



## CENTRAL BANK OF CYPRUS

EUROSYSTEM

December 2007

### National Business Continuity (BC) standards for payment systems

#### BC standards (legal requirements, standards, recommendations, guidelines or best practices) for payment systems

BC oversight expectations for SIPS	National standards used for SIPS, SIRPS and PIRPS
<b>BC strategy:</b> Systems should have a well-defined BC strategy and monitoring mechanism endorsed by the board of directors.	It is implied by the adopted Standards. The Central Bank's Oversight policy envisages adoption of all Eurosystem policies and as such, as of 1 January 2008, the BCOE and the Oversight Standards will be implemented and required. This will be communicated to systems as part of the 2008/2009 assessment process. A well defined strategy has to be implemented.
<b>Critical functions:</b> Critical 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.	Some critical functions have been identified at the system level without categorisation. Critical functions have to be better identified and be categorised taking into account all possible disasters.
<b>BC plans</b> BC plans should envisage a variety 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, which involves assessing possible threats, the likelihood that they will occur, and the financial or operational impact on the system.	BC Plans envisage a variety of scenarios; however without taking into account all potential problems or disasters. They should be expanded to be more complete and should be documented.
<b>Level of service provided to the participants</b> BC 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.	The service that can be provided to the participants is limited to the critical payments only.

<p><b>Recovery objectives</b> BC objectives for SIPS should be clearly defined and aim at the recovery and resumption of critical functions <b>within the same settlement day</b> in order to ensure that all pending transactions are completed on the scheduled settlement date in all envisaged scenarios. 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) <b>no later than two hours after the occurrence of a disruption.</b></p>	<p>BC objectives for SIPS were to recover and operate critical functions within the same settlement day, whereas the objective for SIRPS was by the end of the settlement day. Recommendations will be made, in the context of the assessments, to align to Eurosystem recovery objectives, depending on systemic importance.</p>
<p><b>Secondary site:</b> 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.</p> <p>Ensuring that the secondary site has access to current data is a critical component of business continuity. 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.</p> <p>Secondary sites should be fully operational, have adequate capacity and be able to process volumes exceeding those of a normal operating day.</p>	<p>For the SIPS and PIRPS that exist in Cyprus a secondary site has been set up, located in alternative premises. The secondary site though cannot currently offer full operational functionality but only limited critical functions.</p>
<p><b>Participants’ secondary site</b> It is recommended that participants which are identified as critical by relevant system operator 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.</p>	<p>The Central Bank of Cyprus is the only critical participant for the Cypriot SIPS with a limited functionality secondary site. There are no formal secondary site requirements by the systems’ access requirements.</p>
<p><b>Staff</b> 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. Moreover, SIPS operators could conclude bilateral agreements with other external sources on the resumption of operations from the</p>	<p>Staff has to relocate to the secondary site in case of disaster. The primary operators though can stay at the primary site since there are other groups of operators that are trained to perform the same operations.</p>

<p>secondary site in the event of the total unavailability of its staff resources.</p> <p>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. 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.</p>	
<p><b>Utilities and telecommunications: Dependence on third party providers</b> 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. There should be no dependence on a single supplier and the lines ought to be physically separated.</p>	<p>There is dependence on a single supplier in telecommunications rendering business continuity impossible in case of a disaster in this utility company.</p>
<p><b>Outsourcing of critical functions</b> 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.</p>	<p>There is no outsourcing of critical functions.</p>
<p><b>Communication and crisis management</b> System operators should establish crisis management teams and well-structured formal procedures to manage a crisis and internal/external crisis communication.</p>	<p>For the Central Bank of Cyprus, a crisis management team has been established in order to assess and act appropriately in any critical situation. However well-structured formal procedures have not been adopted yet.</p>
<p><b>Testing and updating:</b> 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</p>	<p>These requirements have not been addressed yet, and for some systems the set up is such that they cannot be fully changed over to the secondary site.</p>

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.	
<b>Communication of BC plans:</b> Operators should consider the partial disclosure of business continuity plans to external stakeholders such as other SIPS, overseers and banking supervisors.	This is not currently transparent and substantial progress needs to be achieved in this area.