EUROPEAN CENTRAL BANK

ISSUES PAPER

PAYMENT SYSTEMS BUSINESS CONTINUITY

10 May 2005

EUROPEAN CENTRAL BANK

ISSUES PAPER

PAYMENT SYSTEMS BUSINESS CONTINUITY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Investigation into payment systems business continuity…

The development of sound and efficient business continuity plans within the financial sector is of common interest to financial authorities, financial institutions and market infrastructure providers in many countries. Besides the specific interactions between central banks and payment systems infrastructures, the field of business continuity covers a broad range of important issues.

The purpose of this paper is to provide guidance to systemically important payment systems (SIPS) operators in order to achieve sufficiently robust and consistent levels of resilience across those systems, building on efforts to improve their recovery and resumption capabilities.

… to continue open dialogue with the market

This issues paper is meant as a follow-up to the Eurosystem's closed-door round-table discussion on business continuity held in April 2004. The ECB seeks to encourage dialogue with the industry across the euro area with regard to the operational resilience of payment systems.

Requirements for payment systems

A series of major incidents over the last few years (e.g. terrorist attacks, power outages, etc.) have shown how the payments industry critically depends on a resilient payment system infrastructure with appropriate operational and communication procedures. Further development of CPSS Core Principle VII would allow central banks, financial institutions and market infrastructures to work together to develop a common framework consisting of implementation guidelines which define their need for resilience, and establish best practices to ensure that this is delivered. The framework will consist of three key elements: (i) a well-defined business continuity strategy; (ii) appropriate business continuity plans that envisage a variety of plausible scenarios, recovery and resumption objectives; and (iii) regular industry-wide or local testing of the effectiveness of each aspect contained in the business continuity plans. The implementation of a common framework will contribute to building a level playing-field for all stakeholders in the payments industry when implementing and evaluating resilience and, simultaneously, will also take into consideration oversight expectations that should be addressed by system operators.

INTRODUCTION

Market participants and public authorities in many countries have recently been reconsidering their business continuity policies and reassessing their adequacy and plans in the light of the vulnerabilities revealed by the events of 11 September 2001. In the euro area, there have already been in-depth and fruitful discussions and initiatives with regard to business continuity planning. However, so far, these have taken place mostly at national level, and have not systematically considered that the financial system of the euro operates as a euro area-wide network of interrelated markets, market infrastructures and participants. Because of the network nature of the financial system, the Eurosystem considers that there is now the need for coordination of business continuity policies and plans at the euro area level, with the aim of making the financial system of the euro area as a whole more resilient.

From this perspective, the Eurosystem is willing to discuss with the industry new business continuity requirements that it envisages integrating into its oversight policy. These requirements would apply to all systemically important payment systems in euro. They would provide guidance to system operators so that all achieve a sufficiently high and consistent level of resilience. However, each would remain responsible for its own business continuity planning and in particular would be free to target higher resilience objectives. This note outlines several requirements and points to be addressed in the near future, with the aim of serving as a basis for discussion of the topics mentioned above.

This document contains new implementation guidelines with regard to business continuity of CPSS Core Principle VII for systemically important payment systems (SIPS). These implementation guidelines have been adapted:

- to cover more comprehensively the key elements of business continuity plans, such as the formulation of business continuity objectives and the development, testing and updating of business continuity plans; and
- to update oversight expectations that should be taken into account by system operators with regard to the content of these key elements, most notably on the basis of the lessons drawn from the events of 11 September 2001, for instance in terms of disaster scenarios to consider and recovery and resumption objectives to be met.

EVOLUTION OF CORE PRINCIPLE VII

The rapid recovery and resumption of systemically important payment systems (SIPS) in euro is a key prerequisite if the euro financial system is to be resilient to adverse shocks. In light of the new risks posed by the post-11 September environment, the Eurosystem proposes to adapt its oversight framework for SIPS in order to help improve the operational safety of such systems. This fulfils the Eurosystem’s statutory responsibilities of promoting the smooth functioning of payment systems, and is also in line with the initiatives taken by Economic and Monetary Union (EMU) Member States to review and strengthen business continuity arrangements for SIPS.[1] The objective of this would be to provide guidance to SIPS operators so that sufficiently robust and consistent levels of resilience can be achieved across these systems as a result of efforts currently under way to improve their recovery and resumption capabilities.

From a practical perspective, the evolution of the oversight framework for SIPS would consist of a further specification of Core Principle VII (CP VII).[2] Although CP VII states that "*the system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of daily processing*", it contains implementation guidelines which cover business continuity arrangements in a rather generic way.

The proposed revised implementation guidelines identify key elements of business continuity plans that should contribute to ensuring a level of resilience of SIPS consistent with the objective set by CP VII, and provide an explanatory memorandum for those key elements which build on and expand the memorandum currently referring to CP VII in the CPSS report entitled "*Core principles for systemically important payment systems*".

These **key elements** are as follows:

1. Systems should have a well-defined business continuity strategy that is endorsed by senior management. Critical functions should be identified and processes within these functions categorised according to their criticality. Business continuity objectives should aim at the recovery and resumption of critical functions within the same settlement day.

2. Business continuity plans should envisage a variety of plausible scenarios, including major disasters affecting a wide area. Systems should have a secondary site, and the latter's dependency on the same critical infrastructure components used by the primary site should be the minimum compatible with the stated recovery objectives under the scenarios considered. A well-structured crisis management team and formal procedures to manage a crisis should be set up.

3. The effectiveness of the business continuity plans needs to be ensured through regular testing of each aspect of the plan. Performing whole days of live operations from the backup site should be considered, and the latter should also be tested periodically with the backup facilities of major participants. Systems could also participate in industry-wide testing.

[1] In addition, as the technical failure of major participants in the systems may induce systemic risk, some recommendations address the resilience of their infrastructures. These recommendations should apply to participants of both centralised and decentralised systems (i.e. ones without a central operator, based on a bilateral exchange of messages and settlement, such as POPS in Finland). All other recommendations concern the operators of systemically important centralised systems.

[2] See "Core principles for systemically important payment systems", CPSS, Bank for International Settlements (BIS), January 2001.

System operators' business continuity plans should be periodically updated and their disclosure considered.

1. FORMULATION OF BUSINESS CONTINUITY OBJECTIVES

1.1 Definition of a strategy in terms of business continuity

The purpose of a system's business continuity arrangements is to seek to ensure that the agreed service levels are met even in the event that one or more components of the system fail.

It should be seen as standard practice that senior management review and endorse business continuity strategies to ensure that plans are consistent with overall business objectives, risk management strategies and financial resources. Business continuity should be expressly discussed by the Board from time to time, both in setting objectives for the organisation and in assessing how effectively those objectives have been met. Senior management should be expressly accountable to the Board for achieving the system's stated objectives, which should be clearly documented.

Best practice could also entail the setting up of a formal central business continuity management function with the task of coordinating planning between functions.

1.2 Identification of critical functions

Out of all the functions that support the settlement process and that are performed by payment systems operators, key functions should be identified and processes within these functions categorised according to their criticality. Any assumptions behind this categorisation should be fully documented and regularly reviewed. If any critical functions are dependent on outsourcing arrangements, adequate provisions should be in place to ensure service provision by third parties.

1.3 Resumption and recovery objectives

Business continuity objectives should be clearly defined and aim at the recovery and resumption of critical functions within the same settlement day to ensure that all pending transactions are completed on the scheduled settlement date in all envisaged scenarios. Under the emerging, more demanding best practice, SIPS should aim to recover and resume critical functions no later than two hours after the occurrence of a disruption.[3]

A payment system's business continuity arrangements should include a "minimum level of service" to be used, in case of severe disruption, to process a small number of critical payments (for instance relating to the settlement of other payment and settlement systems, or in connection with market liquidity or monetary policy). This would ensure as far as possible that time-critical payments are made on time. This

[3] Such an objective is consistent with the user requirements for TARGET 2 as compiled by the EBF TARGET Working Group.

minimum level of service could be achieved, for example, through manual paper-based processing, authenticated facsimile messages, or a basic PC-based system using physical media for data transfer.

2. DEVELOPING BUSINESS CONTINUITY PLANS

2.1 Scenarios

The payment system operator and, where relevant, the participants and infrastructure service providers should plan arrangements to ensure continuity of the service in a variety of plausible scenarios including major disasters covering a wide area. These scenarios should be documented by a regularly updated Business Impact Analysis, which should assess possible threats and their impact and probability. Both internal and external threats should be considered, and the impact of each failure should be identified and assessed. These assessments should address the potential failure of each of the central components, the participant's components, and the infrastructure services used. Moreover, business continuity plans should allow for the occurrence of major (wide-area) disasters. Indeed, the events of 11 September have tragically shown the plausibility of wider-scale disruptions, resulting in the loss of key personnel or in severe disruptions to transportation, telecommunications, the power system or other key infrastructure elements. Therefore, such scenarios should also be envisaged by systems when performing Business Impact Analysis.

The duration of a disruption is another key element to be considered in identifying scenarios. In the event of a major disaster covering a wide area, the primary site may be destroyed or severely damaged. Hence, it may not be sensible to assume that business continuity plans will always only be operated for a short period of time. Best practice could be to take into account scenarios where the primary site is rendered unusable and/or the site's staff remain unavailable for more than a day.[4]

Arrangements to prevent, mitigate and/or react to the failure can then be developed. Simplicity and practicality are key considerations when designing contingency systems and procedures; they need to work at times of stress and (despite training and testing) are inevitably less familiar to the personnel involved than the normal operating procedures.

2.2 Backup site(s)

The business continuity arrangements of a SIPS should include, at a minimum, a second processing site. In its simplest form, the traditional model is based on an "active" operating site with a corresponding backup site.[5]

[4] Such a scenario is clearly identified in the user requirements for TARGET 2 as compiled by the TARGET Working Group, which state that contingency arrangements "*should ensure a level of backup appropriate to guarantee equal service at all times as the primary site, even in the case of a total loss of a primary site and/or personnel within*".

[5] It is however acknowledged that a real system is more complex than this model and is composed of different components/structures (e.g. computer operators, system controls, relationships with participants, senior management, etc.), all of which may be located in different primary and secondary sites.

The traditional approach tends to limit geographic separation to reduce the relocation time of key staff to the backup site. However, when both primary and backup sites depend on the same labour pool or infrastructure components (transportation, telecommunications, water supply and electric power), large-scale events could render both sites inaccessible or inoperable. This emphasises how important it is for systems to ensure an appropriate geographic separation between the primary and the secondary site. Therefore, the dependence of the second processing site on the same critical infrastructure components used by the primary site (telecommunications, water supply and electric power) should be the minimum compatible with the stated recovery objectives.

Furthermore, geographic separation may not be sufficient, especially in scenarios involving terrorist attacks. Indeed, terrorism means that sites can be targeted regardless of their location. One defence against targeted attacks is, as far as possible, to ensure the anonymity of primary and backup sites.

Ensuring that backup facilities have access to current data is a critical component of business recovery. Systems should preferably employ data mirroring or logging technologies for remote real-time transactions through which transactions are automatically and continuously transferred to the second site. However, current technological limitations may rule out a wide separation of sites that use fully real-time, high-volume synchronous data-mirroring backup technologies, so a balanced approach should be considered. If another method to replicate data is used, systems should evaluate it carefully and in particular its capacity to reconcile large amounts of data. Therefore, systems should use a method for replicating data which ensures that backup facilities have access to all data necessary to allow business to recommence within business resumption objectives.

Secondary processing sites are generally designed to have identical software, hardware and telecommunications to the primary site, as this simplifies control, maintenance and testing. Identical software, however, is unlikely to protect against a software failure at the primary site. When designing and equipping their backup sites, therefore, systems should assess the risk of simultaneous failure owing to exposure to similar software and hardware vulnerabilities (including peripheral systems, mainframes, etc.).

Backup sites should be fully operational, have adequate capacity and be able to process volumes exceeding those of a normal day of operations. Indeed, when operations resume after a serious disaster, the flow of payments would be expected to rise well above the average level. The daily volumes following a major disruption also generally exceed those of a normal day.

2.3 Staff

Steps should be taken to ensure that not all staff is in the same place at the same time. This applies to computer operators as well as system control and management. If all staff is based on one site, systems should avoid having just two shifts in the event that a disaster happens during the shift changeover.

Systems should also minimise the reliance on relocating key staff in the event of a disaster and, in cases where this is unavoidable, should anticipate how such relocation could be achieved. With this in mind, systems could investigate possibilities for remote access in cases where the systems are still running but staff cannot access the site. The automation of backup arrangements could also be increased, which would allow the primary site automatically to shift production with little or no staff involvement. Accordingly, it would be best practice for systems to require the primary and secondary sites to be located in different geographical areas and to require the sites to be operated by different staff.

2.4 Dependency on third-party providers

An important consideration during the design of the system should be to avoid a situation whereby the failure of any particular component or service could cause the whole system to fail (i.e. single points of failure). Based on this consideration, a good strategy would be to recognise external dependencies and to highlight any remaining single points of failure. When a single point of failure cannot be avoided, steps should be taken to respond promptly to this threat. In particular, the operational reliability of telecommunications facilities is generally critical for payment systems. The key methods of ensuring telecommunications continuity are redundancy and alternative routing: there should be no dependence on a single supplier, and there should be an actual physical separation of the lines. System operators should be aware of the actual level of diversity, and identify single points of failure even if arrangements have been made with multiple telecommunication providers or by contracting for diverse routing.

Systems should consider the need for contingency and disaster procedures for critical functions in the event of a total failure of the telecommunication networks.

As far as backup arrangements are concerned, systems should preferably use dedicated facilities. If shared facilities are used, these must actually be available for use in the event of a disaster upon demand. At present, in some cases third-party vendors might not be able to accommodate all of their clients' requests at the same time.

2.5 Participants

The technical failure of major participants in the system may induce systemic risk. For this reason, major[6] participants should have a second processing site. This should be part of the technical requirement to access the system. It could also be considered that at a minimum, relevant participants should be able to close one day and reopen the following day on the backup system. Cost-efficient solutions may be considered, such as bilateral arrangements between the participants to use each other's processing sites, or by a central (shared) contingency site for use by any participant suffering a serious failure. However, in the latter case, participants should secure the actual availability of the central (shared) contingency site, as large-scale events could lead to a number of participants needing to access the contingency site at the

[6] A major participant can be defined as one which accounts for more than 5-20 % (according to the market in question) of the payments processed in the system in terms of value or volume. This definition may however need to be reassessed.

same time. Similarly, system operators should be aware of, and potentially guard against, major participants choosing to concentrate their live/backup sites in similar geographical areas, as this would make them potentially vulnerable to any widespread disruptions in that area.

The effectiveness of the major participants' backup arrangements should be ensured through periodical testing. Best practice would be to perform these tests periodically in real-life situations.

2.6 Communication and crisis management

Clear procedures must be in place for identifying and responding to a crisis and for instigating contingency procedures. A multi-skilled crisis management team should coordinate action and communication with and between participants, overseers and other interested parties. There should be formal, well-prepared procedures to address these issues. The authority and criteria for invoking aspects of or all of the Business Continuity Plan should be clear, as should the responsibilities of each business function and each level of management/staff within these functions. There should be clear lines of reporting and lines of succession in each key function, particularly for key managerial and operational staff.

Contact lists of key personnel (both at operational and crisis manager level) of major participants, authorities and infrastructure providers, including contacts at their backup location, should be up to date and readily available both at the primary and at the backup location.

The importance of accurate and clear information flows, both internally and externally, is evident. The need for effective communication between key players may be starkly highlighted in the event of a major, wide-ranging disaster. During a crisis, accurate and clear information flow help others make informed decisions and avoid exacerbating credit and liquidity problems. Therefore, system operators should define in advance procedures for both internal and external communication. The arrangements could, for example, include measures to inform participants, their customers, other financial services, overseers and the media rapidly and regularly about any incident and its impact on the payment service.

The extent to which systems depend on the functioning of the public switched telephone networks should be identified and reduced; best practice would be to envisage alternative means of communication for sharing information in the immediate aftermath of a crisis (such as by mobile phone, radio or satellite communication, private telecommunication networks or internet-based forms of communication such as e-mail and communication via websites). Systems should also ensure in advance that such facilities are sufficiently robust to deal with the high volumes expected in a crisis situation.

Having a single source of reliable and timely information on the nature of threats may prove decisive in overcoming a crisis. This may be achieved by ensuring adequate communication with the other national agencies entrusted with managing large-scale crises. System operators should as best practice already have established any necessary lines of communication with other public authorities that would be required in a crisis situation.

3. TESTING AND UPDATING OF BUSINESS CONTINUITY PLANS

3.1 Testing of business continuity plans

All elements need regular testing, involving the system's participants and any other parties which would be affected by the arrangements. Testing is an important and long-standing component of the business continuity planning process. The effectiveness of business continuity plans needs to be ensured through regular testing of each aspect of the plan. Responsibility for determining the appropriate frequency and depth should ultimately lie at a high level and the decision should take into account factors such as the criticality of the functions/process being tested, as well as the cost/complexity of the testing. However, business continuity plans should in general be tested once a year at a minimum, and more frequently where indicated (e.g. for the most critical parts).

All aspects of the business continuity arrangements should be clearly and fully documented. The operational staff of both the payment system operator and the participants should be thoroughly trained in the use of the contingency procedures and the recovery and resumption arrangements; they should also be involved in testing. Preferably, staff should participate in the development of these arrangements.

When testing, all elements should be considered, including the Business Impact Analysis, Business Continuity Management and the Business Continuity Plan itself. The aim of the tests is to verify that the arrangements are workable in practice, to identify issues not apparent during the planning stage, and to familiarise staff with the operation of the plan. Where the business continuity arrangements include the diversion of critical payments to another payment system, this possibility should be discussed, agreed and tested in advance with the operator of that system, so as to prevent the diverted payments from adversely affecting the performance of the other payment system. Testing could include verifying the completeness and adequacy of the plans, evaluating coordination needs with external service providers, measuring the success of the plan against the stated objectives, and taking into account the experience of previous operational failures. Systems should properly document the tests, recording observations, problems and their resolution. However, even with regular testing and staff training, it may be difficult for systems to maintain the effectiveness of a backup site which is not routinely used for production purposes. Therefore systems could also, as best practice, consider periodically performing whole days of live operations from the backup site.

In the event of a major disaster affecting a wide area, the system as well as some market participants may be compelled to operate from their secondary sites. Consequently, testing of internal systems alone cannot be considered sufficient. Business continuity plans should reflect this external dependency, and systems should test their backup with the backup facilities of major participants at least once a year to ensure connectivity as well as the capacity and integrity of data transmission. Participants could also consider performing these tests in a real-life situation in order to obtain a complete picture of the behaviour of the parties and staff involved.

Given the high degree of interdependence within the financial system as whole, systems could also consider as best practice the need to participate in industry-wide testing of contingency and business continuity measures involving participants, financial authorities and other systems. These coordinated tests would ensure the compatibility of individual recovery and resumption arrangements and usefully supplement the individual testing of the different institutions.

3.2 Updating of business continuity plans

Another key element to ensure the effectiveness of the Business Continuity Plan is its periodic update by relevant members of management at an appropriate frequency.

3.3 Communication of business continuity plans

An important issue for system operators to consider is how best, without increasing the risk of attack, to communicate their business continuity and disaster recovery plans to other market participants so as to enable others to assess the operational risks to which they in turn are exposed. Market participants given information related to other institutions' business continuity plans should treat this with the necessary degree of confidentiality. Such transparency will further improve the compatibility of individual business continuity arrangements.