contribueront directement à la résilience et à la préparation du secteur financier de l'UE face aux crises, par la protection contre la fraude et l'usurpation d'identité dans les paiements, l'entrée en relation avec le client et d'autres services financiers.

[11] Les trois AES sont l'Autorité bancaire européenne (ABE), l'Autorité européenne des assurances et des pensions professionnelles (AEAPP) et l'Autorité européenne des marchés financiers (AEMF).

ont publié la liste des prestataires tiers de services TIC désignés comme critiques conformément au règlement DORA. Le cadre DORA est particulièrement bien adapté pour gérer la cybersécurité, la connectivité, la préparation et les risques opérationnels revêtant une forte dimension internationale.

Outre le règlement DORA, qui est une *lex specialis* pour le secteur financier, ce secteur est également couvert par des accords de coopération horizontale sur la résilience physique et numérique au titre de la directive sur la résilience des entités critiques (directive CER) [12]et de la directive SRI 2.

La directive CER crée un cadre général qui traite de la résilience des entités critiques en ce qui concerne tous les dangers. Elle impose des évaluations des risques, des stratégies nationales et des mesures de résilience spécifiques pour les entités désignées comme critiques afin de veiller à ce qu'elles puissent continuer à assurer des fonctions sociétales vitales. Bien que la directive CER inclue le secteur bancaire et les infrastructures de marchés financiers parmi les secteurs critiques, le secteur financier est hors du champ d'application de toutes ses exigences de fond, étant donné qu'il est couvert par des dispositions beaucoup plus spécifiques au titre du règlement DORA. Le secteur financier demeure néanmoins dans le champ d'application de la directive CER pour les accords de coopération horizontale.

La directive SRI 2 fournit un cadre plus large pour la cybersécurité, qui couvre différents secteurs critiques. Le règlement DORA est considéré comme une *lex specialis* par rapport à la directive SRI 2, ce qui signifie que les exigences relatives à la gestion des risques et à la notification des incidents énoncées dans le règlement DORA s'appliquent en tant qu'acte juridique sectoriel de l'Union au lieu des dispositions de la directive SRI 2. Comme indiqué par la Commission dans ses lignes directrices sur l'application de l'article 4, paragraphes 1 et 2, de la directive SRI 2[13], certaines dispositions énoncées dans ladite directive qui sont essentielles pour assurer la préparation et atteindre un niveau élevé de résilience des entités financières continuent de s'appliquer, notamment les exigences relatives à l'adoption d'une stratégie de cybersécurité et à l'établissement d'un cadre national relatif à la gestion des crises de cybersécurité (avec obligation de désigner des autorités de gestion des crises de cybersécurité et d'adopter des plans nationaux de réaction aux crises et incidents de cybersécurité majeurs) qui couvrent les secteurs des banques et des infrastructures de marchés financiers. En outre, les centres de réponse aux incidents de sécurité informatiques (CSIRT) et le réseau européen d'organisations de liaison en cas de crises de cybersécurité (EU-CyCLONe) devraient s'acquitter de leurs tâches en ce qui concerne ces deux secteurs.

Les mesures de préparation décrites pour le secteur financier sont conçues pour trouver un équilibre entre le besoin de résilience et le principe de proportionnalité. Les exigences réglementaires et de surveillance sont adaptées à la taille, à la complexité et à l'importance systémique des établissements afin de ne pas imposer une charge disproportionnée aux petites

---

[12] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil. L'article 5, paragraphe 5, de la directive prévoit que la Commission, en coopération avec les États membres, élabore un modèle commun facultatif de rapport aux fins du respect du paragraphe 4 dudit article.

[13] C(2023) 6068.

entités. Pour éviter une charge administrative inutile, les cadres harmonisés tels que DORA rationalisent les exigences dans l'ensemble du secteur, en assurant la cohérence tout en réduisant les doubles emplois.

2.2 Autorités de l'UE: outils et coopération

Les autorités de l'UE se voient confier des outils spécifiques qui peuvent être activés dans des situations d'urgence et qui maintiennent des dispositifs de préparation afin d'assurer la continuité des activités. Par exemple, les trois AES se sont vu attribuer des pouvoirs d'urgence en vertu de leurs règlements fondateurs. Dès qu'une situation d'urgence est officiellement constatée par le Conseil (en vertu de l'article 18 des règlements instituant les AES), ces autorités peuvent restreindre temporairement les activités financières visées à l'article 9 par des décisions individuelles. Elles exercent également une fonction de coordination générale entre les autorités nationales et au sein du système européen de surveillance financière (SESF) (article 31).

Comme indiqué ci-dessus, la BCE est l'autorité de surveillance unique pour les banques des 21 États membres qui participent au mécanisme de surveillance unique, ce qui assure une surveillance prudentielle cohérente dans l'ensemble de la zone. Le Conseil de résolution unique est l'autorité de résolution unique pour ces États membres, responsable de la résolution ordonnée des défaillances bancaires, préservant ainsi la stabilité financière et réduisant au minimum les coûts pour les contribuables.

Afin de renforcer la résilience opérationnelle, toutes les autorités de l'UE ont mis au point des procédures internes en matière de continuité des activités, de dispositifs de préparation et de gestion des incidents critiques afin de faire face à divers dangers. Elles testent régulièrement ces mesures afin d'assurer la continuité des activités et de déterminer quels sont les processus opérationnels prioritaires à mettre en œuvre en cas d'urgence, et à quel niveau.

Compte tenu de la nécessité de préserver l'intégrité et le bon fonctionnement du marché unique et du degré élevé d'interconnexion et de risque d'effets d'entraînement dans le secteur financier de l'UE, la coordination entre les différentes autorités de l'UE et la participation des États membres sont essentielles pour anticiper et gérer les crises susceptibles de toucher simultanément plusieurs régions de l'UE. Une participation précoce et une coopération rapide sont essentielles tant lors de la phase de planification qu'à chaque stade de la crise. Afin de faciliter la coopération et l'échange d'informations qui peuvent également être pertinents en cas de crise, plusieurs autorités de l'UE ont mis en place des instruments de coopération entre elles ou avec les autorités nationales compétentes ou les autorités nationales de résolution, ou ont conclu des protocoles d'accord (par exemple le protocole d'accord entre la BCE et le CRU); elles procèdent également à des exercices de simulation pour assurer une préparation adéquate aux crises.

Une étape importante dans ces travaux est le cadre de l'Union européenne pour la coordination des cyberincidents systémiques (EU-SCICF), établi en janvier 2025 par les AES. Ce cadre

fournit une base stratégique pour la coopération lors d'incidents de cybersécurité importants[14] Il vise à faciliter le partage rapide d'informations et les réponses conjointes en mettant en place des protocoles pour évaluer et atténuer les menaces dans l'ensemble des États membres de l'UE.

En outre, le Conseil a adopté en juin 2025 un schéma directeur pour la gestion des crises de cybersécurité[15], qui constitue un guide important pour les États membres en ce qui concerne l'amélioration de leur préparation, de leurs capacités de détection et de leur réaction aux incidents de cybersécurité, sur la base de tous les mécanismes pertinents, y compris ceux créés par la directive SRI 2, le règlement DORA (EU-SCICF) et le règlement sur la cybersolidarité.

Des exercices réguliers peuvent être menés dans ce cadre pour veiller à ce que la préparation et les capacités de réaction restent robustes et efficaces. En outre, au niveau international, le protocole de réponse aux incidents de cybersécurité du G7 vise à unifier les efforts mondiaux de réaction aux menaces en matière de cybersécurité qui ont une incidence sur le secteur financier et à assurer des réactions rapides et coordonnées entre les pays et territoires.

Chaque autorité de l'UE procède régulièrement à des évaluations des risques et prend d'autres mesures pour identifier les risques les plus pertinents par rapport à son mandat et à ses fonctions. Les évaluations des risques sont réalisées en coopération avec les autorités nationales, ce qui contribue à développer une compréhension commune et plus approfondie du paysage des risques et des risques auxquels il convient de donner la priorité. Les évaluations des risques alimentent souvent les systèmes d'alerte précoce, qui font eux-mêmes partie des cadres de préparation des autorités de l'UE. En outre, les dispositifs en matière de réglementation et de surveillance existant entre les autorités de l'UE et les parties prenantes du secteur privé permettent un dialogue continu sur les attentes réciproques en matière de préparation[16].

2.3 Cadres aux échelons national et régional

Outre la législation au niveau de l'UE, les États membres ont élaboré leurs propres programmes nationaux de préparation[17]. Ces programmes vont généralement au-delà du secteur financier et couvrent la préparation de la société dans son ensemble à l'échelle nationale. Pour cette raison, les programmes nationaux diffèrent d'un État membre à l'autre, reflétant les différences entre structures gouvernementales et administratives nationales, ainsi qu'au niveau de l'étendue de leurs compétences. Dans le même temps, ces systèmes nationaux fonctionnent dans un cadre cohérent à l'échelle de l'UE et interagissent de plus en plus avec les dispositifs et les mécanismes de coordination transfrontière de l'UE.

---

14 L'EU-SCICF met également en œuvre l'article 49 du règlement DORA dans le but de renforcer la coordination avec d'autres cadres de crise de l'UE.

15 Recommandation du Conseil du 6 juin 2025 sur un schéma directeur de l'UE pour la gestion des crises de cybersécurité, *JO C, C/2025/3445, 20.6.2025*, http://data.europa.eu/eli/C/2025/3445/oj.

16 La stratégie européenne pour une union de la préparation reconnaît l'importance de ces partenariats. Ses actions clés 36 et 37 visent à mettre en place une task-force public-privé en matière de préparation et à élaborer des protocoles d'urgence public-privé dans tous les secteurs.

17 Dans le cadre de ses travaux visant à mettre en œuvre le mandat de l'action 25 de l'annexe de la communication conjointe sur la stratégie pour une union de la préparation, la Commission s'est également appuyée sur des discussions continues avec les États membres sur les programmes de préparation.

La préparation du secteur financier est toujours un élément clé des stratégies nationales de préparation. Ce secteur, qui joue un rôle de premier plan en matière de préparation, est un exemple à suivre pour d'autres secteurs. Les stratégies nationales de préparation du secteur financier vont au-delà de l'acquis de l'UE et mettent l'accent sur des questions opérationnelles nationales. Les différences entre les systèmes financiers nationaux (par exemple: principales caractéristiques du secteur bancaire national, ampleur de l'utilisation des espèces, adoption de l'euro, participation à l'union bancaire) se reflètent naturellement dans la manière dont le niveau de préparation national du secteur financier est évalué et assuré.

Compte tenu du rôle central joué par les pouvoirs publics, en particulier en cas de crise ou d'incident majeur, des fonctions fiables de financement à court terme doivent rester disponibles afin d'éviter des pénuries de liquidités ou de financement au niveau de l'État et du secteur public au sens large, et d'éviter des répercussions plus vastes sur la société en termes de confiance du public et de stabilité financière. Toutefois, cela ne s'applique pas de la même manière à tous les cadres de crise: en particulier, la résolution des défaillances bancaires est conçue pour limiter le recours aux fonds publics, au moyen de mécanismes de renflouement interne et de mécanismes de résolution financés par le secteur.

Afin d'assurer la résilience des fonctions de financement à court terme des gouvernements, les bureaux nationaux de gestion de la dette (BGD) ont élaboré des plans d'urgence et de continuité des activités afin de continuer à fonctionner également en cas de crise. Ces dispositifs sont de plus en plus souvent complétés par des échanges de bonnes pratiques et une coordination tant à l'échelon de l'UE qu'à l'échelon régional.

En outre, le mécanisme européen de stabilité (MES) propose plusieurs instruments destinés à préserver la stabilité financière en apportant une assistance financière aux membres du MES, afin de renforcer la capacité de la zone euro à gérer les difficultés des émetteurs souverains et des banques. Ces instruments sont destinés à faire face aux crises systémiques et à compléter la préparation opérationnelle des États membres et de l'UE à des scénarios de perturbation plus tangibles. Certains États membres ont mis au point des accords bilatéraux pour assurer la disponibilité d'un financement à court terme en cas d'indisponibilité de l'une des fonctions de base du BGD. La modification du traité instituant le MES est en suspens; sa finalisation renforcerait encore le filet de sécurité de la zone euro.

Parallèlement, il existe des enceintes de coordination régionale, telles que le mécanisme de coopération nordique-baltique, une importante initiative régionale axée sur les pays de la mer Baltique. Ces enceintes favorisent la collaboration en matière de surveillance financière et de gestion des crises, les échanges d'informations sur les évaluations des risques et la planification stratégique. Elles illustrent la manière dont la coopération régionale peut améliorer la préparation.

Plusieurs États membres ont mis en place des partenariats ou des enceintes de discussion public-privé spécifiques dans le cadre de leurs programmes nationaux de préparation (avec la participation de représentants du secteur privé de plusieurs secteurs).

Dans l'ensemble, ces dispositifs à l'échelon de l'UE, à l'échelon régional et à l'échelon national font partie d'un cadre de préparation à plusieurs niveaux, dans lequel la coordination et la coopération européennes et régionales sont complétées par des actions nationales.

3. Tests de résistance

Les tests de résistance constituent un aspect essentiel de la préparation, comme le Conseil le reconnaît dans sa recommandation relative au renforcement de la résilience des infrastructures critiques[18]. Dans le secteur financier, les tests de résistance constituent déjà une partie intégrante et essentielle de la surveillance des établissements financiers et des prestataires d'infrastructures de marchés financiers. Les tests de résistance renforcent la préparation du secteur financier en simulant des crises graves (telles que des récessions, des chocs climatiques ou des cyberattaques) afin de mettre au jour les vulnérabilités des établissements financiers en matière de fonds propres et de liquidité. Cela oblige les établissements et les prestataires à améliorer leur gestion des risques, à renforcer leurs coussins de fonds propres, à affiner leur planification stratégique et à renforcer leur résilience face aux chocs futurs, ce qui renforce la stabilité financière globale et la confiance des marchés.

Les tests de résistance contribuent également à la préparation en révélant des canaux de risque systémiques et transfrontières, notamment les sources d'instabilité financière mondiale, les tensions géopolitiques, les cyberincidents et les perturbations des infrastructures critiques.

En ce qui concerne le **système bancaire**, l'Autorité bancaire européenne (ABE) est habilitée à lancer et à coordonner des tests de résistance du secteur bancaire à l'échelle de l'Union. Sur la base de ce mandat, l'ABE effectue tous les deux ans un test de résistance à l'échelle de l'UE couvrant environ 75 % du secteur bancaire. La CRD impose également aux autorités compétentes d'effectuer des tests de résistance prudentiels sur les établissements qu'elles surveillent, selon le cas mais au moins une fois par an. En outre, l'ABE a publié des orientations visant à ce que les autorités utilisent une méthode commune lorsqu'elles effectuent leurs tests de résistance prudentiels annuels.

Au sein de l'union bancaire, la BCE effectue régulièrement des tests de résistance, des analyses de scénarios et des simulations afin d'éclairer le processus de contrôle et d'évaluation prudentiels. La BCE procède également à des examens ciblés des accords de cyberrésilience et d'externalisation.

Dans le secteur **des assurances et des fonds de pension professionnels**, l'AEAPP effectue régulièrement, tous les trois ans, des tests de résistance à l'échelle de l'UE pour les entreprises d'assurance et de réassurance et pour les institutions de retraite professionnelle (IRP)[19], avec une composante "cyberrisque" et une composante "risque climatique".

---

[18] Recommandation du Conseil du 8 décembre 2022 relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques (2023/C 20/01).

[19] Dans plusieurs États membres, les institutions de retraite professionnelle ne relèvent pas du champ d'application de la directive IRP II et ne sont donc pas soumises aux règles de l'UE. De tels fonds de pension ne sont pas soumis aux tests de résistance de l'AEAPP.

L'Autorité européenne des marchés financiers (AEMF) effectue régulièrement des tests de résistance à l'échelle de l'UE portant sur la résilience des contreparties centrales, dans le cadre des évaluations prévues à l'article 32 du règlement instituant l'AEMF et à l'article 24 *bis* du règlement EMIR. Bien que ces tests se concentrent sur la résilience des contreparties centrales face à des évolutions négatives des marchés, l'AEMF y inclut également d'autres types de risques exogènes.

Le comité européen du risque systémique (CERS) élabore des scénarios défavorables pour les tests de résistance menés par l'ABE (banques), par l'AEAPP (assurances, fonds de pension) et par l'AEMF (contreparties centrales).

La directive 2014/49/UE relative aux systèmes de garantie des dépôts (SGD) impose aux États membres de s'acquitter des tâches qui leur incombent en vertu de la directive. Les résultats de ces tests sont ensuite utilisés par l'ABE pour réaliser des examens par les pairs afin d'examiner la résilience des SGD.

4. Perspectives

La préparation du secteur financier de l'UE repose sur un cadre solide et multidimensionnel. Ce cadre se compose d'une législation sectorielle spécifique, d'une législation transversale et de mécanismes de coopération entre les secteurs et entre les États membres. La préparation du secteur financier de l'UE comporte également une dimension extérieure, par laquelle l'UE renforce non seulement sa stabilité financière, mais aussi son rôle en tant qu'entité dotée d'un secteur financier fiable et crédible au niveau mondial.

Le secteur financier de l'UE a fait la preuve de sa résilience lors de crises passées. Il a prouvé sa capacité à résister aux tempêtes qu'ont été la pandémie de COVID-19, l'agression menée par la Russie contre l'Ukraine, les crises financières dans d'autres pays et territoires, les cyberattaques et de nombreux autres épisodes.

Cependant, compte tenu des menaces sans précédent et de l'environnement géopolitique plus incertain auquel l'UE est confrontée, il importe d'évaluer en permanence le niveau de préparation du secteur financier de l'UE. L'UE poursuit ces travaux et pourrait engager toute adaptation nécessaire pour garantir des actions préventives et réactives rapides, concertées et proportionnées, tant à l'échelon de l'UE qu'à l'échelon des États membres, en vue de maintenir fermement le cap et de préserver les fonctions vitales du secteur financier de l'UE. À l'avenir, le développement de l'union de l'épargne et des investissements et l'introduction de l'euro numérique devraient renforcer la résilience globale du secteur financier de l'UE et améliorer encore son niveau de préparation.