INSURANCE BOARD OF SRI LANKA

Guidelines on Business Continuity Plan

SECTION 1

Introduction

1. The global financial system is a set of interlinked networks of different types of markets, systems, and participants. While business organizations acknowledge the need to strengthen their resilience against disruptions, they also recognize that the network is only as strong as its weakest link and the potential impact of a major operational disruption may incapacitate the financial system.

2. The quick recovery of business functions after disruption is therefore crucial in maintaining confidence in business organizations. Failing which, organizations may compromise its business obligations, which may result in significant financial losses and potentially lead to a contagion effect on the financial system. Insurance coverage may compensate certain quantifiable losses but would not protect organizations against the erosion of brand value or the loss of customers' confidence.

3. Business Continuity Planning provides a quick and smooth restoration of operations after a disruptive event. Business Continuity Planning is a major component of risk management and it includes business impact analysis, business continuity plan (BCP) development, testing, awareness, training, and maintenance.

4. A BCP addresses actions to be taken before, during, and after a disaster. A BCP spells out in detail what, who, how, and when. It requires a continuing investment of time and resources. Interruptions to business functions can result from major natural disasters such as floods, fires and tsunami or from man-made disasters such as terrorist attacks. The most frequent disruptions are less sensational — equipment failures, theft, or employee sabotage. A disaster can de defined as any incident that causes an extended disruption of business functions.

5. Traditionally, disaster recovery planning (DRP) has focused on computer systems. Because mission-critical functions inevitably depend on technology and telecommunications networks, rapid recovery of these mission critical functions is of little value without recovering business unit operations. Mainframe and minicomputer systems usually have reliable recovery plans. Today, however, many critical applications have migrated to distributed and decentralized environments with less rigid controls. Recovering functional processes includes more than just information systems.

6. As with an insurance policy, it is hoped that a business continuity plan is never needed for a real disaster. Keep in mind that a BCP not maintained could be worse than no plan at all. Insurance Company's ability to recover mission-critical processes, resume operations, and eventually return to a normal business environment can be considered a major asset.

7. Thorough planning can reduce liability, disruption to normal operations, decision making during a disaster, and financial loss.

Business Continuity Plan (BCP)

8. A BCP is a set of ongoing processes, procedures, information and measures which are developed, compiled and maintained for critical business functions in readiness for use in an event of an emergency or a disaster which may cause inability to fulfil critical or all business operations. '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 servicing of existing /new policyholders.

9. It is essential that senior leadership of the organization sponsors and takes responsibility for creating, maintaining, testing, and implementing a comprehensive Business Continuity Plan (BCP). This will ensure that management and staff at all levels within the organization understand that the BCP is a critical top management priority. It is equally essential that senior leadership adopt a "top down" approach to the BCP so that management at all levels of the organization understand

accountability for effective and efficient maintenance of the BCP as part of the overall governance priorities. 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.

SECTION 2

Purpose, Scope and Application of the Guidelines

10. Recent world events have challenged us to prepare to manage previously unthinkable situations that may threaten an organization's future. This new challenge goes beyond the mere emergency response plan, disaster recovery plan or disaster management activities that we previously employed. Organizations now must engage in this comprehensive process, which is best described generically as *Business Continuity.* It is no longer enough to draft an emergency response plan or a disaster recovery plan that anticipates naturally, accidentally, or intentionally caused disaster or emergency scenarios.

11. Today's threats require the creation of an on-going, interactive process that serves to assure the continuation of an organization's core activities before, during, and most importantly, after a major crisis event. In the simplest of terms, it is good business for a company to secure its assets. The Board of Directors and shareholders must be prepared to budget for and secure the necessary resources to make this happen. It is necessary that an appropriate administrative structure be put in place to effectively deal with crisis management. This will ensure that all concerned understand who makes decisions, how the decisions are implemented, and what the roles and responsibilities of participants are. Personnel used for crisis management should be assigned to perform these roles as part of their normal duties and not be expected to perform them on a voluntary basis. An organization's leadership has a duty to stakeholders to plan for its survival.

12. The main objective of these guidelines is to explain the IBSL's supervisory approach on BCP and provide guidance on sound practices, which IBSL encourages insurance companies to follow in order to;
    - Have workable and sound BCPs for servicing of existing /new policyholders to ensure that the agreed service levels are met in an event that one or more components of a system fail. Moreover, BCPs should ensure continuity of agreed services in an event of a prolonged and widespread disruption;
    - Minimise the financial, legal, and other risks arising from such disruptions; and
    - Develop a consistent framework for BCPs of Insurance Companies.

13. The Business Continuity Guidelines are applicable to all insurance companies registered in terms of the Regulation of Insurance Industry Act, No. 43 of 2000. One of the supervisory objectives of IBSL is for insurance companies to implement a BCP to ensure high preparedness for continuation of critical operations in the event of a disruption. The IBSL, in the course of its on-site and offsite examinations and reviews, and meetings on prudential issues with insurance companies, will review implementation of BCP on the practices set out in these guidelines particularly:
    - The extent to which the insurance company has observed the BCP Guidelines; and
    - The risk profile of the insurance company and its role in ensuring the stability of the financial system.

SECTION 3

Guideline 1 – The Board of Directors and Senior Management should hold the primary responsibility for the BCP preparedness of their company.

14. The Board of Directors and Senior management of each insurance company should take the primary responsibility for the BCP of their organisation. The Board of Directors and senior management of an insurance company is ultimately responsible for the risk management and effectiveness of the BCP subsequently. The Board of Directors and senior management should involve in business continuity management and consider their organization's business continuity, risks and mitigating measures as part of its overall risk management framework.

15. The Board of Directors is also responsible for endorsing policies, standards and principles developed by senior management for business continuity planning, providing clear guidance and directions in relation to BCP, ensuring maintenance and periodic updating of BCP and reviewing BCP test results.

The senior management has ultimate responsibility for establishing appropriate policies, standards, strategies and processes for developing the BCP, getting the BCP endorsed by the Board of Directors, ensuring that sufficient resources are devoted to implementing the BCP and executing the BCP in an event of a contingency. They must ensure that the necessary administrative support functions in the recovery effort, such as human resources, finance, legal, security, etc., are in place. They should also ensure that all levels of staff within the organization are aware of the importance of BCPs and the role it plays in ensuring the continuous functioning of the organization and preserving the functionality of the financial system as a whole. Further, the senior management is to ensure that employees responsible for managing the BCP are adequately trained and aware of their responsibilities.

16. The Board of Directors and senior management should establish clearly which function of the organization has responsibility for managing the entire process of business continuity planning ("the *BCP function")* and they should ensure that an independent party, such as internal or external audit, tests the BCP and that any shortcomings identified are addressed in an appropriate and timely manner. In support of the corporate governance process, senior management should submit a formal written annual statement to the Board of Directors indicating whether management is satisfied that the recovery strategies adopted are still valid, and whether the BCP management team and/or an independent party have properly tested the BCP during the period. This annual statement should be incorporated into the BCP, as the IBSL will review it as a part of its on-site examinations.

Guideline 2 – Development and implementation of an effective Business Continuity Plan (BCP)

17. The development and implementation of a BCP should involve business impact analyses, business recovery strategies, testing, training programs, communications and crisis management.

17.1 Step One – Conduct a Business Impact Analysis (BIA)

The objective of the business impact analysis is to identify different kinds of risks to business continuity and to assess the potential impact of system failures on core business processes; assess the risks (infrastructure, operational, credit, liquidity, market, solvency, legal and reputation) arising from the total environment in which the organization operates; assess the impact of materialized risks, i.e. loss of revenue, impact upon customers, regulatory issues, impact upon employees, and other business interruption consequences. Based on the results of the analysis, the organization should be able to identify the scope of the critical services to be provided, define the minimum acceptable levels of service for each core business process and establish time frames in which the services should be resumed.

17.2 Step Two – Formulate a Business Recovery Strategy (BRS)

A business recovery strategy sets out recovery objectives and priorities that are based on the business impact analysis. Among other things, it establishes targets for the level of service a company would seek to deliver in the event of a disruption and the framework for ultimately resuming business operations. A recovery strategy should indicate the level of services that the company is able to provide at various stages during and after operational disruptions. In formulating a recovery strategy, insurance company should assess the results of the business impact analysis as well as the interdependency among critical services, as these are key factors in determining the recovery priority of individual services and operations. Individual business and support functions should formulate their own recovery strategies on how to achieve the recovery of a minimum level of critical services within a specified time frame. This involves the determination of an alternate recovery site (see Guideline # 4), total number of recovery personnel and the related workspace, applications and technology requirements, office facilities and vital records required for the provision of such levels of service.

17.3 Testing each aspect of the BCP

The testing of a company's ability to recover critical operations and services as intended in the event of a disruption is an important component of an effective BCP. Insurance Companies should test their BCPs regularly, completely and meaningfully to evaluate its practicality and effectiveness and update the BCPs as appropriate. The testing programme should validate the business continuity strategy; develop and document continuity test plans; prepare and execute tests; update disaster recovery plans (DRPs) and procedures. Insurance companies should test their BCP at least once a year. Frequent testing is a vital element of effective BCP.

Testing should ideally be undertaken by the team who will operate the BCP to ensure effective team working, preparedness and awareness. Management should participate in these tests and be familiar with their roles and responsibilities in the event of activation. Changes in technology, business processes and staffs' roles and responsibilities can affect the appropriateness of the BCP; and ultimately the business continuity preparedness of the company. Continuous reviews and meaningful testing of all components of the BCP should be undertaken to reflect the risks faced by the company, changing circumstances, to familiarize staff with the operation of the plan, to verify that the plan is practically workable, and to identify issues that need to be addressed that were not apparent during the planning stage. An independent party, such as internal or external audit, should assess the effectiveness of the company's testing programme, review test results and report their findings to senior management and the board.

17.4 Provide Training Programs

The roles and responsibilities of each member of the business continuity team should be clearly defined and delegated and appropriate training should be provided to these employees. All employees should also be aware of the importance of the BCP within the company's overall risk management framework and emergency contacts in the event of an operational disruption.

17.5 Communications

The BCP should outline internal and external communication channels (with regulators, reinsurers, investors, customers, business partners, service providers, staff, the media and other stakeholders) in the event of an operational disruption. The BCP should also incorporate comprehensive emergency communication protocols and procedures in the case of a major operational disruption. Due to the increasing interdependency and interconnectedness among financial institutions within and across jurisdictions, a major operational disruption may extend beyond a company's national borders and may consequently affect affiliated institutions in other jurisdictions. This may ultimately impact the financial system of the home and other host countries. A company's BCPs should contain communication protocols for contacting relevant non-domestic financial authorities and institutions in these instances.

17.6 Establish a Crisis Management Process

An effective BCP should set out a crisis management process that serves as documented guidance to assist insurance companies in identifying potential crisis scenarios and develop procedures for managing these scenarios. Insurance Companies should establish crisis management teams, comprised of senior management and heads of major support functions, to respond to and manage the various stages of a crisis.

Guideline 3 – Organisations should incorporate sound practices in the BCP

18. BCP is a risk-based and proactive process that includes understanding the entire ramification to the business, incident response, crisis management and external communications. It addresses operational risks by developing processes and procedures for the recovery of critical business functions to fulfil business obligations.

19. Each insurance company is encouraged to consider the following process for business continuity planning:

- A BCP should be credible, have a clear strategy and accountability, be practical in operation, updated as the business changes.
- Adopt an unambiguous BCP policy and strategies depending on the scale and scope of the business of the organisation.
- Establish clear roles and responsibilities to supervise the BCP implementation programmes. This may be inline with the requirement of setting up of an authorised business continuity management team to coordinate planning and implementation.

- With clear identification of key functions under each system, the processes within these functions should be categorised according to the criticality.
- Establish at least a minimum BCP requirement for the provision of critical businesses. The senior management should approve these minimum BCP requirements before proceeding to the development of BCP. Moreover, BCP requirement should be considered at the development or planning stages of new business services/products.
- Once a BCP is established, it should be regularly reviewed, maintained and each aspect of the BCP regularly and completely tested to ensure its currency, effectiveness and operational viability. Insurance companies should strive to build an organisational culture of embedding risk - based BCP into their business-as-usual operations and day-to-day management.

Guideline 4 – Alternate Recovery Sites for Business Continuity

20. An **alternate recovery site** is a site held in readiness for use during a *business continuity* event to maintain an organization's *business continuity.* A useable functional alternate recovery site is an integral component of all BCPs. In assessing the suitability of an alternate recovery site, emphasis should be placed on location, speed of recovery and adequacy of resources. Alternate recovery sites should be sufficiently distanced to avoid being affected by the same disaster as primary sites and should be readily accessible and available for occupancy within the time requirement specified within the BCP.

21. Business resumption very often relies on the recovery of technology resources that include applications, hardware equipment and network infrastructure as well as electronic records. Insurance Companies should ensure that alternate recovery sites are adequately equipped with the technology requirements that are needed for the recovery of individual business and support functions. Alternate recovery sites should have sufficient technical equipment of appropriate model, size and capacity to meet recovery requirements. The site should also have adequate telecommunication facilities and pre-installed network connections to handle the expected volume of business. Emphasis should be placed on the resilience of critical technology equipment and facilities such as uninterruptible power supply.

22. Equipment and facilities at alternate recovery sites should be subject to continuous monitoring and periodic maintenance and testing to keep them operational. Insurance Companies should also ensure that alternate recovery sites are equipped with the necessary personnel/manpower to perform recovery functions. Copies of vital records should be readily accessible at alternate recovery sites for emergency retrieval by personnel.

Guideline 5 – Manage and appropriately mitigate interdependency risks

23. There is a trend for organizations to divide and redistribute risk and processes locally, regionally or globally. This has led to increased dependency on other internal and external parties. Any mismanagement of interdependency risk could cascade into operational or systemic inefficiencies, potentially leading to the failure of institutions.

24. When developing the business continuity plan of critical business functions, organizations should take into account the interdependencies of these functions, and the extent to which they depend on other parties. Organizations should also be aware of the business processes of these parties that support their critical functions, especially their BCP preparedness and recovery priorities. Such dependencies should be factored in when organizations prepare their recovery strategies and recovery time objectives.

Guideline 6 – Plan for wide-area (zonal) and prolonged disruptions

25. A zone can be defined as a reasonable area (two kilometres in diameter) that could be affected by the same disruption. Organisations should provide adequate measures by broadening and deepening the scope of the BCP, to cater for scenarios where there are significant loss or inaccessibility of critical staff, a widespread and prolonged disruption of critical services such as telecommunications, electricity, etc., in their BCP, taking into consideration their respective levels of critical business activities, risk tolerance and risk management policies.

Guideline 7 – Practice 'Separation Policy' to mitigate concentration risk

26. The organisations should adopt 'separation policy' to mitigate concentration risk. Critical staff and information are important assets that are difficult to replace quickly. Organizations should pay attentions to assess their concentration risk when business operations and technology specially the IT equipment and staff, are housed within the same zone.

27. Hence it is important to strike a proper balance between mitigating concentration risk and increasing human safety, and that of not losing the efficiencies gained from the centralization of business processes and critical staff. Accordingly, the organizations should take measures to separate critical business operations by:
    - Establishing the primary site and alternate recovery site in different zones;
    - Separating critical operations and their supporting IT operations; and
    - Separation of staff/cross training staff.

28. The organizations should take measures to adopt a change management procedure to update their BCPs relating to changes with proper approval and documentation. Further, steps should be taken to store copies in a location, which is separated from the primary site. The companies may disseminate any part of the BCP, which is relevant to a party in concern including customers to create awareness among the public. The part of the BCP available for reference for public may contain information without any confidential details, regarding preparedness of the company.

Guideline 8 – Reporting requirements

29. Each insurance company is required to inform the Director General of Insurance Board of Sri Lanka immediately if its BCP is activated. The company should send periodic progress reports to DG, IBSL until the company resolves the crisis.

30. Each insurance company is required to forward their BCP following these guidelines and approved by the Board of Directors for perusal of the Insurance Board of Sri Lanka on or before 31st July 2007.

31. Senior management should submit an annual statement to the Board of Directors of their organisation indicating whether management is satisfied that the recovery strategies adopted are still valid, and whether the BCP management team and/or an independent party have properly tested the BCP during the period and it should be incorporated in to the BCP, which will be reviewed by he IBSL as a part of its on-site examinations.