March 29, 2006

BCP Guidelines No: 01/2006

To : Chief Executive Officers of
all Licensed Commercial Banks, Primary Dealers, Central Depository Systems (Pvt) Ltd.
and LankaClear (Pvt.) Ltd.

Guidelines on Business Continuity Planning

Introduction

1. Financial sector is an interdependent network of financial institutions, markets and systems. Fast advancement of technology and sophistication of financial products and systems have made financial institutions[1)] (FIs) vulnerable to operational risk caused by inadequacies or failures of internal processes, systems and external events including natural disasters. Therefore, a failure to manage operational risks may expose the FIs to significant losses. There is a growing interest internationally among regulatory bodies and FIs to strengthen Business Continuity Planning (BCP). Basel II framework has identified operational risk of banks as a distinct risk category (in addition to credit risk, interest rate risk and liquidity risk that financial institutions take in return for an expected reward), which exists in day-to-day operations. Therefore, supervisory authorities in many developed countries and Bank for International Settlements (BIS) – Committee on Payment and Settlement Systems (CPSS) have recommended 10 Core Principles for Systemically Important Payment Systems (Principle VII – Security, Reliability & Continuity), BIS/International Organization of Securities Commissions (IOSCO) Recommendations for Securities Settlement (recommendation 11 – Operational Reliability) and Recommendations for Central Counterparties (recommendation 7 – Operational Risk) to cope effectively with the consequences of operational risk in payment and securities settlement systems.

2. Having considered the consequences of systemic risk which could be caused by disruption to operations of participating institutions (PIs) of LankaSettle System, which is the systemically important payment and settlement system, the Central Bank of Sri Lanka (CBSL) advised PIs to have proper business continuity plans in order to achieve consistent level of resilience in LankaSettle System. Accordingly, CBSL requested PIs to submit their BCPs to CBSL by end March, 2005. Since most of the BCPs forwarded by PIs were incomplete or applied a multitude of standards of their own, CBSL held one to one meeting with each PI during the period of July to August 2005 to explain the required standard of BCP, and requested to submit revised BCPs to CBSL before the end of August, 2005. Since a number of PIs requested CBSL to provide written guidelines on BCPs and the fact that CBSL also desires to develop a consistent framework for BCPs, the CBSL has prepared a set of guidelines.

3. The main objective of these guidelines is to explain the CBSL's supervisory and oversight approach on BCP and provide guidance on sound practices, which CBSL encourages, FIs to follow in order to:

- Have workable and sound BCPs for core banking/critical businesses and systems including systemically important and system-wide important payment and securities settlement systems to ensure that the agreed service levels are met in an event that one or more business or components of a system fail. Moreover, BCPs should ensure continuity of agreed services in an event of a prolonged and widespread disruption;
    - Minimize the financial, legal, and other risks arising from such disruptions; and
    - Develop a consistent framework for BCPs of FIs supervised/overseen by CBSL.

[1)] Includes licensed commercial banks, Primary Dealers and other payment, clearing and settlement service providers supervised/overseen by the Central Bank of Sri Lanka.

Definition of Business Continuity Plan (BCP)

4. 'Business continuity planning' refers to: planning and preparation need to be carried out in advance to identify the impact of potential risks and losses caused by a disruption or a disaster; formulating and implementing viable recovery strategies; and planning to ensure continuity of an institution's services particularly in the area of core banking/critical businesses, payment, clearing and securities settlement; and administering of comprehensive testing and maintenance. A 'Business Continuity Plan' (BCP) refers to a set of processes, procedures, information and measures which are developed, compiled and maintained for critical business functions including core banking and payment and settlement, in readiness for use in an event of an emergency or a disaster which may cause inability to fulfill critical or all business operations. In contrast to BCP, a 'contingency plan', refers to measures, which will enable the most critical business functions to be performed in an event of a disruption. Therefore, the concept of BCP is much wider than a contingency plan.

5. Business continuity planning is a culture to be developed at all levels of staff and the required process needs to be well integrated with the day-to-day operations. The Board and the senior management of each FI should adopt a risk-based framework in BCP. Establishing a comprehensive BCP with a minimum cost without compromising risk management is a challenging task. It would seem sensible for all FIs to have BCPs on the assumption that they may have to face and manage an event of a widespread and prolonged disruption with the complete destruction of buildings and infrastructure in which the main offices of FIs are located, the loss of key staff, complete inaccessibility of the primary site, forcing the FIs to use back-up facilities for an extended period of time. Board of directors (Board) should take responsibility of BCP readiness.

6. FIs may decide to have two-tier plans – one (which would be fully developed with adequate resources to put into effect immediately) to handle short-term problems; and the other (may be a medium/long term plan) to cope with long-term issues.

7. These guidelines are not intended to prescribe step-by-step guidance as to how FIs should conduct their BCP process and it could be considered as a minimum. The following of these guidelines will contribute to building a level playing field for all FIs when implementing the BCPs and will help supervisors and overseers to evaluate the resilience of the operations of FIs.

Application of the guidelines

One of the supervisory/oversight objectives of CBSL is for FIs to have BCPs to ensure high preparedness for continuation of critical operations particularly core banking, payment, clearing and settlement in an event of a disruption. In the course of its on-site examinations, offsite reviews, oversight and meetings on prudential issues with a FI, CBSL will review implementation of the BCP on the practices set out in these guidelines particularly:

- The extent to which the FI has observed the guidelines; and
- The risk profile of the FI and its role in ensuring the stability of the financial system.

Guideline 1: Vest the primary responsibility for BCP preparedness on the Board of Directors and the management of each FI

8. The Board and the senior management of each FI should take the primary responsibility for the BCP of the institution and its effectiveness in relation to the nature and scale of its operations. The Board and the senior management should involve in business continuity management and consider FI's business continuity, risks and mitigating measures as part of its overall risk management framework. The Board should: provide clear guidance and directions in respect of BCP; approve policy on BCP, prioritize critical banking/operations and payment system related business functions, allocate sufficient resources, review BCP test results; and ensure maintenance and periodic updating of BCP.

9. The senior management is responsible for: establishing appropriate policies, standards, strategies and processes for BCP; getting the BCP approved by the Board; getting commitment of all

staff and executing such a BCP in an event of a contingency. Senior management should endorse business continuity strategies of each system to ensure that plans are consistent with overall business objectives, risk management strategy and financial and other resources. The senior management should also evaluate the adequacy of contingency planning for each system and its periodic testing by its own staff/service providers whenever critical operations are outsourced. Resilience and recovery measures should adequately cover the level of business activity, risk tolerance and its role in preserving the systemic stability of the financial system. Such measures should be clearly stated in the BCP and regularly reviewed. Senior management should be accountable to the Board for achieving the stated objectives of each system in the BCP and submit a report to the Board at least annually indicating clearly:

- The preparedness of the institution to achieve stated objectives of each system; and
- The extent of alignment with these guidelines.

Such a report should be reviewed and updated regularly. The BCP must be reviewed at least annually by the FI's internal auditor/or an external expert.

Guideline 2: Incorporate sound practices in the BCP

10. Each FI is encouraged to consider and follow the suggested process for business continuity planning:

- Adopt clear and well defined BCP policy and strategy;
- Establish clear roles and responsibilities to oversee the BCP implementation programme. This may require setting up of a formal business continuity management team with the powers and responsibilities to coordinate planning and implementation;
- Key functions under each system should be clearly identified and processes within these functions to be categorized against their criticality. Assumptions behind these categorization need to be documented and reviewed regularly by the senior management;
- Conduct a business impact analysis to assess the impact and probability of possible disruption scenarios on all (owned, shared and external) critical banking/business, payment and settlement systems; resources and infrastructure, and formulate recovery time objectives (RTO); and resumption of critical functions;
- Each critical business/support functions should formulate its own recovery strategy on how to achieve the RTO and to deliver the minimum level of critical services derived from business impact analysis. In the case of a payment and settlement system, the best practice for a business continuity arrangement is to aim at recovery and resumption of critical operations of systemically important payment systems not later than 2 hours after the occurrence of a disruption; system-wide important payment and settlement system within the same/scheduled settlement date; and effecting a small number of critical payments (such as payment settlement on market liquidity or monetary policy) on time.
- Adopt critical and tough assumptions for each plausible disruption to: assess possible threats (external and internal), their impact and probability; and ensure that the framework would be sufficient to withstand the impact of the disruption (on each component of the system). This involves establishing a disaster recovery site (minimum one site in Sri Lanka with critical infrastructure components, required number of skilled staff, work space, software application, technology requirement, relevant SWIFT link and vital data/information compatible with recovery objectives stated in the BCP). It is important to ensure geographical separation between primary site and disaster recovery site (DRS).
- Determine recovery strategies and providing of each service considering the interdependency among critical services and time frame assessment in business impact analysis.
- Establish at least the minimum BCP requirement for the provision of critical businesses. These BCP requirements should be approved by the senior management before proceeding to the development of BCP. Further, BCP requirement should be considered at the planning/development stages of new business services/products.
- The best practice is to establish 'Disaster Management Team (DMT)'. The DMT may be a group of senior management (for example: heads of department of banking operations, IT,

Back Office, building/premises, human resources and communication) who would direct the recovery operations.

- FI must develop, implement and maintain a BCP document, which provides guidance for crisis management procedure and information, which enable the senior management of FI to respond to disruption and recover critical businesses in a contingency event to avoid contagion effect on business of the FI as a whole.
- The dimension of a disruption is another important element to be considered in identifying scenarios. The best practice is for senior management to identify all plausible crisis scenarios including disasters covering a wide area, transportation, telecommunication, key personnel, payment system and other key infrastructure and develop crisis management process and procedures. Scenarios should be documented and revised when regular business impact analysis requires them to be changed. The crisis management process at a minimum should include:
  - The process for ensuring early detection of an emergency/contingency and prompt notification to the DMT about the incident;
  - The process for the DMT to assess the overall impact on the respective institution and to make quick decision on the appropriate action;
  - Clear criteria for activation of the BCP and/or alternate sites;
  - The process for obtaining information on the status of the recovery process;
  - A process for timely internal and external communication; and
  - A process for overseeing the recovery and restoration efforts of the affected services/facilities.
- The best practice is for each business/support function to establish a business recovery team (which may have sub teams) to carry out the business resumption process. FI should assign recovery personnel (as well as alternate personnel) with required knowledge/skills to each such team.
- Business resumption process generally has three phases:
  - The mobilization phase – This phase involves notification to business recovery teams (using call-out tree, the predefined sequence of points of contact of staff for dissemination of information) and vendors to obtain required services; and follow predetermined sequence in the BCP (or revising the sequence if it is necessary);
  - The alternate processing phase – This phase involves the resumption of the business/service at DRS/or in a different way than the stipulated process. This may need record reconstruction and verification, establishment of new controls, alternative manual processes and alternative ways of dealing with customers/counterparties.
  - The full recovery phase - This phase involves a process for moving back to the primary site after a disaster/contingency event.
- The BCP should: identify and plan for activities which would be required under each phase of business resumption process; establish clear responsibilities; and develop and include recovery task's checklist.
- FI should pay special emphasis to ensure resilience of critical technology equipments/facilities to reduce the probability of having to activate the BCP in an inevitable disruption to business. The technology requirement for recovery of each business/support function should be specified in the recovery strategy for each function and FI should assign appropriate personnel/with alternate personnel for recovery of technical failures.
- FI may use an appropriate business continuity model to handle prolonged disruptions, based on the risk assessment of their business environment and the characteristics of their own operations.
- Each BCP should clearly identify the recovery point objectives for data losses for each of the critical system and the strategy to handle such data losses and information deemed vital for recovery of critical business/support functions in the event of a contingency/disaster. Some of the protection measures:
  - Back-up vital records must be readily accessible for emergency retrieval;
  - Access to back up vital records should be adequately controlled to ensure the reliability of them for the use of business resumption.

- Clear procedure indicating how and in what priority the vital records to be retrieved/created in the event that they are lost/damaged/destroyed.
- Institution should formulate a formal strategy for internal as well as external communication with key external parties (regulators, investors, customers, counterparties, service providers, the media and other stakeholders) to ensure dissemination of up-to-date and consistent information in a contingency situation.

Guideline 3: Test each aspect of the BCP regularly, completely and meaningfully

11. BCP should be tested regularly, completely and meaningfully considering qualitative and quantitative aspects, to measure its practicality and effectiveness; and to familiarize the staff with the location, recovery procedure at a disruption. This should include:

- Testing meaningfully all components of business processes including of connectivity, functionality and capacity of the infrastructure at the DRS;
- Testing the applicability of strategic planning assumptions to evaluate its applicability, particularly in respect of changes in the business scope;
- Measuring the awareness and preparedness of personnel and coordination with external parties;
- Testing of interdependencies especially with external parties. These would be the offices or service providers located outside Sri Lanka; and
- Management should participate in the tests and be familiar with their roles and responsibilities in a contingency event.
- To ensure effectiveness of a BCP, it is important to test regularly:
  - The whole system;
  - Call tree activation;
  - Backup site to backup site;
  - Shared services;
  - Backup tape restoration; and
  - Retrieval of vital records.
- A BCP needs to be tested at least once a year.
- A document should be prepared giving test results, lessons learned and risk mitigating measures to be adopted and submitted for the approval of the senior management.

Guideline 4: Formulate recovery strategies and set recovery time objectives for critical operations

12. Effective recovery strategies help FIs to implement their BCPs in an orderly manner as planned, minimizing disruptions and financial losses. FIs should identify their critical businesses and potential monetary as well as non-monetary losses in an event of a contingency. This process helps the FIs to prioritize critical operations and determine recovery strategies and RTO for critical business functions based on business impact analysis. Critical business functions vary among FIs but functions, which involve core banking and settlement of large value payment instructions, clearing of payment instruments, obligations on settling funds/securities and maintaining customer/investor/public confidence are critically important. The RTO is the maximum acceptable duration of time that can elapse, before the lack of a business function severely impacts on the business entity. This includes both the time before a contingency is declared and the time to perform tasks to the point of business resumption.

Guideline 5: Manage interdependency risks

13. There is a growing interest in FI to redistribute risks and processes locally, regionally or globally. This has resulted higher dependency on internal and external parties (clearing institutions, financial utility service providers, vendors and infrastructure providers). Therefore, they should understand and appropriately mitigate interdependency risks of critical business functions. Any failure to manage interdependency risk has a potential to cause operational or systemic inefficiencies or the failure of institutions. These interdependency need to be taken into consideration in a BCP and steps to be taken to establish a DRS (with SWIFT and other required communication links and

systems) in Sri Lanka, and to develop recovery strategies as well as RTO to mitigate risks. A business continuity arrangement of a FI should not introduce any risk to a systemically important or system-wide important payment, clearing and settlement system, its operator or participants and each FI should have an independent BCP for widespread and prolonged disruption to its infrastructure and critical services, without relying on another participant of such systems. If any critical functions are dependent on outsourced arrangements, adequate provisions should be in place to ensure operation of services by third parties.

Guideline 6: Plan for wide-area and prolonged disruptions

14. FIs should provide measures for scenarios, which may result significant losses or inaccessibility of critical infrastructure including SWIFT and telecommunication where there is a widespread or prolonged disruption.

Guideline 7: Practice separation policy to minimize concentration risk

15. FIs should practice separation policy to mitigate concentration risk. Disruptions may result in a non-availability of critical staff, information and required telecommunication links and payment infrastructure such as SWIFT. FIs should balance and properly mitigate concentration risk, while not sacrificing the efficiency gains from centralization of business processes and staff. Accordingly, FIs should take measures to separate critical business operations by:

- Establishing primary site and DRS in different zones. One DRS with SWIFT and other required communication links should be in Sri Lanka;
- Separation of critical operations and their supporting IT operations; and
- Separation of staff/cross training of staff.

16. FIs should adopt a change management procedure to update their BCPs in respect of changes with proper approval and documentation and also take steps to store copies of BCP at a location separate from the primary site. FI may disseminate any part of the BCP relevant to a concerned party including customers to create awareness enabling them to act in agreement with the FI. The part of the BCP available for reference of public may contain information relating to general readiness of the FI without any details of confidential nature.

17. FIs may also have insurance coverage as a mitigation strategy to minimize foreseeable risks and financial exposure in an event of a disaster. But diligence needs to be exercised with regard to the nature of insurance and the certainty of payments.

18. Each FI is required to inform Director, Payments and Settlements (DPS) of CBSL immediately if its BCP is activated. Until the FI resolves the crisis, it should send periodic progress reports to DPS.

19. Each FI is required to forward the following documents to the Director, Payments and Settlements, Level 8, Tower 1, Central Bank of Sri Lanka, Colombo 1:

(i) A copy of the revised BCP following these guidelines and approved by the Board for perusal of CBSL on or before September 29, 2006;
(ii) An annual risk management statement on or before January 15 of each year, indicating the critical systems, recovery time objective of each system and plans as well as strategies to achieve them; and
(iii) A quarterly statement within two weeks from the end of the relevant quarter, reporting contingency events (date, time and nature of the problem) occurred during the period for core banking/business and payment clearing and settlement systems; action taken in each event to rectify; and time of rectification and steps taken to avoid such failures in future.

Dr. Ranee Jayamaha
Deputy Governor