EUROPEAN CENTRAL BANK

EUROSYSTEM

EUROSYSTEM ASSESSMENT REPORT ON THE IMPLEMENTATION OF THE BUSINESS CONTINUITY OVERSIGHT EXPECTATIONS FOR SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS

INTRODUCTION

Payment systems are part of the basic infrastructure required to allow market economies to function properly. The smooth functioning of payment systems is crucial for the practical implementation of the central bank's monetary policy and for maintaining the stability of and confidence in the currency, the financial system and the economy in general. Payment systems are exposed to a wide range of risks, including legal risks, financial risks and operational risks, which may result in losses for the system operator, the participants in the system or the public at large. The Eurosystem, via its oversight function, applies a number of standards and requirements to payment system operators in the euro area in order to assess whether they are satisfactorily addressing these risks.

In June 2006 the Eurosystem published its "Business continuity oversight expectations for systemically important payment systems)"[1] with the aim of ensuring sufficiently robust and consistent levels of operational resilience across payment systems processing the euro. These expectations specify in more detail what the Eurosystem expects from operators of systemically important payment systems (SIPS) in terms of compliance with the business continuity aspects of CPSS Core Principle VII.[2] They focus on business continuity strategy, planning and testing, as well as on crisis management. Some of the oversight expectations have an impact on critical participants in SIPS and the SIPS' third-party providers of critical services/functions.

The deadline set by the ECB's Governing Council for the implementation and testing of the business continuity oversight expectations by the system operators was end-June 2009. None of the system operators requested an extension of this deadline.

The payment systems operating in the euro area that have been classified by the Eurosystem as SIPS, and which are thus included in the scope of this assessment report, are TARGET2 and EURO1, as well as four retail payment systems, namely POPS (Finland), PMJ (Finland), CORE (France) and CSS (Netherlands).

The report summarises the results of the comprehensive assessment of the relevant systems against the business continuity oversight expectations.

1 APPROACH AND METHODOLOGY

Although the practical assessment of the payment systems' compliance with the business continuity oversight expectations was left to the relevant overseeing central bank, a harmonised approach has been ensured by basing all assessments on the "Guide for the assessment against the business continuity oversight expectations for SIPS" which was published by the ECB on 12 November 2007. This document aims to provide the Eurosystem's payment system overseers with clear and comprehensive guidelines for the assessment of the relevant systems and the preparation of oversight reports. The chosen approach promotes a level playing field for SIPS in terms of applicable oversight requirements and provides payment system operators with greater insight into overseers'

1 The BCOE can be accessed via the following link: http://www.ecb.europa.eu/pub/pdf/other/businesscontinuitysips2006en.pdf.
2 Core Principles for Systemically Important Payment Systems, Bank for International Settlements, January 2001.

concerns related to operational resilience. Furthermore, it gives system operators additional incentives to continue their efforts to mitigate or limit the operational risks that their systems may face and, ultimately, helps them to ensure the smooth functioning of their systems.

The assessment guide contains a comprehensive list of questions which are used to evaluate the extent to which the overseen entities fulfil the Eurosystem's requirements with regard to a number of key issues. The relevant central banks performed a first assessment based on information collected during the assessment process. For TARGET2 and EURO1, this work was led and coordinated by the ECB with the participation of a number of volunteering NCBs. The first assessments of the retail SIPS, each of which was conducted by the respective overseeing NCB individually, were subject to a subsequent peer review by volunteering euro area central banks to ensure the consistent application of the assessment guide.

2 OVERALL ASSESSMENT RESULT

Following the detailed analysis of the individual assessments performed by the central banks and the volunteering peer reviewers, it can be concluded that *the business continuity and crisis communication arrangements of the relevant systemically important payment systems are maintained at high standards by their system operators*. Nevertheless, for several of the systems assessed, further improvements were recommended in some areas of the individual business continuity and crisis communication arrangements. However, none of these areas for improvement pose a significant risk to the effective functioning of the overall business continuity framework of the systems that were subject to this oversight assessment.

The respective system operators were informed and agreed to take a number of actions to improve their existing business continuity and crisis communication arrangements on the basis of the oversight findings to achieve full compliance with the business continuity oversight expectations. The implementation of the recommendations will be monitored by the overseeing central banks and will be reported to the Governing Council of the ECB in a follow-up assessment report.

3 ASSESSMENT BY KEY ISSUE

3.1 KEY ISSUE 1: FORMULATION OF BUSINESS CONTINUITY OBJECTIVES

The aim of this key issue is to ensure that SIPS have a well-defined business continuity strategy and monitoring mechanism endorsed by the Board of Directors. Critical functions/services should be identified and processes within these functions/services categorised according to their criticality and impact. More importantly, business continuity objectives should aim at the recovery and resumption of critical functions/services within the same settlement day. All of the systems assessed were found to fulfil this oversight expectation.

The assessment process also revealed that for two of the payment systems assessed the procedures for reporting changes in the business continuity and crisis management arrangements to the Board could be improved, as otherwise the risk levels might exceed the risk tolerance approved by the Board. In the case of another system, it was found that the roles and responsibilities of the governance bodies with respect to the setting and assessment of the business continuity objectives were not clearly defined and described in the business continuity planning documentation.

Concerning the identification of critical functions/services in the payment system by the system operators, the assessment found that two of the systems should document these functions/services and the associated processes more clearly. In particular, for one of these systems it has been recommended that the system operator clearly describe in the system documentation the applicable recovery times for

the critical functions. Two other systems have also been requested to assess the criticality of the outsourced critical functions to third-party service providers.

The overall conclusion is that the assessed payment systems have sufficiently addressed the overseers' expectations related to this key issue, although improvements were identified and recommended to the respective system operators.

3.2 KEY ISSUE 2: DEVELOPMENT OF BUSINESS CONTINUITY PLANS

This key issue aims to ensure that business continuity plans implemented by the system operators envisage a variety of plausible scenarios, including major natural disasters, outages and terrorist acts affecting a wide area. It also aims to ensure that the overseen systems and their critical participants have a secondary site that enables the systems to meet their stated recovery objectives for the applicable plausible scenarios.

With respect to the identification of scenarios and the existence of a secondary site, all systems were found to be compliant with the oversight expectations. Concerning the location of the secondary site, there is significant variety across systems with regard to the distance between the primary site and the secondary site. However, all the systems were assessed to be compliant with the requirement that the two sites should have a different risk profile.

Concerning the remaining requirements of this key issue, two of the systems were advised to ensure that they are not fully dependent on a single third-party service provider for the provision of critical services. The central banks overseeing these two systems recommended that the respective system operators identify an alternative service provider for the provision of the specific critical services.

In addition, it was considered that one of the payment system operators should revise its business impact analysis process so as to include issues which might adversely affect the operation of the system as a consequence of a failure of one or more of its critical participants. Finally, the operator of another system has been requested to complete as soon as possible the ongoing work on the definition of critical participants and ensure that the associated risks are addressed in a timely manner.

The overall conclusion is that the assessed payment systems have adequately addressed the overseers' main expectations in relation to this key issue by identifying various plausible scenarios and critical functions/services, and by ensuring the existence of secondary sites for the systems and their critical participants/service providers.

3.3 KEY ISSUE 3: COMMUNICATION AND CRISIS MANAGEMENT

The aim of this key issue is to ensure that system operators have established crisis management teams and well-structured formal procedures to manage crisis events and internal/external crisis communication.

While the systems comply with most of the requirements of this key issue, some still need to enhance their compliance in this regard. In particular, the operator of one of the systems has been requested to amend its crisis management arrangements by better describing the various stages of a crisis and the criteria for activating the crisis procedures, including the definition of clear rules for the decision-making process during a crisis.

It was also observed that another system operator should define a procedure for the collection and sharing of information concerning the operational resilience and security of the system's critical participants. In addition, the operators of two

systems have been requested to assess the communication channels established between their participants and the local authorities. The establishment of communication lines between the relevant stakeholders would be very important and crucial for effective coordination during a crisis event.

Overall, the assessment process revealed that sufficient crisis management and communication procedures and arrangements exist in the assessed payment systems. Some improvements were identified for several of the systems, which the respective system operators should implement to fully comply with this key issue.

3.4 KEY ISSUE 4: TESTING AND UPDATING OF BUSINESS CONTINUITY PLANS

The aim of this key issue is to ensure the effectiveness of the business continuity plans implemented by the payment systems, through regular testing of each aspect of the plan. System operators are expected to perform full days of live operations from the secondary site, including participation in industry-wide tests. Periodically, these tests should also involve the participants running operations from their secondary sites. Business continuity plans should be periodically reviewed and updated by the system operators, and audited by an internal or external audit function to ensure that they remain appropriate and effective. Operators should also consider the partial disclosure of business continuity plans to external stakeholders such as other SIPS, overseers and banking supervisors.

As a result of this assessment, one of the systems has been requested to extend the scope of its testing by inviting its participants to participate in business continuity tests. The operator of another system has been advised to investigate the possibility of taking part in industry-wide testing of its business continuity arrangements, in coordination with the Eurosystem. This will ensure that euro area-specific scenarios are adequately addressed by the system in question.

It was also observed that, owing to the recent launch of the operations of one of the systems assessed, the respective system operator had not yet performed an external review of the system's business continuity arrangements. It was thus recommended that such a review be planned.

The assessment has shown that the assessed payment systems sufficiently address most of the overseers' expectations related to this key issue, although specific recommendations have been issued for some systems with the aim of achieving full compliance.

Address: Kaiserstrasse 29, 60311 Frankfurt am Main, Germany

Postal address: Postfach 16 03 19, 60066 Frankfurt am Main, Germany

Telephone: +49 69 1344 0; Website: http://www.ecb.europa.eu; Fax: +49 69 1344 6000

ISBN 978-92-899-0636-4 (online)