GUIDE FOR THE ASSESSMENT AGAINST THE BUSINESS CONTINUITY OVERSIGHT EXPECTATIONS FOR SIPS[1]

1. **Key issue 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.**

    1.1 Definition of a business continuity strategy

    Information to assess the fulfilment of the "standard practices":

    1.1.1 Does the system's board of directors review and endorse the business continuity strategy and monitoring mechanism to ensure that plans are consistent with overall business objectives, the risk management strategy and budgetary arrangements?

    1.1.2 Is the issue of business continuity 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?

    1.1.3 Is senior management expressly accountable to the board of directors for achieving the system's stated business continuity objectives?

    1.1.4 Are the business continuity objectives clearly defined, documented and in line with the service level agreed with participants?

    Information to assess the fulfilment of the "good practice":

---

[1] See "Business continuity oversight expectations for systemically important payment systems (SIPS)", www.ecb.int, 9 June 2006.

1.1.5 Does a *central* business continuity management function with the task of coordinating business areas exist within the organisation? If yes, how is it ensured that this function maintains close contact with senior management and the board of directors?

1.2 Identification of critical functions

Information to assess the fulfilment of the "standard practices":

1.2.1 Have critical functions been identified and the processes within these functions categorised and prioritised according to their criticality? Are any assumptions behind this categorisation fully documented and regularly reviewed?

1.2.2 Has the criticality of *outsourced* functions or services to third-party providers been assessed? If yes, are critical functions or services that are outsourced part of the system's business continuity planning and are adequate controls and agreements in place to ensure that these functions and services can be provided in accordance with the system's business continuity objectives?

1.3 Resumption and recovery objectives

Information to assess the fulfilment of the "standard practices":

1.3.1 Do the business continuity objectives provide for the recovery and resumption of critical functions within the same settlement day?

1.3.2 Do business continuity arrangements in place ensure a "minimum service level of critical functions" with a view to enabling the processing of a limited number of *critical payments (*e.g. payments related to the settlement of other payment and settlement systems, payments associated with market liquidity or monetary policy) in the event of severe disruption? Furthermore, do the business continuity arrangements in place ensure that, in extreme scenarios (e.g. unavailability of both primary and secondary sites), pending time-critical payments are settled on time and within the same settlement day?

Information to assess the fulfilment of the "good practice":

1.3.3 Do the business continuity objectives provide for the recovery and resumption of *critical functions or services* (including critical services outsourced to third-party providers) no later than two hours after the occurrence of a disruption?

2. **Key issue 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.

2.1 Scenarios

<u>Information to assess the fulfilment of the "standard practices":</u>

2.1.1 Do business continuity plans include both a wide variety of plausible scenarios (including major disasters, outages or disruptions covering a wide area, loss of key staff) and respective arrangements to ensure continuity of the service in these scenarios?

2.1.2 Are participants and infrastructure service providers involved in the scenario planning and the planning of business continuity arrangements where relevant?

2.1.3 Are those scenarios documented by a regularly performed Business Impact Analysis (BIA) or risk analysis?

<u>Information to assess the fulfilment of the "good practices":</u>

2.1.4 Do business continuity plans anticipate scenarios in which the primary site is rendered unusable and/or the site's staff remain unavailable for more than a day? What arrangements and controls have been established to prevent, mitigate and/or react to the loss of key staff?

2.1.5 Are the design of contingency systems and the documentation of business procedures simple and practical, so that they can function effectively in times of stress?

2.2   Secondary site(s)

<u>Information to assess the fulfilment of the "standard practices":</u>

2.2.1 Does the system have a secondary processing site?

2.2.2 Does the geographical separation between the primary and secondary site ensure that the dependence of the secondary processing site on the same labour pool and critical infrastructure components used by the primary site (transportation, telecommunications, water supply and electricity) is kept to the minimum necessary to allow the stated recovery objectives to be met?

2.2.3 How is the anonymity of the primary and the secondary site ensured?

2.2.4 Which methods for replicating large amounts of data does the system use to ensure that the secondary site has access to all data necessary to allow business to recommence in accordance with recovery and resumption objectives?

2.2.5 Is the secondary site fully operational and does it have adequate capacity to process volumes exceeding those of a normal business day?

2.2.6 Is the BIA or risk analysis of the system also performed for the secondary site?

2.2.7 Does the BIA or risk analysis of the system address the impact of failure of each of the system's core components, the participants' components and the infrastructure services used?

2.3 Staff

Information to assess the fulfilment of the "standard practices":

2.3.1 What measures have been taken to ensure that not all *key* operational and other staff (e.g. management, IT support), as identified during the BIA or the risk analysis, are simultaneously exposed to the same risk, including at times of shift changeover?

2.3.2 What (organisational) measures have been taken to resume operations from the secondary site in case of total unavailability of key staff?

2.3.3 What measures have been taken to minimise the need for relocating key staff in the event of a disaster (e.g. possibility for remote access, increased automation of contingency arrangements)?

Information to assess the fulfilment of the "good practice":

2.3.4 Are the system's primary and secondary site located in geographical areas with different risk profiles and operated by different staff?

2.4 Dependence on third-party providers

Information to assess the fulfilment of the "standard practices":

2.4.1 What arrangements have the system operator and the participants made with third-party service providers (e.g. in service level agreements) to ensure that third-party service providers are able to provide continuity in the provision of the outsourced functions/services?

2.4.2 Since the operational reliability of telecommunications facilities is generally critical for payment systems, what key methods for ensuring telecommunications continuity have been employed (e.g. redundancy, recoverability, i.e. the ability to measure the amount of time needed to re-establish a connection, alternative routing, no dependence on a single telecommunications supplier, physical separation of the telecommunication lines)?

2.4.3 Has the system operator considered the need to establish contingency procedures and bilateral arrangements for performing critical functions in the

event of a total failure of the telecommunication networks? What has been the result of these considerations?

2.4.4 As far as contingency arrangements at the secondary site are concerned, does the system make use of dedicated facilities and resources (i.e. storage capacity, hardware and software infrastructure, staff, etc.) or are those facilities and resources shared with other organisations? If the latter applies, are those facilities and resources available for use, on demand, in the event of a disaster?

Information to assess the fulfilment of the "good practices":

2.4.5 Has the system operator recognised any dependencies on third-party providers and highlighted any remaining single points of failure? Where the existence of a single point of failure cannot be avoided, what contingency arrangements have been made to address this issue?

2.4.6 Since in "wide-area" events syndicated recovery service providers might not be able to accommodate all of their clients' needs at the same time, have thorough tests and simulations with the involvement of these service providers been organised, in order to verify the availability of facilities and resources and to assess the prioritisation and space allocation criteria of contingency arrangements?

2.5 Participants

Information to assess the fulfilment of the "standard practices":

2.5.1 What criteria are used by the system operator for the identification of *critical* participants?

2.5.2 Do technical access criteria require *critical* participants, identified as such by the system operator, to have a secondary processing site? Are these critical participants, at a minimum, able to close one business day and reopen the following day on the secondary site?

2.5.3 In case that critical participants employ a central (shared) secondary site for use by any participant suffering a serious failure, how do they ensure that the syndicated recovery service provider can actually make the secondary site available in case of a wide-area event?

2.5.4 What measures has the system operator taken to become aware of and potentially guard against critical participants choosing to concentrate their primary/secondary sites in similar geographical areas?

2.5.5 Do critical participants perform periodic testing of the business continuity arrangements at the secondary site involving all *key* staff members (in rotation)?

2.5.6 Are these tests performed using live data?

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

   3.1. Crisis management

   Information to assess the fulfilment of the "standard practices":

   3.1.1 Are clear procedures and communication channels in place for identifying and swiftly responding to a crisis that requires business continuity measures?

   3.1.2 Has a multi-skilled crisis management team been established to coordinate action and communication with and among participants, overseers and other interested stakeholders?

   3.1.3 Are the criteria for implementing the business continuity plan, the persons who have the authority to do so and the responsibilities of each business function and each level of management/staff within each function precise and unambiguous? Do clear lines of reporting and succession in each key function exist, particularly for key managerial and operational staff?

   3.1.4 Are contact lists of key staff (both at operational and at crisis management level) of critical participants, authorities and third-party providers of critical infrastructure and functions/services, including contacts at their secondary location, up to date, reviewed regularly and readily available at both the primary and the secondary location?

   Information to assess the fulfilment of the "good practices":

   3.1.5 Is a crisis management plan in place that enables the system operator to effectively manage a crisis situation when it arises? Is the crisis management team also responsible for maintaining the crisis management plan?

   3.1.6 Is knowledge/expertise transmitted also to staff members other than key staff? If yes, are these other staff members trained to take over in the event of unavailability of key staff?

   3.2. Crisis communication management

   Information to assess the fulfilment of the "standard practices":

   3.2.1 Has the system operator established a crisis communication plan in which procedures and adequate communication media are defined for the rapid dissemination and exchange of crisis-related and other information that is

pertinent to the relevant internal and external stakeholders (e.g. participants, their customers, other financial services, overseers, the media)?

3.2.2 Has the system operator assessed the extent to which crisis communication arrangements depend on the proper functioning of the public switched telephone network and tried to minimise any dependency as far as possible?

Information to assess the fulfilment of the "good practices":

3.2.3 Does the system 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 dedicated websites, etc.)? If such alternative means of sharing information in the immediate aftermath of a crisis are employed, how does the system operator ensure that such means are sufficiently robust to deal with the high communication needs expected in a crisis situation?

3.2.4 What measures has the system operator taken to minimise dependence on cell networks as a medium for crisis communication?

3.2.5 Has the system operator established and tested the necessary and adequate lines of communication with the public authorities entrusted with managing large-scale crisis (e.g. overseers, banking supervisors) and any other public authorities whose involvement would be required in a crisis situation?

4. **Key issue 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.**

   4.1 Testing of business continuity plans

   Information to assess the fulfilment of the "standard practices":

   4.1.1 Are all elements of the business continuity plans tested regularly, i.e. 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 or risk analysis)? Does testing

involve both the system's participants and any other parties which would be affected by the business continuity arrangements?

4.1.2 Who determines the frequency and depth of the testing of business continuity plans?

4.1.3 Does the decision on the frequency and depth take into account the criticality of the functions/processes being tested as well as the scale and the cost/complexity of the testing?

4.1.4 Are additional business continuity tests organised in certain cases 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?

4.1.5 Does the content of testing include the verification of the completeness and adequacy of business continuity plans, the evaluation of coordination needs with external service providers and the measurement of the success of the business continuity plan against the stated objectives? Furthermore, does testing take into account the experience of previous operational failures?

4.1.6 If the business continuity arrangements include the diversion of critical payments to another payment system, is this possibility discussed, agreed and tested in advance with the operator of that system?

4.1.7 Does the system operator document the tests by recording observations, problems and the means for their resolution? Are reports on the tests provided to senior management and, whenever required, to auditors, the relevant overseer or regulators?

4.1.8 Have the operational staff been thoroughly trained in the use of the contingency procedures and the recovery and resumption arrangements? Have they also been involved (in rotation) in testing?

4.1.9 Are business continuity arrangements and procedures tested from the secondary site at least once a year with the participants' business continuity facilities to ensure connectivity as well as the capacity and integrity of data transmission? Are such tests performed occasionally also simulating a live operation mode, in order to obtain a complete picture of how the parties and staff involved react?

Information to assess the fulfilment of the "good practices":

4.1.10 Does the system operator periodically perform full days of live operation from the secondary site, after having taken into account its operational features and evaluated carefully the related risks?

4.1.11 Have staff been involved in the development of business continuity arrangements and in the development of tests?

4.1.12 Has the system operator considered the need to participate in industry-wide testing of contingency and business continuity arrangements focusing primarily on critical functions, involving other systems of systemic importance, a selected group of participants, market infrastructures, financial authorities, critical service providers and other interconnected systems? What have been the results of such considerations?

4.2 Updating of business continuity plans

Information to assess the fulfilment of the "standard practice":

4.2.1 Is the business continuity plan updated by relevant members of management 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? Do updates to business continuity plans take into consideration test results and recommendations from auditors, the relevant overseer and regulators?

4.3 Communication of business continuity plans

Information to assess the fulfilment of the "standard practice":

4.3.1 Has the system operator considered the possibility of communicating selected information, relevant to the business continuity arrangements, to participants, in order to enable them to assess the operational risks they incur through their participation in the system? Is the dissemination of such information internally authorised by the system's board of directors? Are participants required to sign a confidentiality agreement with respect to such information?