GROUPE DE PLACE ROBUSTESSE
LES 20 ANS DU GROUPE (2005-2025)
Mieux se préparer aux crises et renforcer la résilience opérationnelle de Place

FÉVRIER 2025

BANQUE DE FRANCE
EUROSYSTÈME

GROUPE DE PLACE ROBUSTESSE
LES 20 ANS DU GROUPE (2005-2025)
Mieux se préparer aux crises et renforcer la résilience opérationnelle de Place

FÉVRIER 2025

AVANT-PROPOS

Le Groupe de Place Robustesse : une instance qui reflète la maturité du secteur financier français en matière de résilience

Intensification des menaces cyber dans un contexte de tensions géopolitiques, multiplication des événements climatiques extrêmes, mais aussi défis opérationnels relevés avec succès par le secteur financier à l'occasion des Jeux olympiques et paralympiques de Paris, etc. : l'année 2024 a, une fois de plus, mis en lumière ***l'environnement opérationnel complexe et incertain*** *dans lequel le secteur financier français évolue.*

Face à la diversité de ces risques, la capacité collective du secteur à anticiper, à se coordonner et à rebondir après un incident majeur, ***et donc à renforcer sa résilience opérationnelle****, est plus cruciale que jamais. S'il relève des superviseurs de continuer à* ***renforcer la solidité individuelle des institutions financières****, dans le cadre du dialogue réglementaire établi avec chaque acteur financier, l'ambition du* ***Groupe de Place Robustesse****, qui existe depuis 2005, est, dans une démarche coopérative, de prendre en compte les* ***interdépendances opérationnelles*** *qui unissent l'ensemble de notre écosystème.*

Le secteur financier est caractérisé par un ***tissu dense d'interconnexions financières et technologiques*** *qui reposent sur l'existence de nœuds critiques – qu'il s'agisse des intermédiaires financiers, des infrastructures de marchés financiers ou des prestataires de services essentiels – et qui créent, de fait, un fort* ***potentiel de contagion****. Une perturbation au sein d'une entité peut en effet rapidement se propager et avoir des répercussions importantes sur l'ensemble du système financier. L'anticipation, la gestion et la réduction de ces risques opérationnels, à travers des* ***actions de coordination et de partage d'informations****, s'inscrivent donc pleinement dans la* ***mission de stabilité financière de la Banque de France****.*

C'est dans cet esprit que le Groupe de Place Robustesse a été créé. Ce Groupe se distingue par sa ***gouvernance****, qui repose sur une coopération des membres, et sa* ***structure****, qui rassemble* ***des acteurs publics et privés****, ce qui lui confère une grande richesse de perspectives et d'expertises – la* ***Banque de France agissant comme facilitatrice des échanges****.*

À l'instar d'une équipe, nous avons établi ces dernières années les grands axes de notre coopération, articulée sur la confiance, le partage et les entraînements collectifs. Lors d'une crise opérationnelle majeure, l'intégrité et la stabilité du secteur reposent sur ***la possibilité pour les participants d'échanger en temps utile des informations pertinentes et de coordonner leur réponse ou leur communication de crise****. L'instauration d'un contexte de confiance constitue un prérequis à ce partage, tout comme la conduite répétée d'exercices de gestion de crise, dont le dernier en 2024 a porté sur un scénario de cyberattaque. L'ensemble de ces travaux se distingue des missions de supervision prudentielle, en raison de leur* ***approche collaborative fondée sur le volontariat****, axée sur la préparation collective et la résilience sectorielle globale.*

Au-delà de la Place financière de Paris, la ***dimension transfrontalière de plusieurs des risques opérationnels****, comme le risque cyber, appelle la mise en place de mécanismes de gestion coordonnés entre les juridictions pour endiguer la contagion et atténuer les impacts potentiels sur l'ensemble du système financier international. Nous veillons par conséquent à* ***densifier en continu nos liens de coopération avec nos homologues à l'étranger****.*

Notre Groupe a désormais 20 ans et son évolution constante depuis 2005 témoigne de la ***maturité du secteur en matière de résilience opérationnelle****. C'est un effort collectif et toujours renouvelé du Groupe de Place Robustesse qui doit permettre de pérenniser cette résilience au cours des prochaines années.*

Emmanuelle Assouan*,*
Directrice générale de la Stabilité financière
et des Opérations à la Banque de France
Présidente du Groupe de Place Robustesse

SOMMAIRE

1

LE GROUPE DE PLACE ROBUSTESSE : UNE COLLABORATION PUBLIC-PRIVÉ EFFICACE DEPUIS VINGT ANS

1.1 Un groupe créé pour renforcer la résilience opérationnelle du secteur financier

Afin de faire face aux différentes menaces opérationnelles auxquelles elle pourrait être confrontée, la Place financière de Paris s'est dotée, dès 2005, d'une instance destinée à renforcer sa résilience, le **Groupe de Place Robustesse (GPR)**. Créé à l'initiative de la Banque de France dans le cadre de sa mission de stabilité financière, le GPR vise, par des actions de coordination et de partage d'informations, à éviter qu'une crise opérationnelle majeure ne bloque durablement le fonctionnement du système financier.

Au-delà du renforcement de la **robustesse** du secteur financier, c'est-à-dire de sa capacité à résister à des chocs externes, l'action du GPR se concentre sur l'amélioration de la **résilience** de Place, à savoir sa capacité à absorber les impacts d'une perturbation exogène et à rebondir pour assurer la continuité des services financiers critiques.

Depuis sa création, le Groupe s'est attaché à identifier et à anticiper les **menaces opérationnelles** auxquelles le secteur financier peut être exposé. Si le risque cyber demeure prégnant depuis plusieurs années, les tensions géopolitiques, les pandémies, les évènements climatiques majeurs, les contextes socioéconomique et politique dégradés ou encore la défaillance d'un prestataire critique représentent autant de risques exogènes sous surveillance.

Présidé par la directrice générale de la Stabilité financière et des Opérations de la Banque de France, le GPR a la singularité d'associer à la fois des **acteurs du secteur public et du secteur privé** :

- **les établissements de crédit et assimilés** (BNP Paribas, Crédit Agricole, BPCE, La Banque Postale, Crédit Mutuel, Société Générale, Caisse des dépôts et consignations, HSBC Continental Europe) ;
- les infrastructures de marché (LCH SA, Euronext, Euroclear, STET, Groupement des Cartes Bancaires, ABE Clearing) ;
- **la Banque de France** ;
- **les autorités de supervision et de régulation** : Autorité de contrôle prudentiel et de résolution (ACPR), Autorité des marchés financiers (AMF) ;
- **le Haut fonctionnaire de défense et de sécurité du ministère de l'Économie et des Finances** ;
- **la direction générale du Trésor** ;
- **l'Agence nationale de la sécurité des systèmes d'information** (Anssi) ;
- **la Fédération bancaire française** ;
- les présidents des quatre **cellules de crise de Place** (communication, fiduciaire, liquidité et moyens de paiement scripturaux), réunissant des professionnels des différentes entités membres du GPR et de la Banque de France autour de ces thématiques centrales pour le secteur financier lors d'une crise.

La Banque de France pilote et anime le Groupe. Elle **facilite ainsi les échanges** au sein du dispositif et assure son évolution.

Missions opérationnelles et fonctionnement

Les missions opérationnelles du GPR s'articulent autour de deux phases :

- **Hors crise (ou hors incident)** : une phase d'anticipation et de préparation à la gestion de crise, en particulier au travers de la réalisation d'exercices de simulation de crises opérationnelles majeures et d'actions de sensibilisation. Les exercices, organisés annuellement, contribuent à éprouver le dispositif de gestion de crise ;
- **En crise (ou lors d'un incident)** : une phase de gestion de crise en tant que telle, qui comprend le diagnostic de la situation, la coordination des décisions de gestion de crise (si cela est pertinent) et l'éventuelle prise de décisions communes.

Dans les deux temps, une phase de retour d'expérience contribue à l'**amélioration continue** du dispositif de gestion de crise.

Le fonctionnement du GPR repose sur une structure dédiée, le **Pôle de coordination** *(cf. schéma 1)*. Piloté par la Banque de France, celui-ci regroupe l'ensemble des membres du GPR et s'appuie notamment sur les quatre cellules de crise de Place. Ces cellules sont autonomes par rapport au Pôle, mais se coordonnent étroitement avec ce dernier en cas de crise opérationnelle. Les présidents des cellules sont membres à part entière du Pôle de coordination, ce qui favorise un échange régulier d'informations.

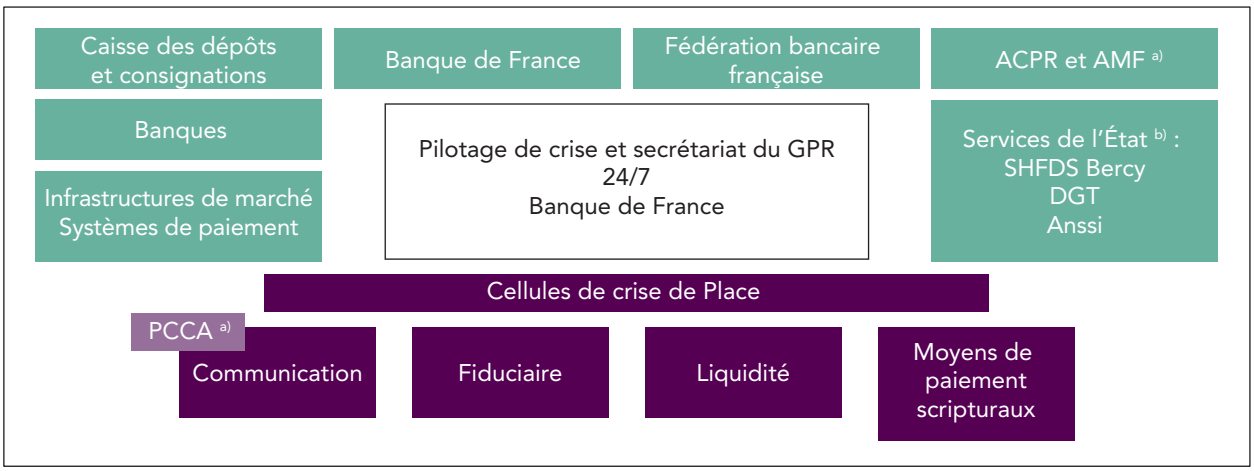
Cette organisation vise à permettre, en cas d'incident, **une évaluation rapide et la plus complète possible** de la situation de la Place, **le partage d'informations en temps opportun** et la prise de décisions collectives le cas échéant. Il s'agit d'une structure flexible, qui doit permettre de prendre en compte, d'une part, **l'origine** de la crise ou de l'incident (catastrophe naturelle, pandémie, mouvement social majeur, défaillance d'un prestataire critique, cyberattaque, etc.) et, d'autre part, ses **conséquences opérationnelles sur les activités financières critiques** (ressources humaines, système d'information, fonctionnement des marchés financiers, gestion de la liquidité, émission et circulation fiduciaire, etc.).

Gouvernance et organisation des travaux

Depuis 2023, les travaux du GPR s'articulent autour de **deux groupes de travail permanents**, dédiés d'une part à la gestion de crise et d'autre part à l'animation et à l'organisation d'exercices de simulation de crise. Ces deux groupes de travail, forts d'une représentativité de l'ensemble des membres du GPR, sont chargés de la mise en œuvre opérationnelle du programme de travail validé en réunion plénière. En outre, les réflexions et travaux menés au sein de ces instances peuvent être source d'amélioration à la fois du dispositif de gestion de crise et des exercices.

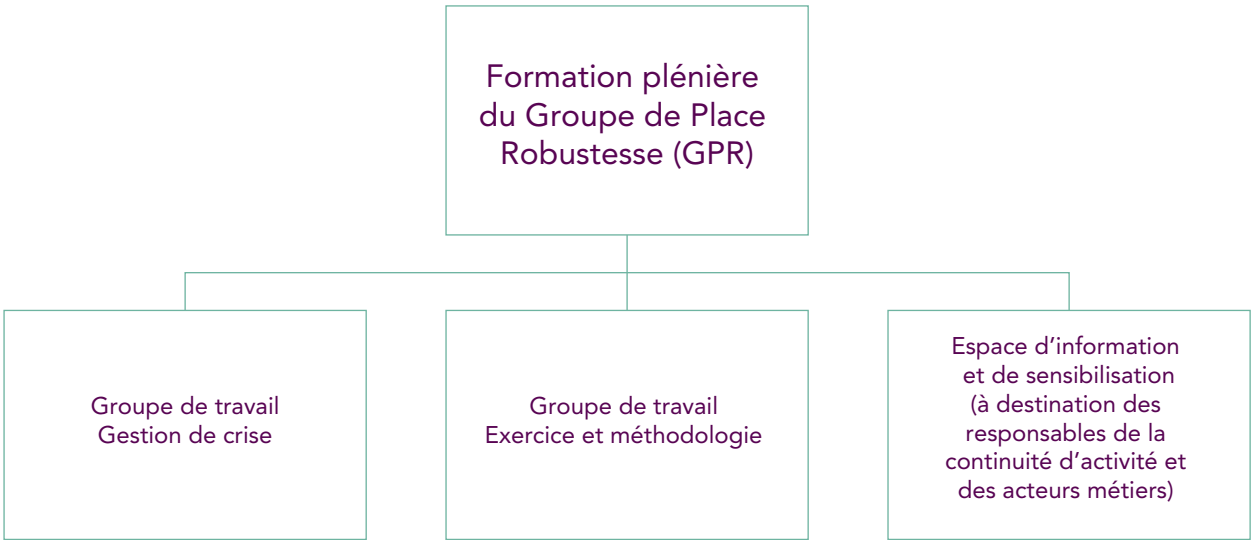
Hors crise (ou hors incident), l'ensemble des membres du Groupe se réunit deux fois par an lors de **réunions plénières**. Ces réunions permettent notamment de définir la

S1 Le Pôle de coordination



a) ACPR, Autorité de contrôle prudentiel et de résolution ; AMF, Autorité des marchés financiers ; PCCA, Pôle de communication de crise des autorités.
b) SHFDS, Service du Haut fonctionnaire de défense et de sécurité ; DGT, direction générale du Trésor ; Anssi, Agence nationale de la sécurité des systèmes d'Information.
Source : Banque de France.

S2 Gouvernance du Groupe de Place Robustesse



Source : Banque de France.

stratégie d'exercice du Groupe et son programme de travail, et de valider les évolutions du dispositif de gestion de crise.

À titre d'illustration, au cours de l'année 2024 :

- le groupe de travail « Animation et organisation d'exercices » a contribué à la réalisation et à la réussite de l'exercice annuel de simulation de crise en particulier grâce aux **travaux de méthodologie relatifs à l'animation d'un exercice** ;
- le groupe de travail « Gestion de crise » a contribué à définir un dispositif de gestion de crise spécifique à la **période des Jeux olympiques et paralympiques** et a permis la création d'une nouvelle cellule de crise de Place dédiée aux moyens de paiement scripturaux.

Enfin, des **réunions d'information, des conférences ou des webinaires** à destination des membres du Groupe sont régulièrement organisés afin de sensibiliser les équipes à de nouveaux types de menaces ou de risques opérationnels *(cf. schéma 2)*.

1.2 L'articulation du Groupe de Place Robustesse avec les dispositifs de gestion de crise cyber européens et internationaux

Si aucun incident cyber critique n'a à ce jour été constaté dans le secteur financier, la numérisation croissante augmente l'exposition à ce risque pour l'ensemble de ses acteurs. En outre, les tensions géopolitiques récentes ont exacerbé le risque de cyberattaques, qui se diffusent au-delà des limites physiques des conflits.

Le GPR s'inscrit ainsi dans un **paysage plus large de dispositifs de gestion de crise** axés sur le risque cyber. La Banque de France prend en effet part à des **instances de coordination européennes et internationales**, dans l'objectif de travailler à l'harmonisation des protocoles de réponse aux incidents et d'organiser des exercices de gestion de crise plurijuridictionnels :

- **Au niveau européen d'abord**, au sein de l'Euro Cyber Resilience Board for pan-European Financial Infrastructures [1] (ECRB) qui réunit des acteurs à la fois publics et privés [2] et a développé un protocole spécifique de gestion de crise, le *Crisis Coordination Protocol*. Ce dernier s'applique aux cybermenaces ou incidents majeurs qui affectent une ou plusieurs infrastructures financières de l'ECRB et qui ont un impact paneuropéen. L'objectif est de partager de manière efficace des informations sur une cyber menace ou un incident majeur impliquant un ou plusieurs membres et de mettre en place des processus

1 *https://www.ecb.europa.eu/*

2 Banques centrales, autorités financières et infrastructures de marché paneuropéennes.

de coordination et d'escalade ainsi que des procédures de communication de crise pour renforcer la confiance du public et du marché ;

- **Au niveau international ensuite**, dans le cadre du groupe d'experts cyber du G7 [3] (CEG, Cyber Expert Group) qui coordonne la politique et la stratégie en matière de cybersécurité dans les huit juridictions du G7 [4]. Afin de vérifier la capacité des autorités financières du G7 à apporter une réponse opportune, efficace et coordonnée aux incidents cyber à portée transfrontalière, le CEG a organisé deux exercices de gestion de crise internationaux (en 2019 et en 2024), dont la Banque de France a piloté la préparation et l'exécution.

3 G7 Cyber Expert Group, U.S. Department of the Treasury.

4 Allemagne, Canada, États-Unis, France, Italie, Japon, Royaume-Uni, Union européenne.

ENCADRÉ

❶

Dispositifs semblables au Groupe de Place Robustesse instaurés par d'autres Places financières

Si la Place financière française présente en 2024 un dispositif mature en matière de résilience face aux risques opérationnels au travers du Groupe de Place Robustesse (GPR), d'autres places, notamment en Europe, se distinguent par des dispositifs similaires construits autour d'une collaboration public-privé.

Italie [1] : Dès 2003, la Place italienne, sous l'impulsion de la Banca d'Italia, s'est dotée d'un dispositif de partage d'informations et de coordination en cas de crise opérationnelle : le Codise. Ce dispositif, qui rassemble les autorités financières italiennes ainsi que les opérateurs financiers systémiques, couvre les crises opérationnelles affectant la Place financière italienne et susceptibles de compromettre la continuité opérationnelle du secteur financier, le fonctionnement des infrastructures financières et la confiance du public dans la monnaie. À l'instar du GPR en France, le Codise organise de façon régulière des exercices de simulation de crise avec l'ensemble de ses membres.

Royaume-Uni [2] : Les autorités financières britanniques coordonnent le Cross Market Business Continuity Group (CMBCG) afin d'assurer la résilience opérationnelle du secteur financier britannique. Ce dispositif permet aux autorités, banques, assureurs et infrastructures des marchés financiers de partager des informations sensibles ou urgentes et de coordonner les actions et la prise de décision en cas de perturbation opérationnelle majeure. Le CMBCG est complété par le CMORG (Cross Market Operationnal Resilience Group) qui prépare la stratégie de cyber-résilience du secteur hors crise.

Pays-Bas [3] : Les autorités financières néerlandaises (banque centrale – DNB, Autorité des marchés financiers et ministère des Finances) ont mis en place un dispositif de gestion de crise tripartite (*Tripartiet crisismanagement operationeel*, TCO) en collaboration avec le secteur financier. Il devient opérationnel en cas de perturbation majeure, réelle ou imminente, des systèmes de paiement ou de titres et a notamment pour mission de prendre et d'annoncer des mesures et d'assurer la liaison avec les parties prenantes.

1 Bank of Italy - CODISE and the business continuity in the Italian financial market (*bancaditalia.it*)

2 Bank of England, Operational resilience of the financial sector (*bankofengland.co.uk*)

3 *https://pywb.nationaalarchief.nl/nl/all/20170401200000/https://www.dnb.nl/en/payments/BCP-and-Crisismanagement/index.jsp*

2

LES EXERCICES DE GESTION DE CRISE : UN LEVIER INDISPENSABLE DE PRÉPARATION DE LA PLACE

2.1 Les exercices du GPR : objectifs et organisation type

Depuis 2005, le secrétariat du GPR (SGPR), géré par les équipes de la Banque de France, organise des **exercices de gestion de crise annuels** impliquant l'ensemble des membres du Groupe.

Les exercices préparés par la Banque de France sont **de type « fonctionnel »** : ils se concentrent sur les processus décisionnels, la coordination et la communication entre les différents acteurs impliqués dans la gestion de crise, en simulant les actions et les réactions à un scénario donné en temps réel.

D'une durée variable (de quelques heures à quelques jours), leur objectif principal est de renforcer la capacité de chaque entité et de la Place dans son ensemble **à se coordonner, en interne comme avec d'autres parties prenantes, face aux incidents qui pourraient perturber la continuité des services financiers critiques**. Au sein de chaque entité, ces exercices permettent de tester l'adéquation des procédures de gestion de crise et de continuité d'activité existantes, d'identifier d'éventuelles faiblesses dans les plans de contingence, de clarifier les rôles et responsabilités de chacun et d'entraîner les équipes à la coordination et à la prise de décision en temps réel. Au niveau de la Place, les exercices du GPR permettent de **s'assurer de l'efficacité des mécanismes de communication et d'échange d'informations entre les membres**.

Ces exercices mobilisent **trois catégories de participants** dans chacune des entités du GPR :

- **Une équipe dite « d'animation »** se charge de la préparation de son établissement à l'exercice, notamment en constituant l'interface avec les équipes de la Banque de France, et s'occupe de la distribution des événements de jeu et du suivi de l'exercice pour son entité le jour J ;
- **L'équipe de « gestion de crise »** joue « son propre rôle » lors de l'exercice. Elle ne connaît pas le scénario à l'avance. Elle met en œuvre les actions de gestion de crise pour son établissement, partage au sein du Groupe l'information sur l'état de ses processus critiques et participe aux conférences de crise du GPR ;
- **Les joueurs des équipes métiers**, comme l'équipe de gestion de crise, découvrent le scénario en temps réel, reçoivent les événements de jeu et doivent y répondre en adoptant le comportement le plus proche possible de celui qu'ils auraient en situation réelle. Ils remontent l'information relative à leur ligne de métier à l'équipe de gestion de crise.

Les exercices s'articulent autour d'un **scénario de crise sévère mais plausible**, qui fait écho à des menaces réelles et qui est préparé par le SGPR, en liaison avec des « complices » au sein de quelques entités afin d'en accroître le réalisme. L'exercice se conclut systématiquement par une **phase de retour d'expérience (Retex)**, qui permet de tirer tous les enseignements nécessaires à la poursuite de l'amélioration du dispositif de gestion de crise.

2.2 La menace cyber : premier risque opérationnel pour les acteurs du secteur financier et clé de voûte des exercices du GPR

L'accélération de la transformation numérique de l'économie, qui favorise une plus grande interconnexion entre les acteurs, et la généralisation du travail à distance (notamment depuis la pandémie de Covid) ont profondément accru la **vulnérabilité des organisations face à une cyber criminalité qui se professionnalise**. En effet, ces facteurs ont considérablement **élargi la surface d'attaque**, augmentant la fréquence et la gravité des incidents cyber. En outre, l'accroissement des tensions géopolitiques a conduit à une militarisation du cyberespace et à l'ouverture de lignes de front virtuelles.

Dans ce contexte, du fait de leur caractère stratégique, les institutions financières et les infrastructures des marchés financiers sont particulièrement visées, notamment par appât du gain, mais aussi dans une optique de déstabilisation étatique. Le secteur financier se classe ainsi parmi les industries les plus menacées, soulevant la crainte de potentielles crises systémiques. Face à ce constat inquiétant, le renforcement de la cyber-résilience du système financier français, et plus largement européen et mondial, constitue une priorité pour les autorités financières et les gouvernements [1].

Se préparer à une crise systémique d'origine cyber

Dès 2018, le GPR a adopté un **prisme cyber dans ses exercices de gestion de crise** [2], notamment en intégrant dans ses scénarios un événement déclencheur de nature cyber, générant des perturbations opérationnelles et financières d'ampleur pour le secteur financier, afin de préparer la Place à un incident informatique généralisé (cyberattaque ou incident non malveillant, comme par exemple le cas récent de CrowdStrike [3]).

Les exercices du GPR n'ont pas vocation à mettre techniquement au défi les experts cyber et IT (informatique-télécommunications) des membres participants, ces derniers réalisant fréquemment des exercices en interne adaptés à leurs systèmes et technologies. Il s'agit avant tout de promouvoir une résilience collective, en **mettant en pratique une coordination à l'échelle de la Place**, les interdépendances entre les membres étant nombreuses et matérialisées notamment par des interconnexions informatiques. De plus, bien que le déclencheur de la crise simulée soit un vecteur cyber affectant plusieurs membres, à des degrés différents ou par effet domino (à travers une attaque de la chaîne d'approvisionnement, un logiciel malveillant ou « maliciel » : *wiper* [4], rançongiciel [5], etc.), la finalité des exercices du GPR est de **créer des impacts sur différentes lignes d'activité** (communication de crise, *trading* et post-marché, usines de paiement, liquidité interbancaire, gestion des ressources humaines, fiduciaire, IT par exemple, en fonction du scénario de l'exercice) et de mobiliser tout un écosystème d'acteurs qui contribuent à gérer la situation de crise.

L'étude du panorama de la menace cyber pour accentuer le réalisme des exercices du GPR

Afin de construire un scénario d'exercice réaliste et vraisemblable, le SGPR réalise dans un premier temps une **étude du panorama de la menace cyber pour le secteur financier**, ce qui permet d'identifier les modes opératoires privilégiés par les groupes malveillants.

En fonction de la cible à atteindre, les vecteurs d'infection seront :

- **Opportunistes** : ils visent le plus grand nombre pour maximiser les chances de réussite de l'attaque. Cela peut par exemple prendre la forme d'une campagne d'hameçonnage [6] massive ;
- **Ciblés** : ils essaient d'atteindre des acteurs ou organisations définis. Des Recon [7] avancés permettent de recueillir toutes les informations disponibles sur la cible avant de lancer une attaque réelle. Les cyberattaquants vont notamment utiliser pour cela des techniques d'ingénierie sociale et exploiter les réseaux sociaux afin de collecter des informations sur les locaux de la cible, des noms d'employés et leurs coordonnées, etc. Tout renseignement peut être utilisé pour développer un exploit logiciel [8] ou pour révéler des faiblesses dans les systèmes défensifs de la cible ;
- **De type *supply chain*** [9] : ils visent à contourner les mesures de cybersécurité des cibles finales en infiltrant une ressource d'un prestataire tiers. Cela permet notamment d'atteindre des cibles dont la maturité en matière de cybersécurité est avancée et dont la surface d'attaque est donc restreinte.

La motivation des acteurs malveillants va, quant à elle, définir le type d'attaque employé :

- **Appât du gain** : l'extorsion de fonds par l'utilisation d'un rançongiciel par exemple est aujourd'hui la principale menace observée ;
- **Déstabilisation** : l'utilisation d'attaques de type DDoS [10] pour rendre indisponibles les sites internet des organisations visées devient une pratique courante ;

- **Espionnage** : l'attaque peut être commanditée par des nations à des fins politiques ou des entreprises visant des gains de compétitivité (cf. l'exemple récent de Pegasus [11]).

Enfin, le rôle des nouvelles technologies, notamment de l'intelligence artificielle, dans la démocratisation et la sophistication des pratiques cyber malveillantes est également suivi de près par le SGPR, du fait de son potentiel dans l'évolution de la menace cyber.

2.3 L'exercice 2024 : la préparation à une crise de grande ampleur

Le risque cyber revêt **une dimension transfrontalière** en raison de l'interconnexion mondiale des réseaux numériques, ce qui facilite la propagation des impacts des cyberattaques au-delà des frontières nationales. Ainsi, un incident qui affecte une entité du secteur est susceptible de se propager rapidement à l'ensemble du système financier, chaque lien financier ou technologique constituant de fait une **chaîne de contagion potentielle**. La nature même du risque cyber appelle donc une **coopération étroite entre autorités financières au niveau international**, afin de maximiser la cohérence et l'efficacité des réponses aux crises cyber.

C'est la raison pour laquelle le groupe d'experts cyber du G7 (CEG, Cyber Expert Group) pilote des travaux visant à renforcer la résilience cyber du système financier au niveau international depuis 2015.

En 2024, le CEG a organisé son **deuxième exercice de gestion de crise cyber transfrontalière**. L'objectif principal de cet exercice de **deux jours** était de renforcer la capacité des autorités financières du G7 à partager de l'information, entre elles et avec l'industrie, à communiquer et à coordonner efficacement leurs réponses respectives afin de faciliter la gestion de crise en cas d'incident cyber dont les impacts concerneraient plusieurs pays.

Un double niveau d'exercice

En France, l'exercice interautorités G7 a été associé à l'exercice national du GPR [12], afin, d'une part, de **mieux intégrer la réalité des interconnexions avec les autres Places financières dans les scénarios de crise** et, d'autre part, de **tester la bonne articulation des dispositifs de coordination à plusieurs échelles**. Après la mise en place de protocoles de partage d'informations et de gestion de crise aux niveaux européen et international, l'enjeu est en effet désormais de **s'assurer que les dispositifs se répondent entre eux** et que l'information circule de manière fluide d'un niveau à l'autre. Ce sont les autorités financières, parties prenantes des deux dispositifs, qui doivent assurer ce rôle d'interface entre les niveaux national et international afin de garantir une gestion de crise complète et cohérente.

Un scénario pluridimensionnel, ancré dans l'actualité de la menace

Fruit d'une préparation de près de dix-huit mois pilotée par la Banque de France, l'exercice G7 a mobilisé **23 autorités financières sur 4 fuseaux horaires différents** *(cf. schéma 3)* autour d'un scénario commun sévère, mais ancré dans l'actualité de la menace. Il s'articulait autour d'une **campagne de déstabilisation du système financier international**, orchestrée par un groupe malveillant et fondée sur le **déploiement d'un maliciel de type « *wiper* »** dans les systèmes d'information de nombreuses institutions financières à travers le monde. Cette attaque a généré des réactions en chaîne en raison

1 Cf. par exemple le communiqué de presse d'octobre 2024 des ministres des Finances et gouverneurs des banques centrales du G7, G7 Finance Ministers and Central Bank Governors' statements, Washington, DC, 25 October 2024 – Consilium (*europa.eu*).

2 Cf. communiqué de presse de l'exercice de 2023 : Banque de France, « Pour la 3ème année consécutive, la Place financière de Paris a mené un exercice de coordination de crise cyber de grande ampleur » (*banque-france.fr*).

3 Panne informatique ayant frappé des millions de systèmes Windows à travers le monde à la suite d'une mise à jour logicielle CrowdStrike défectueuse en juillet 2024.

4 Logiciel malveillant dont le but est de détruire le maximum de données sur l'ordinateur infecté afin qu'elles soient irrécupérables.

5 Logiciel malveillant qui chiffre et vole des données dans le but de demander une rançon à leurs victimes.

6 Ou *phishing*, méthode qui consiste à envoyer des courriels malveillants conçus pour tromper et escroquer les utilisateurs. L'objectif est souvent d'amener les utilisateurs à révéler des informations financières, des informations d'identification du système ou d'autres données sensibles.

7 La reconnaissance est la première étape d'un piratage durant laquelle l'attaquant collecte des informations pertinentes à propos de la cible. Cela se fait dans le but d'identifier les différentes vulnérabilités afin de définir les moyens possibles pour l'attaquer.

8 Un exploit logiciel est une méthode ou un programme utilisé pour exploiter une faille de sécurité dans un logiciel ou un système informatique. En d'autres termes, c'est une technique qui permet à un attaquant de tirer parti d'une vulnérabilité pour exécuter des actions non autorisées, comme accéder à des données, exécuter du code ou prendre le contrôle d'un système.

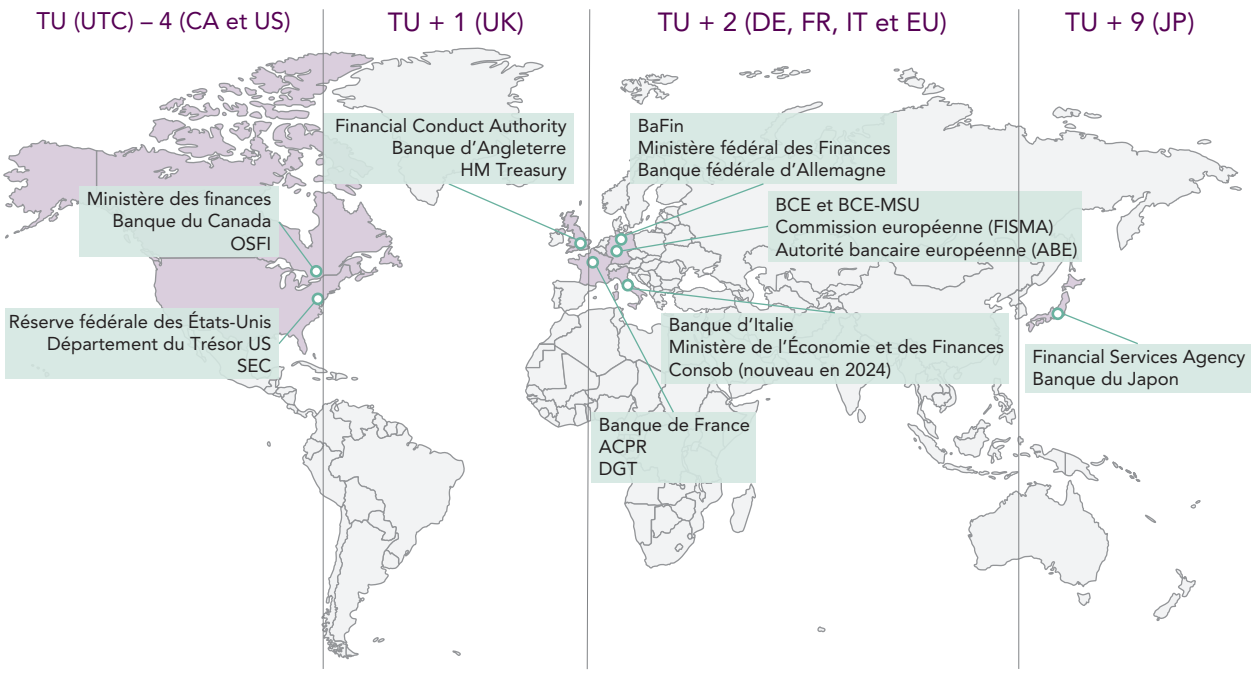
9 Méthode qui consiste à déployer un virus ou autre logiciel malveillant par le biais d'un fournisseur.

10 Une attaque en déni de service ou en déni de service distribué (DDoS pour *Distributed Denial of Service*) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer.

11 Pegasus est un logiciel espion destiné à attaquer les smartphones sous iOS et Android.

12 Banque de France (2024), « En coordination avec les autorités financières du G7, la Place financière de Paris a mené avec succès un exercice de crise cyber de grande ampleur ».

S3 Exercice de crise 2024 : les 23 autorités financières du G7, une mobilisation sur 4 fuseaux horaires



CA : Canada ; DE : Allemagne ; EU : Union européenne ; FR : France ; IT : Italie ; JP : Japon ; UK : Royaume-Uni ; US : États-Unis.
Notes : TU, temps universel ; UTC, temps universel coordonné.
ACPR, Autorité de contrôle prudentiel et de résolution (FR) ; BaFin, Autorité fédérale de supervision financière (DE) ; BCE, Banque centrale européenne (EU) ; Consob, Commissione Nazionale per le Società e la Borsa (IT) ; DGT : direction générale du Trésor (FR) ; FISMA, Financial Stability, Financial Services and Capital Markets Union (EU) ; MSU, mécanisme de surveillance unique (EU) ; OSFI, Office of the Superintendent of Financial Institutions (CA) ; SEC, Securities and Exchange Commission (US).
Source : Banque de France.

des interdépendances entre les acteurs et d'importantes perturbations des activités de marché, alimentées par une forte désinformation de la part des *hackers* sur les réseaux sociaux. En France, le choix a été fait d'ajouter à ce scénario « marchés » une dimension transsectorielle, avec la simulation d'un **incident sur le secteur des télécommunications et des impacts supplémentaires sur les activités fiduciaires et monétiques des acteurs financiers**.

Une mobilisation inédite et des pistes ambitieuses pour l'avenir

Ce scénario dense et pluridimensionnel a permis à plus de **2 500 professionnels du secteur financier** de se mobiliser sur les deux jours d'exercice, témoignant de l'importance de ce rendez-vous annuel pour les acteurs de Place.

L'exercice a permis à chaque entité d'éprouver ses plans de contingence et a démontré une nouvelle fois l'utilité du dispositif du GPR, qui offre un **cadre d'échange fiable**, y compris en temps de crise où le stress est exacerbé.

Le succès de cet exercice a montré la **maturité de la Place financière de Paris** et **son haut niveau de préparation**, quelques mois avant le début des Jeux olympiques et paralympiques de Paris (JOP) 2024.

Les **pistes d'action issues du Retex**, qu'il s'agisse de l'amélioration des outils et des méthodologies du GPR, du renforcement des partenariats à l'international ou d'une collaboration rapprochée avec d'autres secteurs stratégiques pour favoriser la compréhension et la gestion collectives des risques, participeront à la professionnalisation croissante du dispositif.

3

UN DISPOSITIF DE GESTION DE CRISE ÉPROUVÉ ET EN CONSTANTE AMÉLIORATION

3.1 Des espaces de collaboration dédiés pour préparer la gestion de crise

Hors crise, le GPR a un rôle d'anticipation et de préparation en vue des crises futures. À cet effet, le Groupe dispose d'un espace d'échange pour faire intervenir des experts sur des sujets d'actualité à fort impact pour les activités des membres. Au cours des dernières années, cet espace a par exemple été activé lors de l'agression militaire de la Russie contre l'Ukraine pour dresser un panorama de la menace cyber vis-à-vis du secteur financier ou bien face au risque de survenance d'une panne électrique à l'hiver 2022-2023.

Les groupes de travail permanents du GPR contribuent à l'amélioration continue de la préparation à la gestion de crise en approfondissant, lors d'ateliers de travail dédiés, des sujets tels que l'anticipation, la continuité des activités critiques ou encore la préparation de crise lors de grands évènements comme les JOP 2024 *(cf. encadré 2)*.

3.2 Un rôle de facilitateur au service de la Place

Face à des chocs opérationnels qui affectent les fonctions critiques de la Place financière de Paris, le GPR se mobilise avec pour objectifs :

- d'établir un diagnostic complet de la situation de Place grâce à la mobilisation de l'ensemble de ses acteurs ;
- de favoriser les échanges entre les membres pour faciliter la collaboration public-privé ;
- de permettre une coordination sectorielle concernant les phases de reconstruction et de reprise pour les activités communes à plusieurs acteurs de la Place ;
- d'aider les membres pour leur gestion de crise individuelle en favorisant le partage d'informations, à bon escient.

Lors de la pandémie de Covid-19, le GPR s'est réuni à plusieurs reprises afin d'identifier les impacts et les mesures de continuité d'activité à déployer par le secteur financier. Les principales questions soulevées par la pandémie concernaient :

- la continuité de la filière fiduciaire avec l'approvisionnement des distributeurs automatiques de billets (DAB) ou la circulation des espèces comme potentiel vecteur du virus ;
- l'organisation du travail à mettre en place au sein des entités afin de poursuivre l'activité en période de confinement. Les ressources humaines ont constitué un sujet clé tout au long de la pandémie avec une nécessité de séparer les équipes critiques qui n'avaient pas une activité « télétravaillable ». Le GPR s'est également coordonné pour partager de l'information et de bonnes pratiques sur les modalités à mettre en œuvre, afin d'assurer le retour sur site en toute sécurité des collaborateurs.

Au cours des dernières années, le GPR s'est retrouvé à plusieurs reprises en veille active (agression militaire de la Russie contre l'Ukraine en 2022, émeutes urbaines en 2023, CrowdStrike en 2024) afin d'identifier et de surveiller les conséquences potentielles de ces évènements pour les acteurs du système financier. Le Groupe était en mesure de se mobiliser plus largement si ces évènements avaient entraîné une perturbation ou un arrêt des processus critiques de Place.

3.3 Un programme de travail ambitieux pour les prochaines années

L'exercice de simulation de crise d'avril 2024 a marqué l'aboutissement de la stratégie pluriannuelle du GPR articulée autour du risque cyber, tout en ouvrant la voie à un **nouveau plan d'action et au lancement de nouvelles thématiques de travail**, ancrées dans l'actualité de la menace et les enjeux contemporains. Au-delà du risque cyber, la prise en compte d'autres types de menaces opérationnelles, y compris dans une **approche transsectorielle**, sera un élément clé pour renforcer la résilience de Place. Par ailleurs, les pistes de travail identifiées pour le GPR s'appuieront aussi sur les travaux et les priorités du groupe d'experts cyber du G7 (CEG), auquel la Banque de France contribue, afin de maximiser la cohérence globale des initiatives des autorités.

Concernant **l'amélioration du dispositif du GPR**, les futurs travaux porteront en particulier sur :

- le perfectionnement des **outils de gestion de crise**, afin de conjuguer sécurité, fiabilité et accessibilité ;
- une réflexion approfondie sur **les phases d'anticipation et de redémarrage post-incident** ;
- la recherche d'une **articulation toujours plus optimale** entre les dispositifs de gestion de crise à tous les niveaux (national, mais aussi européen et mondial) ;
- le renforcement de la **collaboration avec d'autres secteurs stratégiques, comme ceux de l'énergie ou des télécommunications**, afin de mieux prendre en compte les interconnexions avec le secteur financier, et préparer ainsi une gestion de crise encore plus cohérente et complète.

La nouvelle stratégie d'exercices du GPR capitalisera sur les facteurs de succès identifiés ces dernières années, dont notamment la co-construction du scénario avec des complices au sein des membres du GPR, afin d'accroître la précision et le réalisme des événements de jeu. Le GPR s'appuiera sur différentes méthodologies d'exercices, et renforcera la coopération avec d'autres Places financières ou d'autres secteurs.

ENCADRÉ

❷ Les JOP 2024 : l'entraînement du côté du secteur financier

Les enjeux de continuité d'activité et les risques associés aux Jeux olympiques et paralympiques (JOP) 2024 ont amené le Groupe de Place Robustesse (GPR) à créer un dispositif de gestion de crise spécifique, et à mettre en place une veille des risques renforcée. Dès 2023, le secrétariat du Groupe (SGPR, à la Banque de France) a travaillé avec les membres du GPR pour préparer la Place en prévision des JOP. Ces travaux ont donné lieu à la création d'un dispositif spécifique de veille renforcée, à déployer lors des Jeux, afin d'effectuer **un suivi actif des principaux événements pouvant affecter la continuité d'activité** du secteur financier et **assurer la mise en place d'un canal d'échange dédié et efficace** entre toutes les parties prenantes.

Les travaux préparatoires ont permis d'identifier quatre grands enjeux pour la Place *(cf. schéma)* : i) l'accroissement du risque cyber, en raison de la surexposition médiatique des Jeux [1] ; ii) la sécurité des agences bancaires situées dans des zones olympiques ; mais aussi iii) la gestion des ressources humaines et l'accès aux locaux du fait des contraintes de circulation ; ou encore iv) les enjeux propres à la filière fiduciaire concernant l'accès aux espèces près des sites de compétition.

Pour y répondre, le SGPR a mis en place quatre actions :

i. **Une réunion d'information fin 2023 afin de présenter les risques identifiés** ainsi que les dispositifs de gestion de crise mis en œuvre par les acteurs gouvernementaux en amont et pendant les JOP ;

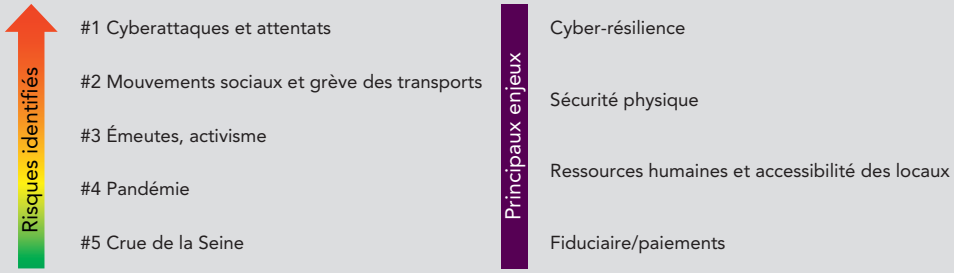
ii. **Un renforcement des canaux d'échange** avec une procédure de gestion de crise spécifique mise en place entre des acteurs spécialisés et le SGPR afin de partager des informations sur les incidents, notamment pendant la période des Jeux ;

iii. **Un entraînement opérationnel à la gestion de crise** intégrant à l'exercice d'avril 2024 la simulation d'incidents fiduciaires, monétiques et sur les réseaux de télécommunications afin de préparer les acteurs ;

iv. **Enfin, la mise en œuvre d'un dispositif de suivi renforcé pendant les JOP** à travers la planification de points hebdomadaires avec l'ensemble des acteurs du Groupe. Ce dispositif déployé de mi-juillet à mi-septembre 2024 visait notamment à centraliser au sein d'une même instance les informations échangées par les présidents des cellules de crise de Place sur leurs périmètres respectifs (communication, fiduciaire, liquidité, moyens de paiement scripturaux). Ces points favorisaient également le partage d'informations entre l'industrie financière et les services de l'État sur les incidents ou les menaces pendant les Jeux (cyber, attentat, activisme) afin d'alimenter les dispositifs de gestion de crise individuels des membres.

1 CERT-FR (Anssi) (2023), Grands évènements sportifs – Évaluation de la menace 2023.

Principaux risques et enjeux associés aux JOP pour le secteur financier



Source : Banque de France.

Dans l'ensemble, aucun événement majeur n'a été signalé pendant la période des JOP, à l'exception des problèmes sur les télécommunications (sabotage de réseaux de fibre optique) au début des Jeux, sans impact toutefois sur le secteur financier. **Le dispositif de suivi renforcé mis en place et l'accompagnement du secteur ont permis une bonne coordination et un partage d'informations efficace.** Ce dispositif de coordination, fondé sur une démarche proactive, pourrait s'inscrire pleinement dans les outils de gestion de crise du GPR, notamment à l'occasion d'autres grands évènements ou encore lors de crises avec une cinétique plus lente, telles qu'une crue de la Seine ou une nouvelle pandémie par exemple. L'orchestration efficace du dispositif et la coordination entre les différents acteurs qui a été éprouvée lors des JOP ont été riches d'enseignements pour contribuer à l'amélioration continue du dispositif de gestion de crise du GPR d'une part, et pour renforcer encore le partage d'informations entre les acteurs publics et privés d'autre part.

POSTFACE

Après vingt ans, un bilan très positif et des perspectives prometteuses

*Après **vingt années de travail collectif**, le bilan que nous dressons aujourd'hui avec fierté est celui d'un **renforcement profond de la résilience opérationnelle de la Place financière de Paris**. Notre Groupe a su, au fil des ans, structurer **un dispositif de gestion de crise robuste et agile**, qui réunit tous les acteurs financiers systémiques dans l'optique d'améliorer la capacité de réponse aux incidents majeurs du secteur et de **maintenir la stabilité financière**.*

*Si le dispositif est aussi mature, c'est parce que depuis 2005, nous ne nous sommes **jamais reposés sur nos acquis**. Conscients de l'évolution et de la sophistication rapides des risques, nous avons systématiquement **mis nos procédures au défi**, les confrontant aux réalités nouvelles, aux enjeux émergents et en nous inspirant des bonnes pratiques observées auprès de nos homologues, tant sur le plan national qu'international. Le **risque cyber**, en particulier, parce qu'il combine perpétuelle mutation et ampleur potentiellement globale des impacts, a exigé une **capacité d'adaptation continue de notre système de réponse**.*

*L'un des principaux leviers sur lequel nous nous sommes appuyés tout au long de ces années pour renforcer notre dispositif est sans aucun doute **l'organisation d'exercices de gestion de crise réguliers**. Ces simulations de grande ampleur renforcent notre **aptitude à la coordination**, au sein de chaque organisation et autorité comme au-delà, **et à la prise de décision en temps réel**. Nous avons progressivement **relevé le niveau d'ambition**, en augmentant chaque fois la profondeur de jeu, le réalisme des scénarios et en impliquant un nombre croissant d'acteurs, avec un apogée atteint avec l'exercice 2024. **Réunir pendant deux jours 8 juridictions et 2 500 professionnels du secteur financier français** autour d'un même scénario de crise relève en effet d'une prouesse organisationnelle sans précédent. La **réussite de cet exercice** réside non seulement dans l'orchestration simultanée de multiples entités à travers le monde, mais aussi dans la **fluidité de la coordination entre les autorités du G7** et dans **l'articulation réussie des dispositifs de gestion de crise à plusieurs échelles**.*

De même, chaque menace, chaque incident réel de ces dernières années a été l'opportunité d'affiner notre vigilance et d'anticiper de nouveaux scénarios. Ces événements, qu'il s'agisse de tentatives de cyberattaques, de défaillances de prestataires tiers ou de crises sociales, outre d'avoir confirmé que notre dispositif était pleinement opérationnel, ont agi comme des catalyseurs, nous poussant à faire évoluer nos outils et à adopter des pratiques toujours plus rigoureuses.

*Toutefois, il est impératif de **ne jamais considérer nos efforts comme achevés** et de toujours f**aire preuve de prudence** face à la montée en puissance de risques qui **déjouent les mécanismes de défense traditionnels**. La poursuite de la transformation numérique, avec le développement de l'intelligence artificielle, la multiplication des phénomènes climatiques extrêmes ou l'exacerbation des tensions politiques et sociales sont autant de facteurs qui peuvent affecter la continuité des opérations critiques.*

*Ainsi, tout en reconnaissant les progrès accomplis, **nous nous tournons vers l'avenir avec humilité**. Forts de notre expérience, nous sommes prêts à relever les défis qui s'annoncent, avec la conviction que notre engagement collectif permettra de façonner **un système financier encore plus résilient**.*

***Claudine Hurman**,*
Directrice de l'Innovation et des Infrastructures des marchés financiers à la Banque de France
Pilote du Groupe de Place Robustesse

Éditeur
Banque de France
39 rue Croix-des-Petits-Champs
75001 Paris

Directrice de la publication
Emmanuelle Assouan
Directrice générale de la Stabilité financière et des Opérations
Banque de France

Directrice de la rédaction
Claudine Hurman
Directrice de l'Innovation et des Infrastructures
des marchés financiers
Banque de France

Secrétariat de rédaction
Jade Al Yahya, Pierre Berger, Paul Capocci,
Raffaella Cartigny, Silvia Gabrieli, Thierry Nardoux,
Hafid Ouaguenouni

Réalisation
Studio Création
Direction de la Communication
de la Banque de France

Contact
Direction de l'Innovation et des Infrastructures
des marchés financiers
Service de Résilience et d'Études
des infrastructures de marché
Code courrier : S1B-2327
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Impression
Navis
Imprimé en France

Dépôt légal
Février 2025
ISSN en cours

Internet
https://www.banque-france.fr/fr

Le *Rapport du Groupe de Place Robustesse* est en libre téléchargement sur le site internet de la Banque de France (*https://www.banque-france.fr/fr/stabilite-financiere/activites*).

www.banque-france.fr