



CENTRAL BANK OF CYPRUS

EUROSYSTEM

January 2008

National Business Continuity (BC) standards for securities clearing and settlement

Securities settlement BC standards (legal requirements, standards, recommendations, guidelines or best practices)

CPSS-IOSCO recommendation for securities settlement systems*	National standard	Legal requirement, standard, recommendation, guideline, best practice, etc.
<p>Contingency plans All key systems should be secure (that is, have access controls, be equipped with adequate safeguards to prevent external intrusions, and provide audit trails), reliable, scalable and able to handle stress volume and have appropriate contingency plans (<i>i.e. BC and disaster recovery plans, including an evaluation of any reliance on third parties</i>) to account for system interruption.</p>	<p>The CSE systems are secure in connection with access controls and have firewalls preventing unauthorised access to the systems. Audit trail facility is provided and can be used to verify the integrity of data stored in the system and to check the authenticity and confidentiality of the transactions processed. There are adequate contingency plans to provide business continuity. Security requirements are also imposed on participants.</p>	<p>Eurosystem Standards for the Use of SSSs in ESCB credit operations – Standard 9.</p> <p>Some provisions in Secondary Legislation: Transactions Regulation (KΔΠ 409/2006).</p>
<p>Level of service provided to the participants System operators should identify sources of operational risk, whether arising from the arrangements of the operator itself or from those of its participants, and establish clear policies and procedures to address those risks. <i>In particular service providers should define clear targets in terms of operational robustness and business continuity, for example through the implementation of Service Level Agreements (SLAs).</i></p>	<p>The CSE has established clear policies and procedures to address various operational risks to ensure high availability. There are specific steps to be taken in case of an error and procedures to correct and anticipate any unexpected problems. There is no SLA with participants but there are certain provisions in the secondary legislation imposing requirements on both the CSE and participants.</p>	
<p>Recovery objectives The system should be able to recover operations and data in a manner that does not disrupt settlement. <i>Several key jurisdictions regard two hours as the time by which critical systems should recommence operations. Depending upon the nature of the problems, recovery may take longer than two hours.</i></p>	<p>There are adequate recovery procedures which safeguard the business continuity without loss of any data or transactions in process on the time of failure of the systems or any other disaster.</p>	
<p>Status of operations Ideally, backup systems should be immediately available. While it may be possible to recommence operations following a system disruption with some data loss, contingency plans should ensure that, as a minimum, the status of all transactions at the time of the disruption can be identified with certainty in a timely manner <i>and should allow systems to continue to operate with certainty in a timely manner.</i></p>	<p>The systems are replicated locally and both systems and data are immediately available in case of disruption to the primary configuration.</p>	

<p>Secondary site Backup facilities should be established to allow for timely recovery of operations and completion of the settlement process. <i>A second processing site should have the requisite level of key resources, capabilities and functionalities, including appropriately skilled and experienced staff that will allow business resumption immediately after the occurrence of a disruption to the primary site. The backup site should provide a level of efficiency comparable to the level provided by the primary site.</i></p> <p><i>The second site should be located at an appropriate geographical distance and be protected from any events potentially affecting the primary site. If processing is to continue at the second site within a short period of time, in principle less than two hours following disruption of the primary site, then data will need to be transmitted to and updated at the second site continuously, preferably in real time.</i></p>	<p>The systems are mirrored at the remote Disaster Recovery Site and the CSE is capable to switch to the remote site in case of disaster. The log files of the systems are replicated to the disaster recovery site ensuring that all transactions are safely stored.</p>	
<p>Staff There should be adequate management controls and sufficient (and sufficiently well qualified) personnel to ensure that procedures to address operational risk are implemented accordingly. <i>The operator of the systems should minimise the reliance on relocating key staff and, where some reliance is unavoidable, the operator should anticipate how such relocation would be achieved.</i></p>	<p>The CSE relies on relocating key staff due to the size of the organisation and the available resources.</p>	
<p>Utilities and telecommunications: Dependence on third party providers Increasingly, SSSs are dependent on electronic communications and need to ensure the integrity of messages through using reliable networks and procedures (such as cryptographic techniques) to transmit data accurately, promptly and without material interruption. <i>All systems should evaluate any reliance on third parties.</i></p>	<p>There is significant reliance on the telecommunication company and a possible disaster at the utility company may have adverse effects on the CSE's systems.</p>	
<p>Outsourcing of critical functions Some clearing and settlement operations may be outsourced to third parties. In these circumstances, operational risk will reside with the outside service provider. System operators who outsource operations should ensure that those operations meet the same standards as if they were provided directly by the system operator.</p>	<p>The CSE does not outsource any critical functions to any third party.</p>	
<p>Communication and crisis management As severe operational failure at a CSD, CCP, cash settlement agent or major participant could have significant adverse effects throughout securities and other markets, <i>the regulators and overseers of significant providers of clearing and settlement services should encourage system operators to set up a plan for industry-wide contingency planning, ensuring interoperability between such institutions.</i></p>	<p>There is a plan for communication and crisis management but this has not been communicated and tested on an industry-wide basis.</p>	
<p>Testing, updating and communication of plans BC and disaster recovery plans should be rehearsed and capacity stress tested. Contingency plans should be reviewed and tested regularly with participants taking part and after modifications to the system. <i>The review, updating and testing of the plans should build upon thorough analysis and established best practices. Tests should especially take into account the experience of previous operational failures; to this end, each operational failure should be documented and analysed in detail. Appropriate adjustments should be made to the plans, based on the results of this exercise.</i> <i>Without increasing the risk of unwanted events or attacks, the disclosure of the BC and disaster recovery plans should be sufficiently transparent and efficiently communicated to other market participants to enable them to assess the operational risks to which they are in turn exposed. This is also crucial for systems that interact with other systems.</i></p>	<p>There is a need to develop further the review and testing processes of the BC and disaster recovery plan, both internally and with market participants.</p>	