

2012

**REPORT**  
**BY THE PARIS ROBUSTESSE GROUP**  
MARKET-WIDE EXERCISE  
ON 21 AND 22 NOVEMBER 2012

Report written at the Banque de France  
(Financial Stability Directorate)  
by the Secretariat of the Robustesse Group Coordination Unit

*A financial centre faces numerous constantly shifting threats to business continuity. To prevent these threats from materialising and minimise their impact, the Banque de France, the French Banking Federation, government representatives and some 15 systemically important institutions, including banks and post-trade infrastructures, have conducted regular exercises since 2006 to simulate crises that could seriously disrupt Paris financial centre. This has enabled the marketplace to demonstrate that it has the organisational structure needed to cope with a variety of crises, both physical, such as flood and epidemics, and logistical, such as a cyber-attack.*

*In November 2012, the Paris financial centre sought to assess its readiness to deal with new kinds of financial crime by choosing to test its responses to a cyber-attack. The main objectives of the exercise were threefold: check the ability to coordinate participants' business continuity plans; enable coordinated, consistent and uniform communication with the financial centre, media and the public; and check that links to government representatives, network operators and critical service providers were sound and effective.*

*The exercise was a success, with all objectives comfortably met. However, it showed that the ability of Paris-based institutions to coordinate measures and respond to constantly shifting threats could be improved. Action plans have been drawn up with this in mind and will be carried out through working groups and a Threat Monitoring Unit.<sup>1</sup>*

*Against the backdrop of the financial crisis, and as vigilance is stepped up in the face of increasingly complex threats, supervising and maintaining the robustness of the Paris financial centre is vital to the stability of the whole French and European financial system. For this reason, Paris will continue organising these exercises on a regular basis, while expanding their cross-border dimension.*

**Denis Beau**

*Chairman, Paris Robustesse Group*

*Director General Operations,  
Banque de France*

---

<sup>1</sup> Set up in January 2011, the Threat Monitoring Unit, which comprises the institutions that belong to the Robustesse Group, is tasked with monitoring the emergence of new risks that could generate serious operational crises on the Paris marketplace and with identifying new crisis scenarios.

## CONTENTS

INTRODUCTION	1
I – A MARKET-WIDE EXERCISE IN 2012 TO TEST RESILIENCE TO NEW FORMS OF CYBER-CRIME	3
II – CONDUCT AND HIGHLIGHTS	5
III – LESSONS	9
IV – OUTLOOK	10
ROBUSTNESS TERMS	11
ANNEXES	12

# The Paris financial centre has organised itself to cope with crisis situations

## 1| The Paris Robustesse Group ensures the resilience of institutions to an exogenous shock

The Paris Robustesse Group (*Groupe de place Robustesse*) was set up in 2005 at the initiative of the Banque de France to meet two objectives:

- resilience: improve the financial system's ability to cope with shocks affecting critical functions, such as payment systems, liquidity and support for financing the real economy;
- credibility: ensure that the Paris marketplace remains one of the financial centres that international investors recognise as one of the

*Chaired by the Director General Operations of the Banque de France, the Paris Robustesse Group comprises:*

- credit institutions and similar institutions (BNP Paribas Group, Crédit Agricole Group, BPCE Group, La Banque Postale, Crédit Mutuel-CIC, Société Générale and Caisse des Dépôts et Consignations Group);
- market infrastructures (LCH.Clearnet, NYSE Euronext, Euroclear, STET, GIE Cartes Bancaires, ABE Clearing);
- the Senior Official for Defence and Security, Ministry for Economy and Finance;
- the French Treasury;
- the French Banking Federation;
- the Banque de France;
- supervisory and regulatory authorities, including Autorité de contrôle prudentiel (ACP) and Autorité des marchés financiers (AMF).

most robust in the event of a major operational crisis.

The organisational structure in place to ensure robustness is based around a Coordination Unit and Crisis Units, whose composition and tasks are described in Annex 1.

## 2| Objectives

Set out formally in a 2007 annual report, the objectives of the Robustesse Group include “endeavouring to identify business continuity-related issues for the Paris financial centre. The Group's work is intended to help to ensure sufficient consistency in the measures taken by the main participants to strengthen the robustness and resilience of the financial system”.

Strengthening robustness, which is a key factor in the financial centre's attractiveness, is designed to ensure that a major disaster does not lastingly disrupt the operation of the financial system. The idea is that in the event of a major crisis, the financial sector, which forms a central component of our economy, must be able to cope even if critical functions are completely paralysed.

Five objectives have been identified:

- detect and classify alerts relating to an event, then set in train appropriate measures;
- draw up a full and overarching assessment of the financial centre's situation and provide the assessment to participants;

- establish and maintain dialogue with government;
- take decisions on possible collective measures and make choices in terms of managing limited resources;
- take decisions on crisis communications.

### 3| An exercise-based strategy to assess the robustness of the Paris financial centre

Basing its approach particularly on the analyses prepared by the Threat Monitoring Unit, the Robustesse Group is continuing with work aimed at preparing a common reference framework of scenarios that will characterise a broad range of crisis situations and assess their impact not just on financial institutions but also on network operators.

#### 3|1 Exercise scenarios: tools for measuring the resilience of the financial centre

The crisis scenario plays a vital role in determining the level of resilience that must be achieved to ensure the robustness of the financial centre, in identifying the appropriate resources and in making sure arrangements are consistent.

But no portfolio of scenarios will ever be exhaustive, regardless which reference framework is available or which methods are used. By nature, the various circumstances in which a crisis may arise are unpredictable and may combine in an infinite number of ways. Even so, some crises produce similar effects and may be grouped together according to impact classifications.

A basic portfolio of scenarios has thus been defined, with the aim of selecting enough different ones to cover the wide range of possible situations.

#### 3|2 A common reference framework

Eight different generic scenarios have been selected for their representativeness:

- general transport strike;
- River Seine flood;
- pandemic;
- terrorist attack;
- widespread power outage;
- industrial incident or nuclear/radiological/biological/chemical attack;
- failure of a “critical” service provider;
- cyber-attack.

The list may of course be changed to reflect the emergence of new threats.

The market-wide exercise on 21 and 22 November 2012 formed part of the exercise-based strategy that the Paris financial centre has pursued in past years. Past simulations have included:

- widespread power outage in 2008;
- an A/H1N1 flu pandemic in 2009 (in a real-life situation);
- a 100-year flood of the Seine in 2010;
- an unannounced general mobilisation of the Robustesse Group in 2011.

*The market-wide exercises, which are designed to assess the robustness of the Paris centre's critical processes, are not the same as bank stress tests. The latter simulate extreme but plausible economic and financial conditions to examine the impact on banks' financial positions and compliance with prudential requirements and to measure banks' ability to withstand such situations.*

# A market-wide exercise in 2012 to test resilience to new kinds of cyber-crime

## 1| Advance preparation by steering committees

To prepare for the exercise, the Cross-Market Group used a service provider that in turn relied on two steering committees.

An Exercise Committee (COEX) (cf. composition in the Annexes), drawn from the Coordination Unit, which met six times before the exercise to:

- determine the objectives and expectations;
- decide on the scope;
- decide on execution procedures;
- monitor progress.

A Validation Committee (COV) (cf. composition in the Annexes) drafted the script and decided on inputs to run the exercise and make it credible.

## 2| A scenario centred on a cyber-attack

The exercise scenario was based on a cyber-attack on the internal platforms used by participating institutions to exchange financial transactions. The idea was that the attack would paralyse certain critical operational processes, with collateral effects particularly on interbank payments, back offices and institutions' accounting systems, but also on clearing houses.

Further, the attack would seriously disrupt operations in the Paris financial centre.

The scenario was extended to include a public transport shutdown to incorporate an outside factor adding to the disruption of the financial centre.

Several combined factors contributed to the realistic nature and severity of the scenario:

- the duration of the exercise, which took place in real time over two separate half-days;
- large-value transfers with an unusual frequency;
- a large volume of unreconciled buy and sell orders;
- an attack on the *Châtelet-les-Halles* underground train station;
- messages and videos sent by a group of activists and picked up by the media (TV especially) and online (Twitter, Facebook and Youtube).

## 3| A scenario likely to involve different business areas

The aim of the exercise was to involve different people within the institutions and test their coordination – even interaction – within the Paris financial centre's crisis management system.

#### 4| A theme that is a key concern for many financial centres

By selecting this scenario, the Paris financial centre was looking to test its readiness to cope with new forms of financial crime.

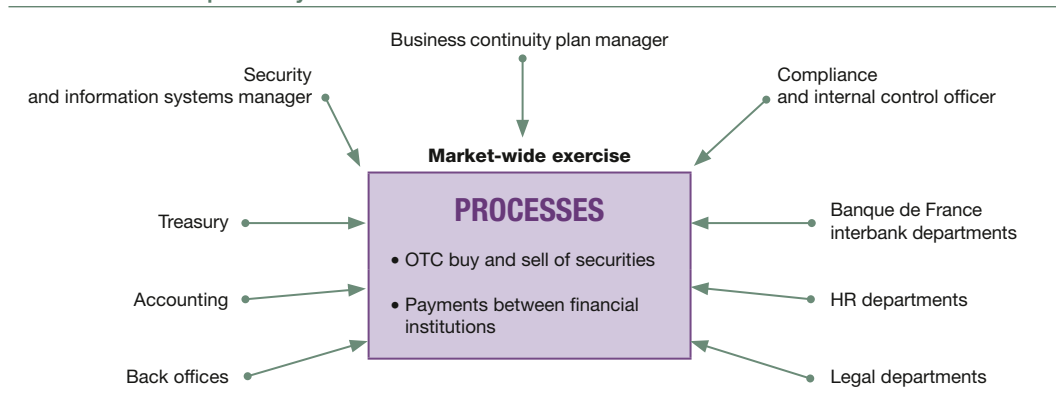
Given actual events in recent years, Europe’s major financial centres, including London and Rome, have also tested this type of

scenario, showing that cyber-terrorism is a major concern for international financial centres.

But the objective of this exercise was also to consider the mechanisms used to respond to all types of threat, and to examine the effectiveness of the organisation and procedures put in place to cope with a crisis of a different sort from those tested previously.

#### Diagram 1

Business areas impacted by the exercise scenario



## Conduct and highlights

Broad participation in the exercise, which took place over two half-days on 21 and 22 November 2012, involved:

- members of the Robustesse Group, including market infrastructures, banks, Caisses des Dépôts et Consignations Group, the French Banking Federation, regulatory authorities, the Banque de France, government authorities, Market Crisis Unit - Liquidity (CCP-L) and Market Crisis Unit - Communication (CCP-Com);
- the National Agency for Information Systems Security (ANSSI) as government expert;
- the service provider as coordinator and observer.

NB: the Market Crisis Unit – Cash (CCP-F), which was not involved operationally in the exercise, nevertheless took part in the Coordination Unit's conference calls.

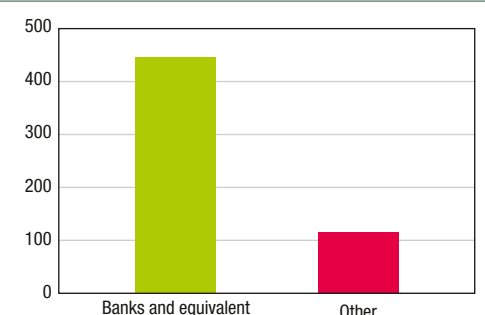
### 1| Major bank involvement

Almost six hundred people from the participating institutions were involved in the exercise, with the actual number of active participants naturally varying according to the nature of the business areas affected and the impacts sustained. Five banks mobilised over 60 people, with one of these institutions getting over 100 people involved.

Banks were the main participants in the exercise because the theme and scenario had a direct impact on their critical processes. Regulatory authorities (ACP and AMF) and market infrastructures were less affected.

**Chart 1**

Persons assigned to the exercise



*Banks and equivalent:*

*BNP Paribas Group, Crédit Agricole Group, BPCE Group, La Banque Postale, Crédit Mutuel-CIC, Société Générale and Caisse des Dépôts et Consignations (CDC) Group.*

*Other:*

*LCH.Clearnet, NYSE Euronext, Euroclear, STET, GIE Cartes Bancaires, ABE Clearing, French Treasury, the French Banking Federation, the Banque de France, General Secretariat of the ACP and the AMF.*

### 2| Institutions used the exercise to assess the impact of a cyber-attack on their critical processes

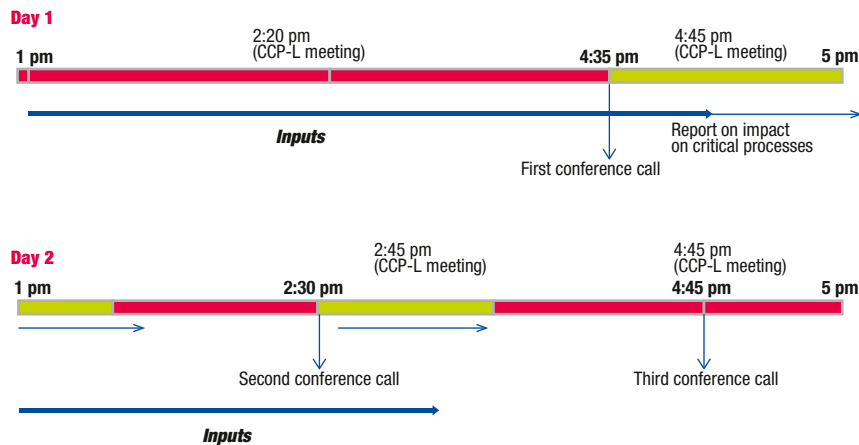
The exercise was an opportunity for participants to conduct a full-scale assessment of the consequences of an attack on the financial system and to identify the business areas and marshal the resources needed to manage the crisis.

In this respect, participants agreed that the objectives of the exercise held on 21 and 22 November 2012 were met.

The scenario had a broad impact on internal control and operational risk management systems, information systems (IS) and securities/cash operations. Treasury and payment instruments were affected, but to a lesser degree.



**Chart 2**  
Conduct of the exercise over two half-days

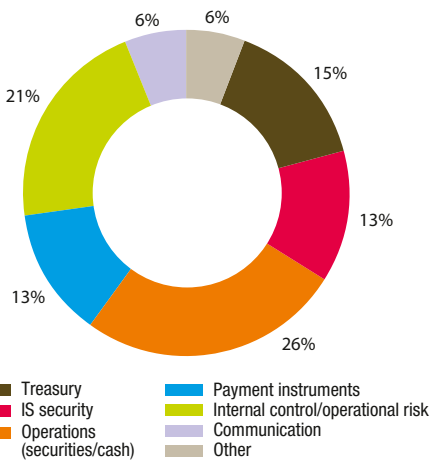


Note: CCP-Com also organised conference calls as needed.

The majority of participants felt that the scenario was realistic, notwithstanding some concerns about the plausibility of simultaneous attacks.

In terms of mobilising resources, participants found that their internal control and IS security teams were activated swiftly, within 10-30 minutes of the start of the exercise. It was unanimously agreed that the teams were involved at the right level and that internal coordination was effective.

**Chart 3**  
Business lines impacted by the exercise within participating institutions



The portion of the exercise dealing with an explosion at the *Châtelet-les-Halles* train station did not arouse particular interest because of its limited impact on personnel.

### 3| The Coordination Unit manager organised crisis management, working in conjunction with the Market Crisis Units and Coordination Unit members

Using the tools at its disposal to mobilise personnel, announce a conference call (via a call centre) and exchange information, the Coordination Unit kept up a sustained pace as it managed the crisis. In part this was because of the number of inputs: the exercise coordinator introduced 39 inputs in all, compared with 18 during the last market-wide exercise involving a River Seine flood.

The manager of the Coordination Unit, who is the Banque de France’s Financial Stability Director, aided by his deputy and the Coordination Unit secretariat, organised three conference calls.

During that time, the internet-based crisis management tool allowed participants to quickly exchange information (reports on the impact level on critical processes, problems)

and enabled the manager to announce the measures taken on an ongoing basis.

The first conference call was designed to assess the initial impact of the crisis. Participants were asked to report on the impact on critical processes, making it possible to prepare a market-wide assessment by the start of the second afternoon.

During the second half-day, institutions provided additional information on the development of the crisis. CCP-L and CCP-Com gave details on actions taken in their respective areas to neutralise the impact of alerts and technical damage to payment platforms.

#### 4| The Coordination Unit established a crisis exit strategy

At the end of the second half-day, crisis exit solutions were determined based on the measures taken by institutions and Crisis Unit

decisions (cf. Boxes). The manager was thus able to coordinate with participants when proposing steps to neutralise the consequences of the attack.

The Liquidity and Communication Crisis Units provided the manager and the Coordination Unit with targeted and relevant expertise given the nature of the crisis. They mobilised their members and, through their actions and information reporting initiatives, promoted the introduction of a coordinated market-wide action plan.

Return to Business As Usual (BAU) was the trickiest phase of the exercise given the technical constraints, which went beyond the Coordination Unit's operational framework.

The crisis exit was achieved through a collective action plan covering, in particular, the terms for CCP-L to sort transactions, and the introduction of an IS task force created around the French Banking Federation, banks and Caisse des Dépôts et Consignations.

#### Box 1

##### CCP-Liquidity

*CCP-L met twice on the first day. All the institutions belonging to CCP-L were represented and participated in the meetings. The four members responsible for chairmanship and vice-chairmanship of the CCP-L passed on information through the various channels available. These meetings made it possible to gain an overall, coordinated view of the situation and crisis management expectations.*

##### First day

*The first crisis conference call (2:20 pm – 3:00 pm) was used to determine the steps that major direct participants in Target2<sup>1</sup> should take to limit the incident. Most affected participants shut down their applications for managing outgoing large-value transfer flows, while the others stopped their exchanges on payment platforms.*

*The meeting was also used to decide whether to implement additional back-up measures.*

*The second crisis conference call (4:45 pm– 5:15 pm) was an opportunity to get a precise update on the situation and to prepare for the end-of-day close on Target, which took place without incident on 21 November at 6 pm.*

*CCP-L did not deem it necessary to ask the European Central Bank to delay the end-of-day close. However, in a real-life situation of the same sort and given the uncertainties involved in this type of crisis, delaying the end-of-day close would have been essential.*

<sup>1</sup> TARGET2 is the real-time gross settlement (RTGS) system for the euro developed and run by the Eurosystem.

*As long as the origin of the fraud was not clearly identified, ring-fenced and controlled, CCP-L agreed that banks should confine themselves to processing critical transactions arising on the morning of 22 November 2012.*

### **Second day**

*CCP-L also met twice on the second day:*

*2:45 pm: take stock of efforts to rebuild systems and forecast restart time.*

*4:45 pm: give the green light to reopen participants' systems and move flows, and take stock of efforts to rebuild systems and forecast restart time.*

## **Box 2**

### **CCP-Communication**

#### **First day**

*A conference call of the full CCP-Com was held at 3 pm by the representatives of the Banque de France's Communication Directorate.*

*After the conference call, it was decided that talking points should be made available to institutions by the Banque de France on the crisis management site, with the agreement of the French Banking Federation, to ensure consistent and uniform market-wide communication. Institutions were able to use these talking points by 4 pm.*

#### **Second day**

*CCP-Com announced that the Banque de France would prepare a press release by 3 pm.*

*The full CCP-Com began a conference call at 3:30 pm:*

- *12 participants took part out of the 15 institutions contacted;*
- *discussions covered the position to adopt vis-à-vis social media, recommendations were made (reminder of the rules of prudence and reserve for employees, suspended access to social networks).*

*A market-wide press release covering the latest developments was made available on the crisis management site managed by the Banque de France between 4 pm and 5 pm and updated at the end of the crisis.*

*The Banque de France took charge of responding to requests for TV interviews.*

# Lessons

The 2012 exercise made it possible to make sure that Coordination Unit members were able to meet the objectives of the Robustesse Group, namely:

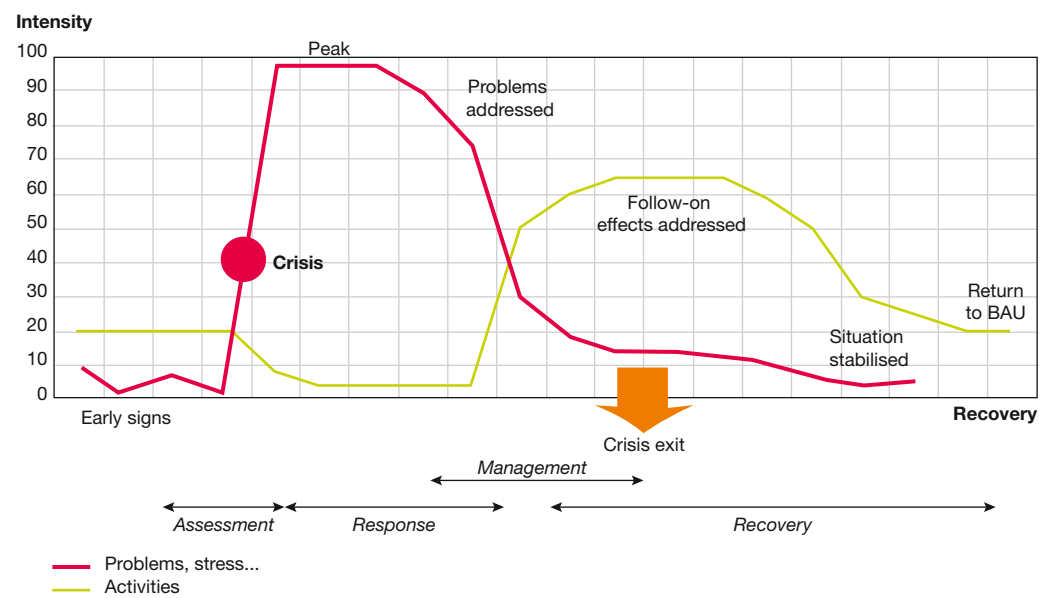
- establish an assessment based on information from participants;
- activate contacts and coordinate with Crisis Units and partners outside the sector to address problem situations;
- coordinate decisions with other participants, especially in terms of determining and applying the crisis exit plan.

The centre’s main financial participants managed to activate their individual continuity plans, internal control systems and information control systems. They also successfully tested their ability to trigger a market-wide action plan rapidly and in a coordinated manner to limit the scale and duration of the disruption to the financial system.

However, coordination between participants (manager, Crisis Units, participants) needs to be improved to make exchanges smoother and establish the procedures for BAU.

Working groups were set up to identify the lessons from the market-wide exercise on 21 and 22 November 2012.

**Chart 4**  
Diagram of crisis scenario



## Outlook

The individual and collective lessons learned from the market-wide exercise of November 2012 provided confirmation to the members of the Coordination Unit of their vision of major operational crises. The unit's members expressed their determination to conduct more tests with a scalable technical component.

The frequency and sophistication of cyber-attacks argue in favour of closely tracking new kinds of cyber-crime and identifying the resources needed by the Coordination Unit to prevent these risks from spreading to the Paris financial centre.

Accordingly, the Coordination Unit will pay close attention to the level of involvement of each of its members in future exercises.

A proposal was put forward to conduct a simulation exercise focusing on one or more business areas to promote rotation of specialists among participants.

The Threat Monitoring Unit, which provides a forum for exchanging experiences and monitoring threats, will be asked to provide the Robustesse Group with its thoughts on the emergence of new risks and on new crisis scenarios.

The issues related to major operational crises are becoming increasingly international because financial centres are interconnected. In consequence, the Robustesse Group will make contact with similar bodies and authorities in other European countries to explore the possibility of joint exercises.

**Table 1**  
Robustness terms

Term	Explanation
<b>Adverse event</b>	Any event with an accidental, natural or criminal cause that disrupts or prevents normal operation for long enough to significantly affect the critical processes of a bank, business area or assignment.
<b>Alert</b>	Formal notification of: <ul style="list-style-type: none"> <li>- an adverse event*;</li> <li>- an incident* that could give rise to an adverse event*;</li> <li>- an emergency (a flood occurring every 100 years).</li> </ul>
<b>Business as usual (BAU)</b>	Resumption of normal business activities.
<b>Business continuity</b>	Set of procedures designed to ensure that critical processes* can be maintained regardless of the circumstances, especially in the case of an adverse event* affecting the information system, buildings or personnel.
<b>Business Continuity Plan (BCP)</b>	Set of plans drawn up preventively and always available. The BCP is activated by the Crisis Unit* following an alert* or adverse event*. Each business area prepares a BCP.
<b>Business impact analysis</b>	Assessment of: <ul style="list-style-type: none"> <li>- financial impact of direct losses (misappropriation of funds, fraud, errors) and indirect losses (reconstruction of systems);</li> <li>- impact on image (lost credibility, court action).</li> </ul>
<b>Crisis</b>	Sudden event causing major losses and damage, forcing one or more critical activities to be stopped or an overall organisation to be shut down, having long-term impacts and requiring the use of the Crisis Unit and, where applicable, a back-up site.
<b>Crisis exit</b>	Phase when the crisis is exited and the process of gathering feedback begins, leading to changes to the BCP.
<b>Crisis unit</b>	Multi-disciplinary group of decision-makers and experts brought together in a crisis to: <ul style="list-style-type: none"> <li>- assess the situation;</li> <li>- estimate the possible consequences;</li> <li>- decide on measures to take;</li> <li>- mobilise the resources needed to return to an acceptable level of activity;</li> <li>- act as the interface for operational teams dealing with the crisis;</li> <li>- coordinate actions;</li> <li>- handle crisis communications with other participants.</li> </ul>
<b>Critical process</b>	Process that, if interrupted, must be restored to prevent the entity from suffering heavy losses or other damaging impacts.
<b>Incident</b>	Any event that affects or could affect normal operation and that requires a response by personnel or automated systems.
<b>Resilience</b>	Ability of a participant in the financial industry, a financial authority or a financial system to absorb the impact of a major operational disruption and continue critical operations or services.
<b>Robustness</b>	Ability of a participant in the financial industry, a financial authority or a financial system to remain operational during a period of major operational disruption.

**CONTENTS**

1	ORGANISATION OF THE PARIS FINANCIAL CENTRE	A1
2	EXCERPTS FROM REGULATION 97-02 OF 21 FEBRUARY 1997	A4
3	COMPOSITION OF STEERING COMMITTEES	A6
4	COORDINATION UNIT SECRETARIAT	A7
5	CATEGORIES OF INPUTS AND SYSTEMS FOR EXCHANGING INFORMATION DURING THE EXERCISE	A8

## Annex 1

### Organisation of the Paris financial centre

The Coordination Unit, working to ensure the robustness of the Paris financial centre

#### Manager

In the event of a major operational crisis, the Banque de France's Financial Stability Director is in charge of managing the Coordination Unit, aided by a secretariat provided by the Banque de France.

The manager is tasked with:

- deciding whether to activate the Coordination Unit or have it stand down;
- providing the crisis secretariat with analytical information supporting this decision;
- coordinating the Coordination Unit based in particular on the briefing sheet and contributions from members;
- preparing a complete and overall assessment of the situation;
- building a consensus and preparing collective decisions; prioritising the collective needs of the financial centre and informing government about these needs, especially in terms of limited resources.

The manager is required to conduct the following consultation and coordination activities:

- submit specific questions to the members of the Coordination Unit, especially the chairs or vice-chairs of specialised Crisis Units (see below);
- invite one or more representatives of market authorities (ACP, AMF) or any other person who can provide answers to the questions of the Coordination Unit;
- coordinate and monitor actions;
- coordinate feedback-gathering and implementation of improvement measures validated by the Paris Robustesse Group following the crisis or exercise.

#### Members

Representatives officially appointed by institutions, the members are in charge of communication within their entity and are in constant contact with the manager to provide information or implement measures determined during the crisis.

They are also in charge of reporting to the secretariat of the Coordination Unit on the impact of the crisis within their entity via a common crisis management tool. These reports must be provided to the manager as needed during the crisis to ensure that the whole unit has an exhaustive map of the identified risks and necessary measures.

Some participants (FBE, ACP, AMF, HFDS) play a specific role in providing the link to institutions that are not members of the unit. Accordingly, their reports must incorporate information from the institutions that they represent or supervise.



The Market Crisis Units (CCPs) are forums for decisions, consultations and information on crisis management.

The CCPs are part of the Paris financial centre's robustness framework. Comprising representatives of the Banque de France and institutions belonging to the Robustesse Group (cf. below), they are involved in several areas that are viewed as critical to business continuity:

- communication;
- liquidity;
- cash.

Depending on the nature of the crisis, the CCPs may be activated individually or jointly. They bring their expertise, action and decision-making scope to bear to help the Coordination Unit identify the impacts of the crisis, the measures to take and the requirements for a return to Business as usual.

## Market Crisis Units (CCP) factsheets

	Market Crisis Unit - Communication (CCP-Com)	Market Crisis Unit - Liquidity (CCP-L)	Cellule de crise de place fiduciaire (CCP-F)
<b>Members</b>	Co-chaired by the Banque de France (BdF) and the French Banking Federation (FBF), CCP-Com has representatives from the ACP, the main banking groups (BNP Paribas, BPCE, Crédit Agricole, Crédit Mutuel/CIC, La Banque Postale and Société Générale), Caisse des Dépôts et Consignations, market infrastructures (STET, Euroclear, LCH Clearnet, NYSE Euronext, ABE Clearing, GIE Cartes Bancaires) and government	CCP-L, which is steered by the BdF and a banking industry representative, has representatives of the Banque de France, LCH Clearnet and Euroclear France, BNP Paribas Group, Crédit Agricole, Crédit Mutuel/CIC, La Banque Postale, BPCE Group and Société Générale Group.  Its membership may be extended if necessary to include other systems (ABE Clearing, STET, NYSE Euronext, Visa France, GIE Cartes Bancaires) or institutions.	CCP-F, which is steered by the BdF, has a representative of the Ministry for Economy and Finance, IEDOM and the French Banking Federation, as well as a representative from each of the major banking networks participating in the Cash Robustness Coordination Unit, La Banque Postale, the Commerce and Distribution Federation (FCD) and the Federation of cash-in-transit firms (Fedesfi)
<b>Secretariat</b>	Communication Directorate of the Banque de France	Payment Systems and Market Infrastructures Directorate	Cash Activities Directorate of the Banque de France
<b>Objectives</b>	<ul style="list-style-type: none"> <li>Coordinate communications between reporting parties and the Robustness Coordination Unit in the event of an operational crisis</li> <li>Raise participant awareness about market-wide communication</li> </ul>	<p>CCP-L has a dual role to play in the Target2 environment:</p> <ul style="list-style-type: none"> <li>be proactively involved in managing liquidity issues, especially in the context of new system or service launches,</li> <li>respond in the management of crises caused by technical or banking problems at the level of Target2, outside systems or participants, with an impact on liquidity, or presenting systemic risk.</li> </ul> <p>CCP-L relies on the need for coordination between securities and cash areas both within institutions and at the level of French and European market infrastructures.</p>	<p>CCP-F centralises local information through its network of branches with a cashier department.</p> <p>There is no standing local crisis management unit: at CCP-F's recommendation, local BdF directors may set up a crisis management unit including banks, cash-in-transit firms and major retailers in their area.</p> <p>In the event of a crisis leading to consultation of the Coordination Unit, CCP-F provides the information that the manager needs (from government departments, the network or its departments).</p>
<b>Meetings</b>	CCP-Com meets as needed in a crisis and at least once a year for discussion, with a view to raising awareness about market-wide communication	CCP-L meets regularly and as needed in the event of individual or collective problems facing members that could affect the liquidity of the financial centre.	CCP-F meets as needed in a crisis and at least once a year to test its ability to mobilise.

## Annex 2

### Excerpts from Regulation 97-02 of 21 February 1997 on the internal control of credit institutions and investment firms

#### Article 4

For the purposes of implementing this Regulation the following definitions shall apply:

- Business continuity plan: a set of measures designed to ensure, according to various crisis scenarios including extreme shocks, the continuation, where appropriate temporarily in degraded mode, of essential or important services or other operational tasks for the institution then the planned resumption of activities;
- essential or important services or other operational tasks or any provision of services where an anomaly or failure in its performance could seriously harm the ability of the reporting institution to comply on a permanent basis with the terms and requirements of its approval and with those pertaining to the exercise of its business, financial performance or the continuity of its services and activities.

#### Article 14

Reporting institutions shall determine the level of computer security deemed necessary with regard to the requirements of their business areas. They shall ensure that this level is maintained and that their information systems are appropriate.

In particular, control of information systems shall ensure that:

[...]

back-up procedures are available to allow business operations to continue in the event of serious systems failure;

#### Article 14-1

In addition to the provisions set forth at Article 14 of this Regulation, reporting institutions must:

- have business continuity plans;
- provide for regular assessment of their organisation and the availability of their human, property, technical and financial resources from the standpoint of business continuity-related risks;
- ensure the coherence and effectiveness of business continuity plans in the framework of a master plan which incorporates the objectives defined by the executive body and, where appropriate, the decision-making body.

### Article 37-2

Reporting institutions that outsource an essential or important service or other operational task within the meaning of Article 4.q) and r) of this Regulation remain fully liable for compliance with their obligations and must in particular comply with the following provisions:

3) Reporting institutions shall ensure, in their relations with outside service providers, that the latter:

[...]

c) implement contingency mechanisms in the event of serious difficulty affecting continuity of service, or ensure that their own continuity plan takes account of a scenario in which it is impossible for the outside provider to provide the service.

### Article 39

At regular intervals and at least once a year, the executive body shall inform the decision-making body and, where appropriate, the audit committee:

[...]

of the measures taken to ensure business continuity and assess the effectiveness of the arrangements in place;

### Article 40

Reporting institutions shall draw up, in the same conditions, documents that set out the means intended to ensure that the internal control system operates smoothly, including:

[...]

the procedures relating to the security of information and communication systems and to business continuity plans;

## Annex 3

### Composition of the steering committees

#### Exercise Committee

BANQUE DE FRANCE  
BNP PARIBAS GROUP  
CRÉDIT AGRICOLE GROUP  
SOCIÉTÉ GÉNÉRALE GROUP  
ABE CLEARING  
NYSE EURONEXT  
GIE-CARTES BANCAIRES  
LCH.CLEARNET  
STET  
MINISTRY FOR ECONOMY AND FINANCE  
THALES

#### Validation Committee

BANQUE DE FRANCE  
BNP PARIBAS GROUP  
BPCE GROUP  
EUROCLEAR FRANCE  
MINISTRY FOR ECONOMY AND FINANCE

## Annex 4

### Coordination Unit Secretariat

Nathalie Bédier  
Laurent Clerc – CU Manager  
Olivier Jaudoin – CU Co-Manager  
Caroline Keribin  
Bernard Palmarini  
Olivier Vigna

A7

## Annex 5

### Categories of inputs and systems used to exchange information during the exercise

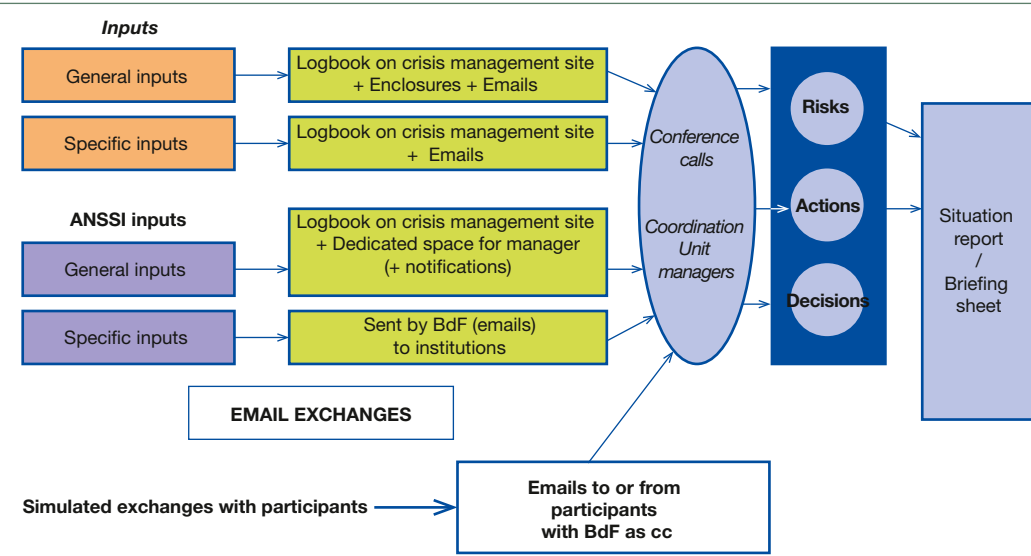
**Table A1**  
Categories of inputs

	Recipient function	Description	Abbreviation
General inputs	Operational staff	Inputs intended for operational staff in all institutions.	GO
	Communicators	Inputs intended for communicators in all institutions.	GC
	Operational staff and communicators	Inputs intended for operational staff and communicators in all institutions.	GT
Specific inputs	Operational staff	Inputs intended for operational staff in some institutions.	SO
	Communicators	Inputs intended for communicators in some institutions.	SC
	Operational staff and communicators	Inputs intended for operational staff and communicators in some institutions.	ST

GO: General inputs, operational staff  
 GC: General inputs, communicators  
 GT: General inputs, operational staff and communicators  
 SO: Specific inputs, operational staff  
 SC: Specific inputs, communicators  
 ST: Specific inputs, operational staff and communicators

**Chart A1**

#### Systems used to exchange information during the exercise



The Report by the Paris Robustesse Group  
can be downloaded for free  
from the Banque de France website  
([www.banque-france.fr](http://www.banque-france.fr)).

**Electronic publication**

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

**Director of publication**

Denis Beau

**Managing editor**

Sylvain Josserand

**Produced by**

Communication Directorate  
Economic Publications Department