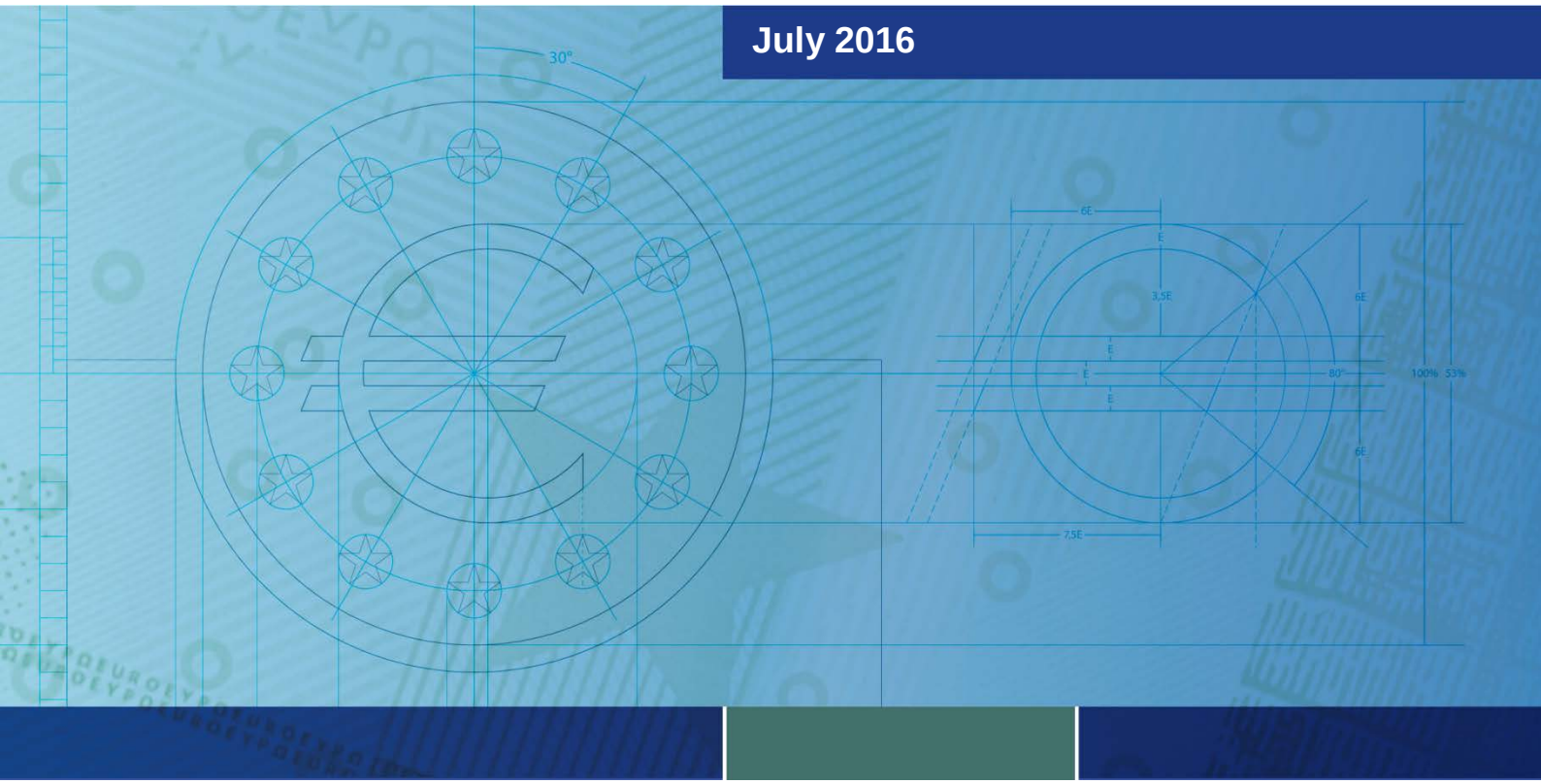
EUROPEAN CENTRAL BANK

EUROSYSTEM

TITUS

Crisis communication exercise for euro area financial market infrastructures report

July 2016



Contents

Foreword

The financial market infrastructures (FMIs) of the euro area are critically important, providing functions the public and the financial system rely on every day. Europe's monetary and financial stability depend on the orderly functioning of these infrastructures. Payment systems allow the purchase of goods and services and the transmission of salaries. Securities settlement systems underpin the operation of stock and bond markets. Central counterparties help to simplify the financial network and protect financial market participants from counterparty default losses. And all of these FMIs operate within a global environment of multiple currencies, where foreign exchange transactions are carried out on a daily basis. Such infrastructures exist within a complex operational network, with a high degree of interdependency. As operators and overseers, it is vital that we ensure the operational resilience of this network on a sector level, and where disruptions do occur we can ensure that FMIs continue to operate or recover quickly, minimising any adverse impact on the functioning of the system as a whole.

In the light of this, I am very pleased that the Eurosystem has carried out a large-scale market-wide business continuity exercise, simulating a cyber-attack on a major, systemically important payment system (SIPS), and involving all TARGET2 central banks (operators and overseers), the other three SIPS located in the euro area (EURO1, STEP2-T, CORE(FR)), 29 banks in their capacity as FMI participants, the New York-based Continuous Linked Settlement System (CLS) for the settlement of foreign exchange transactions (including the euro), and the Federal Reserve Board and the Federal Reserve Bank of New York who acted as observers in their capacity as the overseers of CLS.

It is clear that cyber-attacks, amongst other scenarios, have the potential to cause significant disruption to the normal operations of the financial sector. This exercise was therefore designed to enable the authorities and major wholesale market participants in the financial sector to improve their crisis communication, both individually and collectively, to respond to a major disruption.

There were no "passes" or "fails"; the exercise was about enhancing the financial sector's ability to respond effectively by rehearsing its response arrangements, amending them where appropriate and identifying areas for further attention. Such market-wide exercises are vital to protect the resilience of the financial system.

Finally, I would like to thank the ESCB Market Infrastructure and Payments Committee and its Business Continuity Task Force for organising and successfully conducting this exercise.

Benoît Cœuré
Member of the Executive Board of the European Central Bank

Summary

The TITUS exercise, held on 4 November 2015, was a crisis communication exercise involving the Eurosystem's payment system oversight function, TARGET2 operators and all critical payment infrastructures processing the euro, including some of their major participants. The participants were confronted with a simulated cyber-attack on a major systemically important payment system (SIPS).

The exercise enabled the Eurosystem to evaluate its preparedness to carry out, effectively, its operational and oversight responsibilities during crisis events and provided assurance of the effectiveness of the different stakeholders' crisis management procedures for events with cross-border impacts. In essence, the exercise was designed to test the cohesiveness of the response of an important part of the financial market in order to understand and minimise the impact of a cyber-attack on the sector.

From an organisational perspective, the exercise ran smoothly. However, exercises of this kind are not simply about validating and rehearsing existing response arrangements; they always provide opportunities to identify areas for further improvement. This report outlines a number of findings and lessons learned that are being implemented in 2016. In particular, the overseers should clearly define their role during a crisis event; the criteria for the activation of the contingency arrangements should be explored further; the timeliness of communication flows between the FMI operators and their overseers should be improved; and the crisis communication frameworks of the relevant stakeholders should be aligned.

The SIPS operators and the European Central Bank's (ECB) Oversight function are addressing the findings on the basis of a dedicated action plan.

Feedback on the exercise has been positive and participants have stressed that such market-wide exercises should be organised on a regular basis, with an expanded and more challenging scope involving other types of FMIs, banks and other public authorities/regulators.

1 Introduction

One of the key elements in developing sound and efficient business continuity arrangements within the financial sector is to establish well-defined processes and procedures for effective crisis communication management. In this context, market-wide exercises, involving all relevant stakeholders, play an important role.

Accordingly, in the Eurosystem crisis communication exercise, "TITUS", which took place on 4 November 2015, participants were confronted with a simulated cyber-attack on a major SIPS.

The exercise involved the 24 central banks of the European Union (including the ECB) that are participating in, or connected to, TARGET2 (operations and oversight functions), the SIPS (EURO1, STEP2-T, CORE(FR)), 29 banks in their capacity as

participants in the FMIs, CLS, and the Federal Reserve Board and the Federal Reserve Bank of New York who acted as observers in their capacity as the overseers of CLS. More than 300 staff members and technical experts from all participating institutions were involved in this exercise.

2 Exercise objectives

The exercise focused on disruption in wholesale markets and the payments infrastructure supporting those markets as a result of a cyber-attack. The specific aims of the exercise were to:

1. enable the Eurosystem to evaluate its preparedness to carry out, effectively, its operational and oversight responsibilities during crisis events;
2. provide assurance of the effectiveness and identify areas for improvement of the stakeholders' crisis management procedures, including information flows between participants, decision making processes and external communication/media management;
3. verify the compatibility of stakeholders' and national crisis management procedures in the context of events with cross-border impacts by enabling FMIs to participate in industry-wide tests.

3 Scenario

To meet the exercise objectives, a scenario was devised that placed the sector under severe stress. The scenario was based on a concerted cyber-attack on a major SIPS with a software integrity impact but no data integrity impact. The scenario aimed to cause a significant disruption of the wholesale market and the supporting financial market infrastructure. The cyber-attack theme was considered very relevant given authorities' growing attention to cyber risk. The scenario allowed participants to explore the increasing interconnectedness of FMIs and cyber-attacks, which are becoming ever more sophisticated, more frequent and more severe for their targets, including financial institutions and financial market infrastructures.

On the day, all participants were in receipt of constant email injects that played out the scenario. The scenario was pre-prepared in the form of a playbook and aimed to create a dynamic and evolving scenario (on a minute-by-minute basis) that would challenge all participants. All participants were asked to react pro-actively to the injects they received via email, replicating how they would respond to the events in a real crisis situation.

All participants were actively engaged and contributed during the exercise. Teleconferences were launched by the SIPS operators and the overseers, to discuss the issues that arose and the crisis events triggered by the scenario. These included the activation of the SIPS contingency arrangements for different types of transactions, the settlement of ancillary systems and critical payments, and the

handling of media requests. Furthermore, there was interaction between the SIPS operators and the respective overseers in order to respond to the changing dynamics of the scenario on a real-time basis.

In addition, independent evaluators were assigned, at the level of all central banks and of the SIPS, to observe the participating stakeholders and to evaluate the exercise against the stated objectives.

4 Exercise findings

All in all, an analysis of the feedback received from the participants and of the independent SIPS evaluators' reports show that the TITUS exercise was successful and highly appreciated by all participants. It enabled SIPS operators, overseers and banks to test their crisis communication arrangements. Overall, the crisis communication arrangements worked well during the exercise.

The Eurosystem participants (the TARGET2 operator and central bank overseers) clearly knew how to act during an incident. However, the involvement of all euro area SIPS, CLS and some of their participants in the exercise enabled the Eurosystem to identify areas in its crisis communication and business continuity arrangements that will have to be enhanced going forward. For each of the exercise objectives, the following enhancements were noted:

Objective 1: Enable the Eurosystem to evaluate its preparedness to carry out, effectively, its operational and oversight responsibilities during crisis events.

1. The role of the overseer during a crisis situation should be more clearly defined to ensure that Eurosystem overseers can actively respond and communicate in a consistent manner.

2. In some cases, the contingency arrangements provided by SIPS should be reviewed to ensure that they can suitably address a range of extreme but plausible crisis scenarios; where needed, the criteria to activate and/or use such arrangements should be made clearer to all the relevant stakeholders.

Objective 2: Provide assurance of the effectiveness and identify areas for improvement of the stakeholders' crisis management procedures, including information flows between participants, decision-making processes and external communication/media management.

1. In some cases, the communication between the operators and the overseers could be enhanced.

Objective 3: Verify the compatibility of stakeholders' and national crisis management procedures in the context of events with cross-border impacts by enabling FMIs to participate in industry-wide tests.

1. The crisis communication frameworks for the overseers and the operators could be better aligned to ensure that the appropriate information is disseminated in

an efficient, timely, consistent and well-coordinated manner to the national central banks and the ECB.

5 Next steps

On the basis of the feedback received from the participants, the TITUS crisis communication exercise proved to be an overall success. It enabled the participating FMIs and the central banks to derive useful conclusions about their crisis communication arrangements. The key findings, some of which have been noted above, are being addressed by the SIPS operators and the overseers through dedicated action plans. The aim is to ensure that all parties take on board the findings and further enhance the effectiveness of their crisis communication plans in readiness for real crisis scenarios.

6 Future exercises

In their feedback after the exercise, participants stressed that such market-wide exercises should be organised on a regular basis. In particular, participants provided a number of useful suggestions for future exercises. Among these, participants suggested that future exercises should consider involving other types of FMIs (in addition to the SIPS and CLS), banks and other public authorities/regulators; developing more complex scenarios, which could use quantitative data, thereby making them more challenging; and giving participants a more active role throughout the scenarios. This feedback will be taken on board when preparing for such future exercises.

7 Annex – Participating financial institutions

Country	Bank
BE	KBC
BG	DSK Bank
DK	Danske Bank
DE	Deutsche Bank AG Commerzbank AG Citibank
EE	SEB Pank
IE	Allied Irish Bank
GR	Piraeus Bank
ES	Banco Bilbao Vizcaya Argentaria S.A. Banco Santander S.A.
FR	BCPE Société Générale BNP Paribas Crédit Agricole
IT	UniCredit S.p.A Intesa San Paolo
CY	Bank of Cyprus
LV	Swedbank
LT	AB SEB bankas
LU	Caceis Bank Luxembourg
MT	Bank of Valletta
NL	ING
AT	Raiffeisen Bank International
PL	PKO Bank Polski
PT	None
RO	UniCredit Țiriac Bank
SI	Nova Ljubljanska banka
SK	VUB
FI	Nordea Bank Finland

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

ISBN 978-92-899-2438-2
DOI 10.2866/530575
EU catalogue No QB-04-16-571-EN-N