EUROPEAN CENTRAL BANK

BUSINESS CONTINUITY OVERSIGHT EXPECTATIONS FOR SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS (SIPS)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INVESTIGATION INTO PAYMENT SYSTEMS' BUSINESS CONTINUITY ...

The development of sound and efficient business continuity processes 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 operators of systemically important payment systems (SIPS) in order to achieve sufficiently robust and consistent levels of resilience across these systems, building on efforts to improve their recovery and resumption capabilities.

... TO CONTINUE OPEN DIALOGUE WITH THE MARKET

The paper is 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 and disruptions over the last few years (e.g. terrorist attacks, power outages, etc.) have shown the extent to which the payments industry is critically dependent on a resilient payment system infrastructure with appropriate operational and communication procedures. Further development of Core Principle VII [1] of the Committee on Payment

1 "The system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of daily processing", see "Core Principles for Systemically Important Payment Systems", CPSS, Bank for International Settlements (BIS), January 2001.

and Settlement System (CPSS) would allow central banks, financial institutions and market infrastructures to work together to develop implementation guidelines – in the form of common expectations – which are applicable to all SIPS and which define the required level of resilience, as well as establishing "good practices" to ensure that such a level is delivered. The framework consists of four 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; (iii) the establishment of well-defined procedures for effective crisis and communication management; and (iv) regular reviewing and testing (i.e. industry-wide or local testing) to ensure the effectiveness of each aspect contained in the business continuity plans. The expectations laid down in this paper will contribute to building a level playing-field for all SIPS when implementing and evaluating resilience and, simultaneously, will also be taken into consideration in the oversight expectations that should be met by SIPS.

INTRODUCTION

Market participants and public authorities in many countries have recently been reconsidering their business continuity policies and the adequacy of their business continuity planning in the light of the vulnerabilities revealed by terrorist acts (notably the events of 11 September 2001 in the United States), natural disasters and major power outages. In the euro area, in-depth and fruitful discussions have already taken place and a range of initiatives carried out with regard to business continuity management. However, so far, these have occurred largely at the national level, and have not systematically taken into account that the euro financial system operates as a euro area-wide network of interrelated markets, market infrastructures and participants. Given the 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 presents to the financial industry a set of business continuity expectations – with regard to CPSS Core Principle VII – to be integrated into its oversight policy framework.

The following expectations have been adopted:

– more comprehensive coverage of the key elements of business continuity management, such as the formulation of a business continuity strategy and objectives, the development of effective business continuity plans, the formulation of efficient crisis and communication management procedures, and the implementation of effective testing, updating and reviewing processes; and

– updating of the oversight expectations to 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 terrorist attacks and major disruptions, for instance in terms of scenarios to be considered and recovery and resumption objectives to be met.

These expectations are applicable to all SIPS operating in the euro area. They should be used to provide guidance to SIPS operators in order that all such systems achieve a sufficiently high and consistent level of resilience. However, each SIPS should remain responsible for its own business continuity management and, in particular, should endeavour to achieve higher resilience objectives for the system, its critical participants and its critical function/service third-party providers.

EVOLUTION OF CORE PRINCIPLE VII

The rapid recovery and resumption of SIPS in euro is a key prerequisite for the euro financial system to be resilient to adverse shocks. In the

light of the new risks and threats, the Eurosystem presents its oversight expectations for SIPS with a view to improving the operational safety of such systems. This is in line both with the Eurosystem's statutory responsibilities of promoting the smooth functioning of payment systems and with the initiatives taken by euro area countries to review and strengthen business continuity arrangements for SIPS [2]. The objective of this paper is to provide guidance to SIPS operators in their efforts towards achieving sufficiently robust and consistent levels of resilience across such systems operating in the euro area. The oversight expectations contained in this paper are a follow-up to the Eurosystem's closed-door round-table discussion with major market participants, SIPS operators and critical market infrastructures on business continuity held at the ECB in April 2004.

From a practical perspective, the evolution of the oversight framework for SIPS consists of a further specification of Core Principle VII (CP VII) [3]. 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 revised implementation guidelines, which are described in this paper in the form of oversight expectations, identify key elements of business continuity management. They will contribute to ensuring a level of resilience on the part of SIPS across the euro area which is consistent with the objective set by CP VII, and provide an explanatory memorandum for those key elements which build on and expand the 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 and monitoring mechanism endorsed by the board of directors. Critical functions should be identified and processes within these functions categorised according to their criticality. Business continuity objectives for SIPS 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 natural disasters, outages and terrorist acts affecting a wide area. Systems should have a secondary site, and the latter's dependence on the same critical infrastructure components used by the primary site should be kept to the minimum necessary to enable the stated recovery objectives for the scenarios concerned to be met.

3. System operators should establish crisis management teams and well-structured formal procedures to manage a crisis and internal/external crisis communications.

4. The effectiveness of the business continuity plans needs to be ensured through regular testing of each aspect of the plan. System operators should consider performing whole days of live operations from the secondary site, and the latter should also be tested periodically with the participants' contingency facilities. Systems should participate in industry-wide testing organised and coordinated by a commonly agreed financial authority. System operators' business continuity plans should be periodically updated, reviewed and audited to ensure that they remain appropriate and effective. Operators should consider the partial disclosure of business continuity plans to external stakeholders such as other SIPS, overseers and banking supervisors.

2 As the failure of SIPS participants and third-party providers of SIPS critical services/functions may increase systemic risk, some of the expectations also apply to their infrastructures, although the majority concern SIPS operators only.
3 See footnote 1 above.

IMPLEMENTATION

The Eurosystem is aware that the industry is adjusting to the many changes that are currently taking place in the payment systems landscape within the euro area, triggered mainly by the SEPA and TARGET2 projects. The implementation of common business continuity measures allowing SIPS and their participants to absorb most of the impact of any wide-scale disaster or event affecting either their ability to perform settlement operations or financial stability within the euro area or on a global scale, should nevertheless remain a prime concern.

Immediately following publication of these expectations, SIPS should initiate the procedures necessary to comply with the updated oversight standards. These expectations should be implemented and tested by all SIPS by *June 2009*. However, it is understood that, in some cases, SIPS may need additional time in order to implement the expectations. An extension of the implementation deadline may be granted by the overseeing central bank following submission of a formal request by the SIPS concerned explaining why an extension is required and specifying the date by which implementation is expected to be completed.

As regards the critical participants and the third-party providers of critical functions/services identified by SIPS, the implementation deadline should be extended by no more than one year after the normal deadline for implementation of the equivalent business continuity arrangements by the respective SIPS (i.e. until no later than mid 2010). Exemptions from this requirement may be granted on a case-by-case basis following a request to the overseeing central bank via the SIPS operator.

It is envisaged that the Eurosystem will perform regular reviews until June 2009 in order to measure the progress made by SIPS in implementing the expectations and to assess the risk of any possible delays.

1 FORMULATION OF BUSINESS CONTINUITY OBJECTIVES

1.1 DEFINITION OF A BUSINESS CONTINUITY STRATEGY

The purpose of a system's business continuity management is to seek to ensure that the agreed service levels are met, even in the event that the system fails to pursue its normal settlement business.

It should be considered standard practice that a system's board of directors review and endorse the business continuity strategy and monitoring mechanism in order to ensure that plans are consistent with overall business objectives, risk management strategy and budgetary arrangements. The issue of business continuity should be expressly addressed by the board of directors on an ongoing basis, both in setting objectives for the organisation and in assessing how effectively those objectives have been met. A system's senior management should be expressly accountable to the board of directors for achieving the stated objectives, which should be clearly documented.

"Good practice" should also entail the setting up of a central business continuity management function with the task of coordinating business areas. It is essential to ensure close contact between this function, senior management and the board of directors.

1.2 IDENTIFICATION OF CRITICAL FUNCTIONS

From among all of the functions supporting the settlement process and performed by payment systems operators, critical functions should be identified and the processes within these functions categorised and prioritised according to their criticality. Any assumptions behind this categorisation should be fully documented and regularly reviewed. If any functions or services required by SIPS are dependent on outsourcing arrangements, their criticality should be assessed. Critical functions or services outsourced to third-party providers should be

an integral part of the system's business continuity planning, and adequate controls and agreements should be in place to ensure that they can be provided on a continuous basis.

1.3 RESUMPTION AND RECOVERY OBJECTIVES

Business continuity objectives for SIPS should be clearly defined and aim at the recovery and resumption of critical functions within the same settlement day in order to ensure that all pending transactions are completed on the scheduled settlement date in all envisaged scenarios. This also applies to ancillary systems which are characterised as a SIPS and are participants of other SIPS. Under the emerging and more demanding "good practice", it is recommended that SIPS should aim to recover and resume critical functions or services (including critical services outsourced to third-party providers) no later than two hours after the occurrence of a disruption.[4]

In addition, business continuity plans implemented by SIPS should contain arrangements ensuring a "minimum service level of critical functions". Such arrangements would be activated in the event of severe disruption, thus enabling systems to process a limited number of critical payments (for instance, relating to the settlement of other payment and settlement systems, or payments in connection with market liquidity or monetary policy). The arrangements in place should ensure that in extreme scenarios (for example, unavailability of both primary and secondary sites), pending time-critical payments are settled on time and within the same settlement day. The provision of a "minimum service level of critical functions" could be achieved, for example, through a combination of predetermined business authentication procedures based on 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 SIPS operator and, where relevant, the participants and infrastructure service providers should plan arrangements to ensure continuity of the service in a number of plausible scenarios, including major disasters, outages or disruptions covering a wide area. These scenarios should be documented regularly in the form of a Business Impact Analysis (BIA), which involves assessing possible threats, the likelihood that they will occur, and the financial or operational impact on the system. Both internal and external threats should be identified and considered, and the impact of each failure identified and assessed. Regular conduct of a BIA should enable systems to develop plans for all envisaged scenarios that reflect the most efficient balance between the business continuity investment involved and the exposure to risk. The participation of stakeholders is essential to successful scenario planning, which can benefit from their wide experience.

The recent terrorist attacks and natural disasters have revealed just how real a prospect of wide-scale events which result in the loss of key personnel or in severe disruptions to transportation, telecommunications, utilities services or other key infrastructural elements can be. Systems should therefore anticipate such scenarios when carrying out BIAs.

The duration of a disruption is another key element to be considered in identifying scenarios. Should a major disaster or event covering a wide area occur, the primary site may be destroyed or severely damaged, resulting in the loss of critical staff. Hence, it may not be realistic to assume that business continuity plans will always be activated for a short period of time only. It is "good practice" to anticipate scenarios in which the primary site is rendered unusable and/or the site's staff remain

4 Such an objective is consistent with the user requirements for TARGET2 as compiled by the European Banking Federation (EBF) TARGET Working Group.

unavailable for more than a day.[5] Arrangements and controls to prevent, mitigate and/or react to the loss of critical staff should be developed. Simplicity and practicality should be the main considerations when designing contingency systems and documenting business procedures. These must function effectively in times of stress; furthermore, in certain scenarios, they may have to be operated/implemented by staff that, despite training and testing, are less familiar with normal daily operations than the regular personnel.

2.2 SECONDARY SITE(S)

SIPS' business continuity arrangements should include, as a minimum, a secondary processing site. In its simplest form, the traditional operational resilience model is based on an "active" operating site (primary site) with a corresponding secondary site.[6]

The traditional approach tends to limit geographic separation to reduce the relocation time of key staff to the secondary site. However, when both primary and secondary sites depend on the same labour pool or infrastructure components (transportation, telecommunications, water supply and electric power), major 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. Thus, the dependence of the second processing site on the same critical infrastructure components used by the primary site (telecommunications, water supply and electricity) should be kept to the minimum necessary to allow the stated recovery objectives to be met.

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. A preventative measure against terrorist attack is to ensure, as far as possible, the anonymity of primary and secondary sites.

Ensuring that the secondary site has access to current data is a critical component of business continuity. 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 real-time, high-volume synchronous data-mirroring backup technologies, so a balanced approach should be considered. If another method to replicate data is used, system operators should evaluate it carefully and, in particular, assess its capacity to reconcile large amounts of data. Systems should therefore use a method for replicating data which ensures that the secondary site has access to all data necessary to allow business to recommence rapidly in accordance with recovery and resumption objectives.

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

The BIA, or risk assessment, should also address two key elements of information technology (IT) disaster response planning (DRP), namely the secondary site, and the impact of failure of each of the SIPS' core system components, the participant's system components and the infrastructure services used.

5 Such a scenario is clearly identified in the user requirements for TARGET2 as compiled by the EBF 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".

6 It is, however, acknowledged that the reality is much more complex than suggested in this model, as systems are frequently composed of a wide range of components/structures (e.g. computer operators, system controls, senior management, etc.), all of which may be located at a number of different sites.

2.3 STAFF

Steps should be taken to ensure that not all operational and other (management, IT support, etc.) staff identified as critical during the BIA are in the same place at the same time. This applies to computer operators as well as system control staff and management. If all staff are based at one site and a shift regime is in place, the shift changeover period(s) should be kept as brief as possible. System operators should minimise the risk that all staff members are simultaneously present at the same site. Moreover, SIPS operators could conclude bilateral agreements with other external sources on the resumption of operations from the secondary site in the event of the total unavailability of its staff resources.

System operators should aim not to rely on the possibility of relocating key staff in the event of a disaster; where, however, this is unavoidable, they should of course anticipate how such relocation could be achieved. With this in mind, system operators should investigate possibilities for remote access in the event the systems are still running but staff cannot access the site. The automation of the contingency arrangements should also be increased, which would allow the primary site to move operations to a secondary site automatically, with little or no staff involvement. Accordingly, it would be "good practice" for systems' primary and secondary sites to be located in geographical areas with different risk profiles and for the sites to be operated by different staff.

2.4 DEPENDENCE 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). On the basis of this consideration, a "good practice" would be to recognise external dependencies and to highlight any remaining single points of failure. Where the existence of a single point of failure cannot be avoided, the contingency arrangements should be made to address the issue. In particular, the operational reliability of telecommunications facilities is generally critical for payment systems. The key methods for ensuring telecommunications continuity are redundancy, recoverability (i.e. the ability to measure the amount of time needed to re-establish a connection) and alternative routing: there should be no dependence on a single supplier, and the lines ought to be physically separated. System operators should be aware of the actual level of diversity of physical lines, and identify single points of failure even if arrangements have been made with multiple telecommunication providers under a service level agreement (SLA) or by contracting for diverse routing.

System operators should consider the need to establish contingency procedures and bilateral arrangements for performing critical functions in the event of a total failure of the telecommunication networks.

SIPS and their participants using critical functions or services that are dependent on outsourcing arrangements should consider making it an obligation under the SLA that the third party is capable of providing the outsourced function/service continually and without interruption.

As far as contingency arrangements at the secondary site are concerned, systems should preferably use dedicated facilities and resources. If facilities and resources are to be shared (i.e. storage capacity, hardware and software infrastructure, staff, etc.), these must be available for use, on demand, in the event of a disaster (syndicated disaster response capacity). In some cases (i.e. events covering a wide area) syndicated recovery service providers might not be able to accommodate all of their clients' needs at the same time. It is therefore recommended that thorough tests and simulations be organised with the involvement of the recovery service providers, in order to verify the availability of the recovery service providers' facilities and resources and to assess

the prioritisation and space allocation criteria of the contingency arrangements in anticipation of a scenario in which "wide-area" events occur that affect many of their clients at the same time.

2.5 PARTICIPANTS

The technical failure of critical participants in the system may induce systemic risk. For this reason, it is recommended that participants which are identified as critical by SIPS operators should also have a secondary processing site. This should be part of the technical requirement to access the system. At a minimum, relevant participants should be able to close one business day and reopen the following day on the secondary site. Cost-efficient solutions may be considered, such as bilateral business continuity arrangements between the participants to use each other's processing sites, or a central (shared) secondary site for use by any participant suffering a serious failure. However, in the latter case, participants should ensure the actual availability of the central (shared) secondary site provided by syndicated recovery service providers, as "wide-area" events could result in a number of participants from the affected area needing to access the secondary site at the same time. Similarly, SIPS operators should be aware of, and potentially guard against, critical participants choosing to concentrate their primary/secondary sites in similar geographical areas, as this would make them potentially vulnerable to any widespread disruptions or disasters in that area.

The effectiveness of critical participants' business continuity arrangements when operating from a secondary site should be ensured through the periodic testing (in rotation) of all staff members identified as critical. It would be "good practice" to perform these tests using live data.

3 COMMUNICATION AND CRISIS MANAGEMENT

3.1 CRISIS MANAGEMENT

Clear procedures must be in place for identifying and swiftly responding to a crisis that requires business continuity measures, and for instigating contingency procedures. As "good practice", systems should consider developing a crisis management plan enabling them to effectively manage a crisis situation when it arises. A multi-skilled crisis management team should coordinate action and communication with and between participants, overseers and other interested parties identified during the stakeholder analysis. There should be formal, well-prepared procedures, mechanisms and communication channels to address all issues arising during a crisis situation. The crisis management team should also be responsible for maintaining the crisis management plan which should form part of business continuity management. The criteria for implementing the business continuity plan should be precise and unambiguous, as should those persons who have the authority to do so and the responsibilities of each business function and each level of management/staff within those functions. There should be clear lines of reporting and succession for each key function, and particularly for key managerial and operational staff. It is "good practice" for crisis management not to be dependent on specific staff; knowledge/expertise should instead be transmitted to other staff members, who should be trained to take over in the event of the unavailability of key personnel.

Contact lists of critical personnel (both at operational and crisis management level) of critical participants, authorities and third-party providers of critical infrastructure and functions/services, including contacts at their secondary location, should be up-to-date, reviewed regularly and readily available at both the primary and the secondary location.

3.2 CRISIS COMMUNICATION MANAGEMENT

The importance of clear and accurate information flows, both internally and externally, is self-evident. The need for effective communication between key stakeholders may become all too clear in the event of a major, "wide-area" disaster. During a crisis, clear and accurate information flow help others make informed decisions and avoid exacerbating credit and liquidity problems. Therefore, system operators should define procedures for both internal and external communication, which should be detailed in a crisis communication plan. The arrangements could, for example, include procedures for informing relevant stakeholders (participants, their customers, other financial services, overseers, the media, etc.) rapidly and regularly about any incident and its impact on the payment service. However, crisis communication should not be limited to the transfer of information to stakeholders, but instead should be considered an exchange of information with a view to reaching a common understanding of the issues involved during a crisis.

The communication medium used for disseminating information during a crisis should be appropriate in view of the content and purpose of the information, and the receiving stakeholder. System operators should assess the extent to which crisis communication arrangements depend on the proper functioning of the public switched telephone network and minimise any dependency as far as possible. "Good practice" would be to envisage alternative means of sharing information in the immediate aftermath of a crisis (e.g. radio or satellite communication, private telecommunication networks, and internet-based forms of communication such as e-mail, communication via websites, etc.). Systems should also ensure, in advance, that such facilities are sufficiently robust to deal with the high volumes expected in a crisis situation. Indeed recent crises have demonstrated that, on account of network unavailability, mobile telephone networks alone cannot be relied on to communicate with external or internal sources. A "good practice" for systems is to minimise their dependency on cell networks as a medium for crisis communication.

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 (through participation in tests organised at the national level or in specialised industry-wide tests) with the public authorities entrusted with managing large-scale crises (e.g. overseers, banking supervisors). System operators should, as "good practice", establish the necessary lines of communication with any other public authorities whose involvement would be required in a crisis situation.

4 TESTING AND UPDATING OF BUSINESS CONTINUITY PLANS

4.1 TESTING OF BUSINESS CONTINUITY PLANS

All elements of business continuity plans should be tested on a regular basis; this testing should involve both the system's participants and any other parties which would be affected by the arrangements. Regular testing is an important component of business continuity management, as it contributes to ensuring that plans are effective, achievable and cost-efficient. Responsibility for determining the appropriate frequency and thoroughness of tests should ultimately lie with senior management, and the decision should take into account factors such as the criticality of the functions/processes being tested, and the scale and cost/complexity of testing. However, business continuity plans should in general be tested at least once a year, and more frequently where indicated (e.g. for the most critical parts of the function/service, as identified by the BIA). In addition, certain events may require the organisation of business continuity tests, such as major changes in critical business functions/processes, major changes to the system's infrastructure (at both

sites) and external business requests for coordinated wide-scale tests.

The aim of the tests is to validate the effectiveness of the business continuity strategy, verify that the arrangements are viable in practice, identify issues not apparent during the planning stage, ensure continuing readiness, and to familiarise staff with the operation of the plan, including their roles and responsibilities. Reports on these tests should be provided to senior management, auditors, and, whenever required, to regulators. 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, in order to prevent the diversion adversely affecting the other payment system's performance. Testing should 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 the means for their resolution. However, even with regular testing and staff training, it may be difficult for systems to maintain the effectiveness of a secondary site which is not routinely used for live operations. Systems should also, as "good practice", consider periodically performing full days of live operations from the secondary site. However, before adopting such a practice, the related risks should be carefully evaluated, taking into account the operational features of the secondary site.

The operational staff of SIPS should be thoroughly trained in the use of the contingency procedures and the recovery and resumption arrangements; they should also be involved (in rotation) in testing. It is preferable that staff participate in the development of these business continuity arrangements and tests.

In the event of a disaster affecting a wide area, both SIPS and critical participants may be compelled to operate from their secondary site. Consequently, testing of internal systems alone cannot be considered sufficient. Business continuity plans should reflect this external dependency, and SIPS should test their business continuity arrangements and procedures from the secondary site with their participants' business continuity facilities at least once a year to ensure connectivity as well as the capacity and integrity of data transmission. SIPS and their participants should also consider performing these tests simulating a live operation mode in order to obtain a complete picture of how the parties and staff involved react.

Given the high degree of interdependence within the financial system as a whole, systems should also consider as "good practice" the need to participate in industry-wide testing of contingency and business continuity measures focusing primarily on critical functions. Such tests would involve other SIPS, a selected group of participants, market infrastructures, financial authorities, critical service providers and other interconnected systems. These tests would be coordinated by a commonly agreed financial authority and would ensure the compatibility of individual business continuity arrangements and usefully supplement the individual testing of the different institutions.

4.2 UPDATING OF BUSINESS CONTINUITY PLANS

Another important element to ensure the effectiveness of the business continuity plan is for the relevant management to update it periodically at appropriate intervals (at least every 12 months), or following a major change to infrastructure or business procedures affecting critical functions of the system. Updates to business continuity plans should take test results and recommendations from auditors and regulators into consideration.

4.3 COMMUNICATION OF BUSINESS CONTINUITY PLANS

An important issue for SIPS and their critical participants to consider is how best to communicate information relevant to their business continuity plans to other participants, without increasing the risk of attack, in order to enable others to assess the operational risks to which they in turn are exposed. The dissemination of such information should be authorised internally by a system's board of directors. Participants should treat information related to other institutions' business continuity plans with the necessary degree of confidentiality, which could be enforced by means of a confidentiality agreement. Such transparency will further improve the compatibility of individual business continuity arrangements as well as promoting trust among participants.

GLOSSARY[7]

Business Continuity Management (BCM): A holistic management process that identifies potential risks to an organisation and provides a framework for building resilience in order to ensure that it is able to respond effectively and safeguard the interests of its key stakeholders, reputation, brand and value creating activities.

Business Continuity Plan (BCP): A clearly defined and documented plan for use at the time of a business continuity emergency, event or disaster and/or crisis. A BCP is also referred to as a disaster recovery plan (DRP).

Business Continuity Management Team: A defined number of roles and responsibilities for implementing the business continuity plan.

Business Impact Analysis (BIA): A structured procedure to measure the financial and operational consequences of a disruption over time.

Crisis: An occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust, and/or strategic/business goals of an organisation.

Confidentiality: The quality of being protected against unauthorised disclosure.

Operational risk: The risk that deficiencies in information systems or internal controls, human errors or management failures will result in unexpected losses (internal and external events).

Oversight (payment systems): Oversight of payment and settlement systems is a central bank function whereby the objectives of safety and efficiency are promoted by monitoring existing and planned systems, assessing them against these objectives and, where necessary, introducing change.

Participant: An entity which is identified/recognised by the system and which is allowed to send, and is capable of receiving, transfer orders either directly or indirectly.

Payment System: A payment system consists of a set of instruments, banking procedures and, typically, interbank funds transfer systems that ensure the circulation of money.

Primary site: The main location used by systems from which the daily business operations and other functions are run.

Public disclosure: Making information publicly accessible – for example, by posting it on a website.

Resumption: The process of planning for and/or implementing the restarting of defined business functions and operations following a disaster.

7 A number of these entries are based on the glossary of The Business Continuity Institute (BCI), available on its website at www.thebci.org.

Secondary site: A location other than primary site which can be used by systems to resume business operations and other functions in the event of a disaster, major system or infrastructure malfunction, or inability to access the main site.

Service Level Agreement (SLA): A formal agreement between a service provider (whether internal or external) and their client (whether internal or external) which covers the nature, quality, availability, scope and response of the service provider.

Settlement: The completion of a transaction, or of processing in a transfer system, aiming at discharging participants from their obligations through the transfer of securities and/or funds. A settlement may be final or provisional.

Settlement date: The date agreed upon by the parties to a transaction as the date on which settlement is to take place.

Systemically Important Payment System (SIPS): A payment system is systemically important if a disruption within that system could trigger or transmit further disruptions amongst participants or systemic disruptions in the financial area more widely.

Stakeholders: A payment system's stakeholders are those parties whose interests are affected by the operation of the system.

System recovery: The procedure for rebuilding a computer system and network to a state whereby it can accept data and applications and facilitate network communications.

Systemic risk: The risk that the inability of one participant to meet its obligations in a system or to perform its functions when due will cause other participants to be unable to meet their obligations when due. The inability can be caused by operational or financial problems.

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.int
Fax: +49 69 1344 6000
Telex: 411 144 ecb d

ISBN 92-9181-984-0 (online)