TWENTY YEARS OF THE PARIS RESILIENCE GROUP (2005-25)

Better preparing for crises and strengthening the operational resilience of the Paris financial centre

FEBRUARY 2025

BANQUE DE FRANCE
EUROSYSTÈME

TWENTY YEARS OF THE PARIS RESILIENCE GROUP (2005-25)

Better preparing for crises and strengthening the operational resilience of the Paris financial centre

FEBRUARY 2025

FOREWORD

The Paris Resilience Group (*Groupe de Place Robustesse*): a body reflecting the maturity of the French financial sector in terms of resilience

The year 2024 once again brought to the fore the ***complex and uncertain operational environment*** *in which the French financial sector operates: increased cyberthreats against a backdrop of geopolitical tensions, a proliferation of extreme weather events, but also operational challenges successfully met by the financial sector during the Paris Olympic and Paralympic Games, among others.*

Given the diversity of these risks, the sector's collective ability to anticipate, coordinate and recover from a major incident, and ***thus strengthen its operational resilience****, is more crucial than ever. While it is the responsibility of supervisors to continue to* ***strengthen the soundness of individual financial institutions****, within the framework of the regulatory relations established with each financial player, the objective of the* ***Paris Resilience Group****, which was set up in 2005, is to take into account the* ***operational interdependencies*** *that bind our entire ecosystem, as part of a cooperative approach.*

The financial sector is characterised by a ***dense ecosystem of financial and technological interconnections*** *based on the existence of critical nodes – be they financial intermediaries, financial market infrastructures or essential service providers – which create a high potential for contagion. A disruption within one entity can spread rapidly and have major repercussions for the entire financial system.* ***Anticipating, managing and mitigating*** *these operational risks, through coordination and information-sharing, is therefore an integral part of the* ***Banque de France's financial stability mission****. This was the spirit in which the Paris Resilience Group was created. This Group is unique in terms of its* ***governance****, which is based on cooperation between members, and its* ***structure****, as it brings together* ***public and private players****, giving it a wealth of perspectives and expertise – with the* ***Banque de France acting as a facilitator of exchanges****.*

Over the past years, like a team, we have established the priorities for our cooperation, based on trust, sharing and collective efforts. During a major operational crisis, the integrity and stability of the sector depend on ***participants being able to exchange relevant information in a timely manner and coordinate their crisis response or communication.*** *Establishing a climate of trust is a prerequisite for this sharing, as is regularly conducting crisis management exercises, the last of which in 2024 involved a cyberattack scenario. This work differs from prudential supervision in that it is based on a* ***collaborative, voluntary approach****, focusing on collective preparedness and overall sectoral resilience.*

Beyond the Paris financial centre, the ***cross-border nature of a number of operational risks****, such as cyber risk, calls for the implementation of coordinated management mechanisms between jurisdictions to contain contagion and mitigate the potential impact on the international financial system as a whole. That is why we are constantly striving to* ***strengthen our collaboration with our counterparts abroad****.*

Our Group is now 20 years old and its constant evolution since 2005 testifies to the ***maturity of the sector in terms of operational resilience****. The Paris Resilience Group's collective and ongoing efforts should ensure that this resilience is sustained over the coming years.*

Emmanuelle Assouan*,*
Director General Financial Stability and Operations
Chair of the Paris Resilience Group

CONTENTS

1

THE PARIS RESILIENCE GROUP: 20 YEARS OF EFFECTIVE PUBLIC-PRIVATE COOPERATION

1.1 A group created to strengthen the operational resilience of the financial sector

In 2005, the Paris financial centre set up the **Paris Resilience Group (*Groupe de Place Robustesse* – PRG)** to address the different operational threats to which it may be exposed. Created at the initiative of the Banque de France as part of its financial stability mission, the PRG aims to ensure that a major operational crisis does not cause a prolonged disruption of the functioning of the financial system by coordinating and sharing information.

In addition to strengthening the **robustness** of the financial sector, i.e. its ability to withstand external shocks, the PRG focuses on improving the **resilience** of the Paris financial centre, i.e. its ability to absorb the impact of an exogenous disruption and to recover in order to ensure the continuity of critical financial services.

Since its creation, the Group has been committed to identifying and anticipating the **operational threats** to which the financial sector may be exposed. While cyber risk has remained a major concern for several years, geopolitical tensions, pandemics, extreme weather events, deteriorating socio-economic and political conditions or the failure of a critical service provider are all exogenous risks that need to be monitored.

Chaired by the Director General Financial Stability and Operations of the Banque de France, the PRG is unique in that it brings together **players from both the public and private sectors**:

- **credit institutions and similar entities** (BNP Paribas, Crédit Agricole, BPCE, La Banque Postale, Crédit Mutuel, Société Générale, Caisse des dépôts et consignations, HSBC Continental Europe);
- **financial market infrastructures** (LCH SA, Euronext, Euroclear, STET, GIE Cartes Bancaires, EBA Clearing);
- **the Banque de France**;
- **regulatory and supervisory authorities**: the *Autorité de contrôle prudentiel et de résolution* (ACPR – the French Prudential Supervision and Resolution Authority), *Autorité des marchés financiers* (AMF – Financial Markets Authority);
- **the Senior Official for Defence and Security, Ministry of the Economy and Finance**;
- **the French Treasury**;
- ***Agence nationale de la sécurité des systèmes d'information*** (ANSSI – the French national cybersecurity agency);
- ***Fédération bancaire française*** **(French Banking Federation)**;
- the heads of the four **financial centre crisis units** (communication, cash industry, liquidity and cashless payments), which bring together experts from the Banque de France and from the PRG member entities to discuss these key issues for the financial sector during a crisis.

The Banque de France leads and coordinates the Group. It therefore facilitates exchanges between members and ensures that the framework continues to evolve.

Operational tasks and functioning

There are two timeframes for the PRG's operational tasks.

- **Outside crisis (or incident) periods**: a phase of anticipation and preparation for crisis management, in particular through major operational crisis simulation exercises and awareness-raising initiatives. Exercises are organised annually to test the crisis management system.
- **During a crisis (or incident)**: an actual crisis management phase, which includes assessing the situation, coordinating crisis management decisions (if relevant) and taking any joint decisions.

In both timeframes, a feedback phase contributes to **continually improving** the crisis management system.

The PRG operates through a dedicated structure, the **Coordination Hub** *(see Figure 1)*. Headed by the Banque de France, it brings together all the members of the PRG and is supported in particular by the four crisis units. These units are autonomous from the Hub, but coordinate closely with it in the event of an operational crisis. The heads of the crisis units are full members of the Coordination Hub, which facilitates a regular exchange of information.

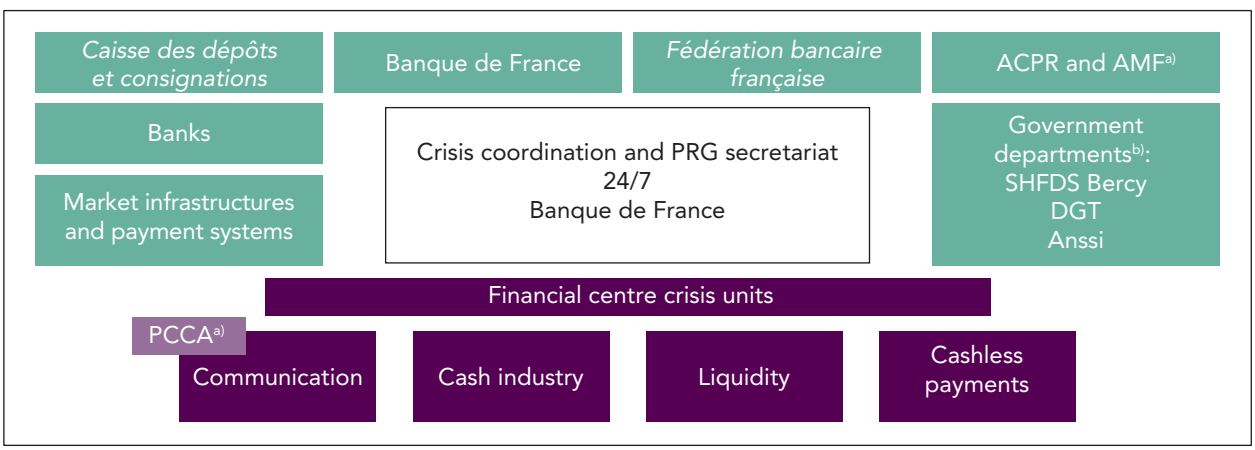
In the event of an incident, this organisation aims to ensure that the situation in the financial centre can be **assessed quickly and as comprehensively as possible**, that information can be **shared in a timely manner** and that collective decisions can be taken if necessary. This is a flexible structure, which makes it possible to take into account both **the origin** of the crisis or incident (natural disaster, pandemic, large-scale industrial action, failure of a critical service provider, cyberattack, etc.) and its **operational consequences on critical financial activities** (human resources, information system, functioning of financial markets, liquidity management, issuance and circulation of banknotes, etc.).

Governance and work organisation

Since 2023, the PRG's work has been organised through **two permanent working groups**, one dedicated to crisis management and the other to conducting and organising crisis simulation exercises. These two working groups, which bring together all the members of the PRG, are responsible for the operational implementation of the work programme approved at the plenary meeting. Furthermore, the discussions and work carried out within these bodies can serve to improve both the crisis management framework and the exercises.

Outside crisis (or incident) periods, all members of the Group meet twice a year in **plenary session**. These meetings are used to define the Group's exercise strategy and work programme, and to approve changes to the crisis management framework.

Figure 1 The Coordination Hub



Source: Banque de France.

a) ACPR: *Autorité de contrôle prudentiel et de résolution* (the French Prudential Supervision and Resolution Authority); AMF: *Autorité des marchés financiers* (Financial Markets Authority); PCCA: Crisis communication unit of the authorities.

b) *Service du Haut Fonctionnaire de défense et de sécurité* (Department of the Senior Official for Defence and Security); DGT: *direction générale du Trésor* (French Treasury); Anssi: *Agence nationale de la sécurité des systèmes d'Information*; *Fédération bancaire française* (French Banking Association).

Figure 2 Governance of the Paris Resilience Group

Source: Banque de France.

For example, in 2024:

- the working group on "facilitating and organising exercises" contributed to the organisation and success of the annual crisis simulation exercise, in particular by **working on the methodology for conducting an exercise**;
- the working group on "crisis management" helped to define a crisis management system specifically for the **period of the Olympic and Paralympic Games**, and led to the creation of a new financial centre crisis unit dedicated to cashless means of payment.

Lastly, **information meetings, conferences and webinars** for Group members are regularly organised to raise awareness of new types of threats and operational risks *(see Figure 2)*.

1.2 The Paris Resilience Group's links to European and international cyber crisis management frameworks

While there have been no critical cyber incidents in the financial sector to date, increasing digitalisation is heightening exposure to this risk for all players in the sector. Moreover, recent geopolitical tensions have exacerbated the risk of cyberattacks, which spread beyond the physical limits of the conflicts.

The PRG is thus part of a **broader landscape of crisis management frameworks** focused on cyber risk. Indeed, the Banque de France participates in **European and international coordination bodies**, working to harmonise incident response protocols and organising multi-jurisdictional crisis management exercises.

- **Firstly, at European level**, within the Euro Cyber Resilience Board for pan-European Financial Infrastructures[1] (ECRB), which brings together both public and private players[2] and has developed a specific crisis management protocol, the Crisis Coordination Protocol. This protocol applies to major cyberthreats or incidents that affect one or more of the ECRB's financial infrastructures and have a pan-European impact. The aim is to effectively share information about a cyberthreat or major incident involving one or more members and to put in place coordination and escalation processes and crisis communication procedures to boost the confidence of the public and markets.

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

2 Central banks, financial authorities and pan-European market infrastructures.

- **Secondly, at international level**, through the G7 Cyber Expert Group (CEG)[3], which coordinates cybersecurity policy and strategy across the eight G7 jurisdictions.[4] In order to test the ability of the G7 financial authorities to provide a timely, effective and coordinated response to cross-border cyber incidents, the CEG organised two international crisis management exercises (in 2019 and 2024), for which the Banque de France managed the preparation and execution.

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

4 Canada, France, the European Union, Germany, Italy, Japan, the United Kingdom and the United States.

BOX

❶

Frameworks similar to the Paris Resilience Group set up by other financial centres

While the Paris financial centre has now achieved a certain level of maturity in addressing operational risks through the Paris Resilience Group (PRG), other financial centres, particularly in Europe, have similar frameworks based on public-private cooperation.

Italy:[1] In 2003, under the impetus of the Banca d'Italia, the Italian financial centre set up Codise, a framework for information sharing and coordination in the event of an operational crisis. This framework, which brings together the Italian financial authorities and systemic financial players, covers operational crises affecting the Italian financial centre and which could compromise the operational continuity of the financial sector, the functioning of financial infrastructures and public confidence in the currency. Like the PRG in France, Codise regularly organises crisis simulation exercises with all its members.

United Kingdom:[2] The UK financial authorities coordinate the Cross Market Business Continuity Group (CMBCG) to ensure the operational resilience of the UK financial sector. This framework enables the authorities, banks, insurers and financial market infrastructures to share sensitive or time-sensitive information and coordinate actions and decision-making in the event of a major operational incident. The CMBCG works alongside the Cross Market Operational Resilience Group (CMORG), which prepares the sector's cyber resilience strategy in the event of a crisis.

Netherlands:[3] The Dutch financial authorities (De Nederlandsche Bank – DNB, Financial Markets Authority and Ministry of Finance) have set up a tripartite crisis management system (*Tripartiet crisismanagement operationeel*, TCO) in cooperation with the financial sector. It is triggered in the event of an actual or imminent major disruption of the payment or securities systems, and is responsible for taking and announcing measures and liaising with stakeholders.

1 Banca d'Italia – 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

CRISIS MANAGEMENT EXERCISES: AN ESSENTIAL TOOL FOR PREPARING THE FINANCIAL CENTRE

2.1 PRG exercises: objectives and organisation

Since 2005, the Secretariat of the PRG (SGPR), managed by Banque de France staff, has organised **annual crisis management exercises** involving all Group members.

The exercises organised by the Banque de France are of a **"functional" nature**: they focus on the decision-making processes, coordination and communication between the various players involved in crisis management, by simulating actions and responses to a given scenario in real time.

They vary in length from a few hours to a few days, and their main objective is strengthen the ability of each entity and the financial centre as a whole to **coordinate, both internally and with other stakeholders, to address incidents that could disrupt the continuity of critical financial services**. Within each entity, these exercises test the appropriateness of existing crisis management and business continuity procedures, identify any weaknesses in contingency plans, clarify each player's roles and responsibilities, and prepare teams for real-time coordination and decision-making. At financial centre level, PRG exercises **ensure that the mechanisms for communication and information exchange between members are effective**.

These exercises involve three **categories of participant** in each of the PRG entities.

- **A team of "coordinators"** is responsible for preparing their institution for the exercise, in particular by acting as an interface with the Banque de France staff, and for delivering the stimuli and monitoring the exercise for their entity on the actual day.
- **The "crisis management" team** plays "its own role" during the exercise. It does not know the scenario beforehand. It implements crisis management measures for its institution, shares information within the Group on the state of its critical processes and participates in PRG crisis conferences.
- **Players from the business line teams**, like the crisis management team, discover the scenario in real time, receive the stimuli and have to respond by adopting the behaviour that is as close as possible to what they would do in a real situation. They pass on information relating to their business line to the crisis management team.

The exercises are based on a **severe but plausible crisis scenario**, which reflects real threats and is prepared by the SGPR, together with "accomplices" within a number of entities, to make them more realistic. The exercise systematically concludes with a **feedback phase**, which enables all the necessary conclusions to be drawn for the continued improvement of the crisis management framework.

2.2 Cyberthreats: the number one operational risk for players in the financial sector and the cornerstone of PRG exercises

The acceleration of the digital transformation of the economy, which is fostering greater interconnections between players, and the growth of remote working (particularly since the Covid pandemic) have greatly increased the **vulnerability of organisations to cybercrime, which is becoming increasingly professional**. Indeed, these factors have considerably widened the **attack surface**, increasing the frequency and severity of cyber-incidents. In addition, growing geopolitical tensions have led to the militarisation of cyberspace and the opening up of virtual front lines.

Against this backdrop, due to their strategic nature, financial institutions and financial market infrastructures are particularly targeted, in particular for financial gain, but also with a view to destabilising the state. The financial sector thus ranks among the industries most at risk, raising fears of potentially systemic crises. In this context, it is a priority for the financial authorities and governments to strengthen the cyber resilience of the French financial system and, more broadly, the European and global financial systems.[1]

Preparing for a systemic cyber crisis

Since 2018, the PRG **has adopted a cyber prism in its crisis management exercises**,[2] in particular by including in its scenarios a cyber trigger event, generating major operational and financial disruptions for the financial sector, in order to prepare the financial centre for a widespread IT incident (cyberattack or non-malicious incident, such as the recent case of CrowdStrike).[3]

PRG exercises are not intended to be technical challenges for the cyber and IT experts of participating members, who frequently carry out in-house exercises adapted to their systems and technologies. Their main aim is to promote collective resilience, **by putting into practice coordination at the financial centre level**, since there are many interdependencies between members, particularly through IT interconnections. Moreover, although the trigger for the simulated crisis is a cyberattack affecting several members, to varying degrees or through a domino effect (i.e. an attack on the supply chain, malicious software or "malware": wiper,[4] ransomware,[5] etc.), the aim of PRG exercises is to **create impacts on different business lines** (e.g. crisis communication, trading and post-trade, payment factories, interbank liquidity, human resources management, the cash sector or IT, depending on the exercise scenario) and to mobilise a whole ecosystem of players who contribute to managing the crisis situation.

Studying the cyberthreat landscape to make PRG exercises more realistic

In order to create realistic and plausible scenarios for the exercise, the SGPR first conducts a **study of the cyberthreat landscape for the financial sector**, which enables it to identify the preferred *modus operandi* of malicious groups.

Depending on the intended target, the infection vectors will be:

- **Opportunistic**: targeting as many people as possible to maximise the chances of a successful attack. This can take the form of a massive phishing[6] scheme, for example.
- **Targeted**: trying to hit specific players or organisations. Advanced Recon[7] allows hackers to gather all available information about the target before launching a real attack. In particular, cyberattackers will use social engineering techniques and exploit social networks to gather information about the target's premises, employees' names and contact details, etc. Any information can be used to develop a software exploit[8] or to uncover weaknesses in the target's defence systems.
- **Supply chain**:[9] attempting to circumvent the end-target's cybersecurity measures by infiltrating a resource belonging to a third-party service provider. In particular, this enables attackers to hit targets with a high level of maturity in terms of cybersecurity, and whose attack surface is therefore limited.

The motivation of the malicious parties will determine the type of attack used.

- **The lure of profit**: extortion of funds through the use of ransomware, for example, is the main threat observed today.
- **Disruption**: the use of DDoS attacks to make the websites of targeted organisations unavailable is becoming common practice.
- **Spying**: the attack can be commissioned by nations for political purposes or by companies seeking to gain a competitive edge (see the recent example of Pegasus).[10]

Lastly, the role of new technologies, particularly artificial intelligence, in the spread and sophistication of malicious cyber practices is also being closely monitored by the SGPR, because of its potential to change cyberthreats.

2.3 The 2024 exercise: preparing for a major crisis

Cyber risk has a **cross-border dimension** due to the global interconnection of digital networks, which makes it easier for the impact of cyberattacks to spread beyond national borders. Therefore, an incident affecting one entity in the sector could spread rapidly to the entire financial system, with each financial or technological link constituting a **potential contagion chain**. The very nature of cyber risk therefore calls for **close cooperation between financial authorities at international level**, in order to maximise the consistency and effectiveness of responses to cyber crises.

This is why the G7 Cyber Expert Group (CEG) has been coordinating efforts to strengthen the cyber resilience of the financial system at international level since 2015.

In 2024, the CEG organised its **second cross-border cyber coordination exercise**. The main objective of this **two-day** exercise was to enhance the ability of the G7 financial authorities to share information with each other and with the industry, and to communicate and coordinate their respective responses effectively in order to facilitate crisis management in the event of a cyber incident affecting several countries.

A two-tier exercise

In France, the G7 inter-authority exercise was combined with the national PRG exercise[11] in order to **better integrate the reality of interconnections with other financial centres into the crisis scenarios** and to **test the coordination mechanisms at several levels**. Following the implementation of information-sharing and crisis-management protocols at the European and international levels, the challenge now is to **ensure that the frameworks interact effectively** and that information flows smoothly from one level to the next. It is the financial authorities, as stakeholders in both frameworks, who must act as the interface between the national and international levels in order to guarantee comprehensive and coherent crisis management.

A multi-dimensional scenario, based on present-day threats

The G7 exercise was the result of almost 18 months of preparation, coordinated by the Banque de France, and involved **23 financial authorities in 4 different time zones** *(see Figure 3)* working on a common scenario that was severe, but based on present-day threats. It consisted of a **campaign to destabilise the international financial system**, orchestrated by a malicious group and based on the **deployment of wiper-type malware** in the information systems of numerous financial institutions around the world. This attack generated chain reactions due to the interdependencies between players and major disruptions to market activities, fuelled by extensive disinformation by hackers on social networks. In France, a cross-sectoral dimension was added to this "market-based" scenario, by simulating an **incident in the telecommunications sector** and additional impacts on **financial players' cash and electronic banking activities**.

1 See, for example, the October 2024 press release from the G7 Finance Ministers and Central Bank Governors, G7 Finance Ministers and Central Bank Governors' statements, Washington, DC, 25 October 2024 – Consilium (*europa.eu*).

2 See the 2023 exercise press release: 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 IT outage affecting millions of Windows systems worldwide following a faulty CrowdStrike software update in July 2024.

4 Malicious software whose aim is to destroy as much data as possible on the infected computer so that it cannot be recovered.

5 Malicious software that encrypts and steals data in order to demand a ransom from its victims.

6 Phishing involves sending malicious emails designed to deceive and defraud users. The aim is often to get users to divulge financial information, system identification information or other sensitive data.

7 Reconnaissance is the first stage of a hacking operation, during which the attacker gathers useful information about the target. This is done in order to identify the different vulnerabilities and define the possible means of attack.

8 A software exploit is a method or program used to exploit a security flaw in software or a computer system. In other words, it is a technique that allows an attacker to take advantage of a vulnerability to perform unauthorised actions, such as accessing data, executing code or taking control of a system.

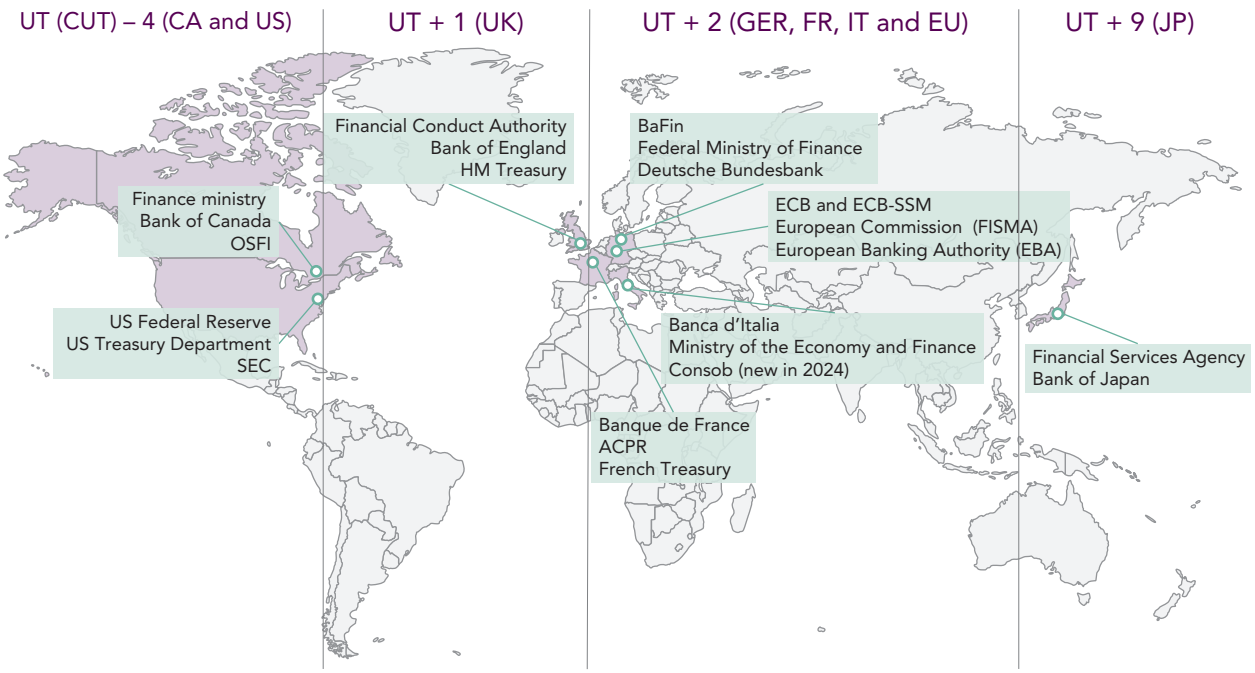
9 A method that involves deploying a virus or other malware through a supplier.

10 A Distributed Denial of Service (DDoS) attack aims to make a server inaccessible by sending multiple requests until it is saturated.

11 Pegasus is spyware designed to attack iOS and Android smartphones.

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".

Figure 3 2024 crisis exercise: 23 financial authorities of the G7, a mobilisation across 4 time zones



Source: Banque de France.
CA: Canada; DE: Germany; EU: European Union; FR: France; IT: Italy; JP: Japan; UK: United Kingdom; US: United States.
Notes: Universal time (UT); Coordinated Universal time (CUT).
ACPR, *Autorité de contrôle prudentiel et de résolution* (FR); BaFin, Federal Financial Supervisory Authority (DE); Consob, Commissione Nazionale per le Società e la Borsa (IT); DGT, French Treasury (FR); ECB, European Central Bank (EU); FISMA, Financial Stability, Financial Services and Capital Markets Union (EU); OSFI, Office of the Superintendent of Financial Institutions (CA); SEC, Securities and Exchange Commission (US); SSM, Single Supervisory Mechanism (EU).

Unprecedented mobilisation and ambitious avenues for the future

Over **2,500 professionals from the financial sector** participated in this two-day event, demonstrating the importance of this annual exercise for the financial community.

This exercise enabled each entity to test its contingency plans and once again highlighted the usefulness of the PRG system, which provides a **reliable framework for exchanges**, even in times of crisis when stress is heightened. The success of this exercise demonstrated the **maturity of the Paris financial centre** and **its high level of preparation**, just a few months before the start of the 2024 Paris Olympic and Paralympic Games.

The **avenues that were identified in the feedback phase**, such as further improving PRG tools and methodologies, strengthening international partnerships and working more closely with other strategic sectors to promote collective understanding and management of risks, will help to make the system increasingly professional.

3

A TRIED AND TESTED CRISIS MANAGEMENT FRAMEWORK THAT IS CONSTANTLY IMPROVING

3.1 Dedicated collaborative spaces to prepare for crisis management

Outside crisis periods, the PRG's role is to anticipate and prepare for future crises. To this end, the Group provides a forum for experts to discuss topical issues that have a major impact on members' activities. In recent years, for example, these spaces have been deployed in response to Russia's war on Ukraine, to provide an overview of the cyberthreats to the financial sector, or in response to the risk of a power outage in the winter of 2022-23.

The PRG's permanent working groups seek to continually improve crisis management preparedness by holding dedicated workshops on subjects such as anticipation, continuity of critical operations and crisis preparedness for major events such as the 2024 Olympic Games *(see Box 2)*.

3.2 Acting as a facilitator for the Paris financial centre

In the event of a major operational shock affecting the critical functions of the Paris financial centre, the PRG mobilises to achieve the following objectives:

- making a complete assessment of the Paris financial centre's situation by mobilising all stakeholders;
- encouraging exchanges between members to facilitate public-private cooperation;
- enabling sectoral coordination for the reconnection and recovery phases, for relevant activities;
- supporting internal crisis management within each entity by providing them with information collected from the market.

During the Covid-19 pandemic, the PRG met on several occasions to identify the impact and business continuity measures to be deployed by the financial sector. The main issues raised by the pandemic were as follows.

- The continuity of the cash industry, ensuring that ATMs were stocked, and the circulation of cash as a potential vector for the virus.
- The organisation of work to be put in place within the entities in order to continue operations during the lockdown period. Human resources were a crucial issue throughout the pandemic, with the need to separate critical staff whose jobs could not be performed remotely. The PRG also worked together to share information and best practices regarding the procedures to be implemented to ensure the safe return of employees to their workplaces.

In recent years, the PRG implemented an active watch on several occasions (Russia's war on Ukraine in 2022, urban riots in France in 2023 and CrowdStrike in 2024) in order to identify and monitor the potential consequences of these events for players in the financial system. The Group was in a position to take broader action had these events led to the disruption or stoppage of financial centre critical functions.

3.3 An ambitious work programme for the coming years

The crisis simulation exercise in April 2024 marked the culmination of the PRG's multi-year strategy focused on cyber risk, while paving the way for a **new action plan and the launch of new areas of work** centred on current threats and contemporary challenges. Beyond cyber risk, taking into account other types of operational threats, including through a **cross-sectoral approach**, will be key to strengthening the resilience of the Paris financial centre. Furthermore, the areas of work identified for the PRG will also be based on the work and priorities of the G7 Cyber Expert Group (CEG), to which the Banque de France contributes, in order to maximise the overall consistency of the authorities' initiatives.

As regards **improving the PRG's framework**, future work will focus in particular on:

- **perfecting crisis management tools** to ensure that they are safe, reliable and accessible;
- conducting an in-depth review of the **anticipation and post-incident reconnection and recovery phases**;
- **continually striving to optimise coordination** between crisis management frameworks at all levels (national, European and global);
- strengthening **cooperation with other strategic sectors, such as energy or telecommunications**, to take better account of interconnections with the financial sector, and thus prepare for even more consistent and comprehensive crisis management.

The PRG's new exercise strategy will capitalise on the successes of recent years, in particular the joint development of the scenario with partners in the PRG, to its increase the accuracy and realism. The PRG will draw on different exercise methodologies, and will strengthen cooperation with other financial centres and other sectors.

BOX

❷ The 2024 Olympic and Paralympic Games: preparation of the financial sector

The stakes for business continuity and the risks associated with the 2024 Olympic and Paralympic Games (OPG) prompted the Paris Resilience Group (PRG) to create a specific crisis management system, and step up its active watch for monitoring risks. As of 2023, the Group's secretariat (SGPR, at the Banque de France) worked with PRG members to prepare the Paris financial centre for the Olympic Games. This work led to the creation of a specific enhanced watch system, which was deployed during the Olympic Games, in order to **actively monitor the main events that could affect business continuity** in the financial sector and to **ensure that a dedicated and effective channel for exchanges between all stakeholders was put in place**.

The preparatory work identified four major challenges for the financial centre *(see figure)*: (i) the increase in cyber risk, due to the intense media coverage of the Games,[1] (ii) the security of bank branches located in Olympic areas; but also (iii) human resources management and access to sites, due to traffic constraints; and (iv) issues specific to the cash industry, concerning access to cash near competition venues.

To address these challenges, the SGPR implemented four actions.

i. **An information meeting at the end of 2023 to present the risks identified** as well as the crisis management measures implemented by government players before and during the Olympic Games.

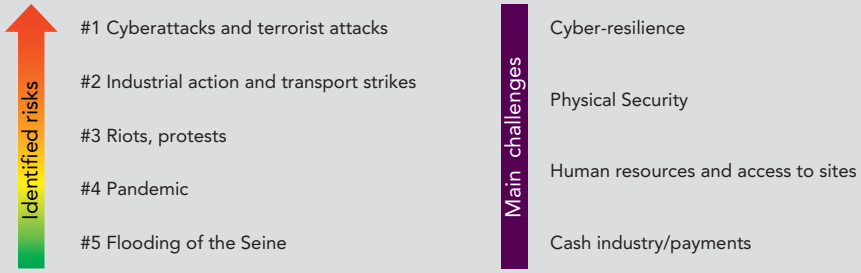
ii. **A strengthening of exchange channels** with a specific crisis management procedure set up between specialised players and the SGPR to share information on incidents, particularly during the period of the Games.

iii. **Operational crisis management preparation**, including PRG for the April 2024 exercise to simulate incidents involving cash, electronic money and telecommunications networks, in order to prepare those involved.

iv. **Lastly, the implementation of a stronger monitoring system during the Olympic Games** through weekly meetings with all the Group's stakeholders. This system, deployed from mid-July to mid-September 2024, was designed to centralise within a single body the information exchanged by the heads of the financial centre crisis units in their respective areas (communication, cash industry, liquidity and cashless payments). These points also encouraged information sharing between the financial industry and government departments on incidents or threats during the Games (cyber, terrorism, activism) in order to provide information for members' individual crisis management systems.

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

Main risks and challenges associated with the Paris Olympic Games for the financial sector



Source: Banque de France.

Overall, no major incidents were reported during the Olympic Games period, with the exception of problems with telecommunications (sabotage of fibre optic networks) at the start of the Games, which had no impact on the financial sector. **The enhanced monitoring system put in place and the support provided to the sector resulted in effective coordination and information sharing**. This coordination mechanism, based on a proactive approach, could be fully integrated into the PRG's crisis management tools, particularly for other major events or slower-onset crises, such as a flooding of the Seine or a new pandemic. The effective coordination among stakeholders during the Olympic Games provided valuable insights to enhance the PRG's crisis management framework and further strengthen information-sharing between public and private entities.

POSTFACE

After 20 years, a very positive record and a promising outlook

*After **20 years of collective work**, we are proud to report that we have profoundly **strengthened the operational resilience of the Paris financial centre**. Over the years, our Group has developed **a robust and agile crisis management framework** that brings together all the systemic financial players with a view to improving our ability to respond to major incidents in the sector and **maintaining financial stability**.*

*The reason why the framework is so mature is that, since 2005, we have **never rested on our laurels**. Mindful of the rapid evolution and sophistication of risks, we have systematically **put our procedures to the test**, confronting them with new realities and emerging issues and drawing inspiration from the best practices observed among our counterparts, both nationally and internationally. **Cyber risk**, due to its evolving nature and potential global impact, has required our **response system to adapt continuously**.*

*Without doubt, **organising regular crisis management exercises** has been one of the main ways in which we have been able to strengthen our framework over the years. These large-scale simulations strengthen our **ability to coordinate**, both within each organisation and authority and beyond, and to **make decisions in real time**. We have gradually been **increasing the level of ambition**, by improving the depth of the game and the realism of the scenarios, and by involving a growing number of players, culminating in the 2024 exercise. **Bringing together 8 jurisdictions and 2,500 professionals from the French financial sector** to address the same crisis scenario over two days is an unprecedented organisational feat. The **success of this exercise** lies not only in the simultaneous coordination of numerous entities around the world, but also in the **smooth collaboration between the G7 authorities and the effective dialogue between crisis management frameworks at various levels**.*

Similarly, every threat and every real incident in recent years has provided an opportunity to sharpen our vigilance and anticipate new scenarios. In addition to demonstrating that our framework is fully operational, these events – whether they be attempted cyberattacks, the failure of third-party service providers or social crises – have acted as catalysts, prompting us to develop our tools and adopt ever more rigorous practices.

*However, **we must not lower our guard**, and we must always **remain cautious** in the face of growing risks that could **bypass traditional defence mechanisms**. The ongoing digital transformation with the development of artificial intelligence, the increase in extreme weather events and the exacerbation of political and social tensions are all factors that could impact the continuity of critical operations.*

*So, while we recognise the progress that has been achieved, **we look to the future with humility**. Bolstered by our experience, we are ready to meet the challenges ahead, with the conviction that our collective commitment will help shape an **even more resilient financial system**.*

***Claudine Hurman**,*
Director, Innovation and Financial Market Infrastructure, Banque de France
Coordinator of the Paris Resilience Group

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

Managing Editor
Emmanuelle Assouan
Director General Financial Stability and Operations
Banque de France

Editor-in-Chief
Claudine Hurman
Director, Innovation and Financial Market Infrastructure
Banque de France

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

Technical production
Studio Création
Press and Communication Directorate
of the Banque de France

Contact
Innovation and Financial Market Infrastructure Directorate
Market Infrastructures Resilience and Research Division
Internal postcode: S1B-2327
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Printing
Navis
Printed in France

Legal deposit
February 2025
ISSN pending

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

The Paris Resilience Group Report can be downloaded for free on the Banque de France's website (*https://www.banque-france.fr/en/financial-stability/activities*).

www.banque-france.fr