EUROPEAN CENTRAL BANK

31 May 2006

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

SUMMARY OF COMMENTS RECEIVED DURING THE PUBLIC CONSULTATION

On 10 May 2005, the Eurosystem launched a public consultation on an issues paper entitled "Payment systems business continuity", with the aim of developing a common oversight policy on business continuity for systemically important payment systems (SIPS), their critical participants and third-party providers of critical functions/services. The majority of responses came from banking associations and a number of financial institutions and market infrastructures, and were generally of high quality. Commentators appreciated the Eurosystem's transparency and acknowledged that the initiative was a useful contribution to the efforts made by all stakeholders in the financial sector to increase the resilience of the payment systems infrastructure in the euro area. Several responses were of an explanatory nature and described the circumstances and common practices relevant to specific systems or market infrastructure arrangements. The Eurosystem appreciates these contributions, but cannot comment on them in detail in this summary. Many of the editorial and technical comments are directly reflected in the revised version of the paper. This summary presents the main comments and indicates the Eurosystem's response.

General comments

Commentators proposed that the financial community adopt a common framework, such as a business continuity management (BCM) framework, as the framework for defining a business continuity policy

applicable to payment systems. Business continuity management[1] is "a process that identifies potential impacts and threats to an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities"[2]. The issues paper reflects the key elements of BCM, such as strategic objectives, business continuity planning, crisis management and testing. Systems can use this structural approach and terminology to address those key elements when defining their business continuity. It is hoped that the BCM framework will help systems to better understand the objectives of the issues paper and provide some guidance on how systems can improve procedures and practices for crisis management and communication, and increase resilience to disruption and loss of tangible and intangible resources.

Following requests from almost all parties responding to the consultation, a glossary has been drafted and is introduced as an annex to the paper. In addition, a number of commentators requested the introduction of an annex describing which of the expectations, or "good practices", are relevant to each particular segment of the payments industry. The paper now clearly indicates those parties to which each of the "good practices" is addressed. Indeed, the paper is intended to set down an oversight framework for SIPS - and in some cases their critical participants as identified by SIPS operators - and not for *all* participants.

A few comments suggested that the paper should be aligned with other international initiatives on business continuity, in the interests of consistency. However, the Eurosystem does not consider alignment with other such initiatives to be necessary at this stage, although it will of course continue to monitor all relevant developments.

Some commentators suggested that the scope of the paper should be extended to cover all participants, and not just SIPS, in order to address the issue of systemic risk more comprehensively. It was stated that business continuity cannot be achieved throughout the industry as a whole without all participants being in a position to recover and resume operations promptly. However, the scope of the paper is to establish a business continuity framework in order to mitigate the systemic risk imposed by SIPS and their participants. The Eurosystem believes that the risk imposed by individual participants and third-party providers of critical functions/services should be assessed by SIPS operators, who should identify any action required within their own framework.

It was also proposed that retail payment systems also be included in the business continuity oversight framework for SIPS. The Eurosystem points out that the paper covers all SIPS, including retail payment systems which are also categorised as systemically important (systemically important retail payment systems; SIRPS)[3] and, in some cases, their critical participants as identified by the SIRPS operators. No other functions or systems are considered to be within the paper's scope.

---

1 The Business Continuity Institute (BCI) has published "Good Practice Guidelines", which provide an overview and guidance on good practice covering the whole Business Continuity Management (BCM) lifecycle from the initial recognition of the need to develop the programme to the ongoing maintenance of a mature business continuity capability.

2 As defined in the "Good Practice Guidelines" issued by the BCI, 2005.

3 For the purposes of the paper and this summary therefore, SIPS includes SIRPS.

Comments were received on the need for third-party providers of critical functions/services to be covered by the oversight expectations. The paper has been amended to make clear that the oversight framework is indeed applicable to third-party providers of outsourced business services/functions which have been identified as critical (in the business impact analysis (BIA), or the risk analysis (RA)). They should also comply with the business continuity expectations contained in the paper. Some commentators requested that the Eurosystem identify the range of critical functions/operations covered by the expectations. However, this would imply the need for a detailed description and analysis of all critical functions applicable to SIPS (and SIRPS) which is beyond the scope of the paper.

It was also requested that the recovery and resumption period for SIPS (i.e. the recovery and resumption of critical functions on the same settlement date, with "good practice" recommending recovery and resumption no later than two hours after the occurrence of the disruption) should be harmonised with the recovery and resumption objectives defined in other financial sector initiatives and applicable to systems or critical functions. The Eurosystem welcomes this comment and recognises its validity. However, such alignment is currently beyond the scope of paper, which focuses on SIPS. It is acknowledged that interdependencies between SIPS and other critical functions or systems might require an alignment of recovery and resumption objectives at a later stage.

Comments were received on the need to apply the resumption and recovery objectives specified in the paper to all systems operated by financial institutions in the euro area, not only SIPS operators. However, the business continuity paper is conceived as a set of implementation guidelines with regard to the business continuity aspect of Core Principle VII[4]; thus, the focus should remain on SIPS. It was also suggested that progressive recovery and resumption should be considered as a solution when defining the oversight expectations. The implementation of a two-hour recovery and resumption timeframe for SIPS implicitly allows the system operators to progressively recover and resume critical functions with the aim of settling all pending transactions and critical payments within the intended settlement day. The explicit reference to a progressive recovery and resumption approach could result in unwarranted complexity in defining the oversight expectation. Finally, other commentators expressed the need to establish a common settlement time-window for settling ancillary systems in participant accounts of critical payment systems. As mentioned above, the aim of the paper is to identify oversight expectations which are specifically addressed to SIPS and not to other systems, such as ancillary systems, as any business continuity issues regarding such systems should be addressed within a SIPS's own framework. However, the issues paper has been amended to make clear that where an ancillary system is also characterised as a SIPS and is a participant in another SIPS, then the same time-settlement expectations should apply

Commentators also expressed their concern about the costs involved in implementing the expectations and the need to weigh them against the risks. The Eurosystem is of the opinion that, while this framework describes a set of oversight expectations and outlines some approaches as to how these expectations

[4] See "Core Principles for Systemically Important Payment Systems", Committee on Payment and Settlement Systems, Bank for International Settlements (BIS), January 2001.

should be met, the responsibility for implementing these expectations lies with the individual institutions, which should define the appropriate measures and address all relevant elements on the basis of clear business continuity objectives in line with the implementation framework adopted by the Eurosystem. It is the role of senior management to decide on the scope of the business continuity measures which need to be implemented for their particular services; this obligation on the part of senior management should indeed be part of the CP VII evolution for SIPS described in the paper.

A few commentators stated that regulators should demand that SIPS operators evaluate and mitigate business continuity risks and that they be held accountable. The Eurosystem believes that the paper should not explicitly address governance issues. Instead, the requirements for risk management contained in the paper are considered adequate for addressing the business continuity issues for SIPS.

Comments specific to the development of the business continuity plan (BCP)

Almost all commentators expressed the view that SIPS should have the flexibility to define disaster scenarios based on local risk profiles. A few of the scenarios which could be considered to have a general impact on the Eurosystem's financial stability objective are covered in the paper ("wide-area" disruptions, terrorist acts, pandemics, etc). The paper foresees that other relevant scenarios should be identified by individual SIPS. A few other commentators suggested that the Eurosystem should identify in the paper as many causes of disruption and exposure to threats as possible. The paper provides a number of plausible scenarios, but the list is not comprehensive; SIPS operators may identify other scenarios on the basis of specific requirements laid down by national authorities or local situations.

Several commentators expressed the need to give more consideration to oversight expectations for dealing with "material risks". The Eurosystem believes that the paper adequately covers such risks where reference is made to external threats. However, there are no specific expectations for the physical security/protection of the premises where a system is located, as such issues should be part of a system's general business continuity framework. It was also stated that "slowly developing threats" should be covered by the paper and that its scope should not be limited to "adverse shock" scenarios only. Although some of the expectations address such a threat indirectly, explicit reference to this scenario has not been considered necessary because the main purpose of the paper is to address specific threats and not all types of threats which should be covered by regular business continuity arrangements.

Some of the commentators were of the view that it is unnecessary for all participants to implement specific operational models such as the resilience model based on a primary operating site with a corresponding secondary site. The Eurosystem wishes to emphasise that establishing a secondary site is a very important oversight expectation addressed to all critical systems (SIPS/SIRPS), but not to all participants in the sector. The location of the sites and the technology used to share data between them could be decided by system operators on the basis of the risk profiles of the two sites, taking into consideration the geographical concentration of similar critical systems in the same region and all other factors mentioned in the paper.

It was also commented that the oversight expectations should include a reference to the necessity of performing a security or risk assessment and/or business impact assessment of both the primary and the secondary sites. This suggestion has been integrated into the paper.

The consultation paper referred to the possibility of simultaneous software failure at both sites. Following a number of comments, this reference has been removed from the paper, since this type of IT-oriented failure does not constitute a threat for other systems.

Other comments suggested that the oversight expectation to implement a "minimum level of service" as regards critical payments should be removed. The "minimum level of service" expectation remains in the paper because, despite current technological advances and solutions, a minimum level of service - as described in the paper - should always be available to system operators and to their participants as a possible fall-back solution.

Commentators expressed concern that ensuring availability of staff resources in the event of disruption might entail the need to establish three shifts (i.e. three recurring periods in which different staff would carry out the same work in relay). The paper does not propose the introduction of a third shift but only the need for appropriate procedures to ensure that staff on both shifts is not present at the site simultaneously for extended periods.

A few other commentators expressed concern that exposures or risks originating from utility service providers (telecommunications, power supply, etc.) should not be formulated as an oversight expectation. The paper does not explicitly cover such risks, which will normally be revealed as a result of a risk assessment and which should be covered in the service level agreement (SLA) concluded by the two parties concerned.

Comments relating to crisis and communication management

Commentators requested that crisis and communication management be clearly defined in the paper. The Eurosystem has introduced a new section in the paper in order to make a clear distinction between crisis and communication management and to introduce more crisis management expectations. In addition, the Eurosystem has adopted terms such as "crisis management team" (CMT), "crisis management plan" (CMP) and "crisis communication plan" (CCP) which would allow the oversight framework to be consistent with the business continuity management terminology used for describing the similar measures.

Comments relating to testing and updating the BCP

A few other commentators expressed the need for the Eurosystem to organise industry-wide tests focusing on critical functions/services rather than on testing the corporate business continuity arrangements. The paper now encourages SIPS to participate in industry-wide tests with a primary focus on critical functions, thus enabling the parties involved in the tests to plan and validate the efficiency of

their business continuity plans with specific reference to critical business functions. Other commentators suggested that the Eurosystem identify and list all possible scenarios that could affect SIPS. As discussed earlier, the Eurosystem is of the opinion that this should be the task of the test organiser (financial authority/SIPS/market infrastructure). The test organiser should identify and distribute all scenarios to be covered during the tests or when implementing business continuity arrangements. It is beyond the scope of the oversight framework for business continuity to cover scenarios other than those resulting from major threats or events.

It was also suggested that the paper include staff exercises in the business continuity arrangements, in addition to staff involvement in testing and trialling. However, arranging and scheduling live trials, drill exercises, relocation exercises or simulations, etc. should be the responsibility of the SIPS operator. As regards the comments received with regard to the frequency of updating the business continuity plans, specific expectations have been included in the paper. These include expectations that plans should be updated every 12 months, or following a major change to infrastructure or business procedures affecting critical functions of the system. Emphasis has also been placed on the fact that the updates to business continuity plans should take account of test results, and recommendations from auditors and regulators.

Comments and suggestions have been received with regard to the entity that should be responsible for coordinating industry-wide tests. The paper has been amended accordingly to reflect the need for coordination of industry-wide tests by "…a commonly agreed financial authority". It was also suggested that the paper elaborate further on the need for private/public partnerships with government authorities. It is hoped that the paper contributes to increasing the awareness of government authorities as regards crisis management and communication arrangements, thus enhancing their overall effectiveness.

Some of the commentators disagreed with the inclusion of the oversight expectation to encourage the disclosure of business continuity plans. Commentators indicated that fulfilling that expectation would be difficult, invoking reasons such as confidentiality and competition. The Eurosystem acknowledges the validity of such arguments from a business perspective. However, transparency and trust between the interdependent and critical payment system infrastructures would not be possible if at least part of the business continuity plans (authorised by management, internal and external auditors, supervisors or overseers) were not disclosed to all parties subject to these oversight expectations.