SUPERVISORY AND REGULATORY GUIDELINES: PU19-0406
Business Continuity
Issued: 1st May, 2007
Revised: 14th October 2008

BUSINESS CONTINUITY GUIDELINES

I. INTRODUCTION

The Central Bank of The Bahamas ("*the Central Bank*") is responsible for the licensing, regulation and supervision of banks and trust companies operating in and from within The Bahamas pursuant to the Central Bank of The Bahamas Act, 2000 ("the CBA") and the Banks and Trust Companies Regulation Act, 2000 ("the BTCRA"). Additionally, the Central Bank has the duty, in collaboration with financial institutions, to promote and maintain high standards of conduct and management in the provision of banking and trust services.

All licensees are expected to adhere to the Central Bank's licensing and prudential requirements and ongoing supervisory programmes, including periodic on-site inspections, and required regulatory reporting. Licensees are also expected to conduct their affairs in conformity with all other Bahamian legal requirements.

II. PURPOSE

The events of September 11, 2001 in the United States, terrorist attacks in London, Madrid, Istanbul and elsewhere, outbreaks of Severe Acute Respiratory Syndrome (SARS) and potentially an Avian Flu epidemic have demonstrated the need for robust business continuity[1] arrangements across the globe. This holds true for The Bahamas, which has been subject to hurricanes and island wide electrical outages in recent times. Licensees could face critical operational disruptions due to natural disasters, island-wide electrical outages, faulty inter-bank electronic linkages and other computer problems, acts of terrorism and system failures among others, hence the need to secure business continuity by formulating action plans in advance to ensure quick recovery.

The quick recovery of business functions after disruptions is therefore crucial to maintaining public confidence in licensees and the financial system as a whole. Failing which, licensees may impair their ability to provide service to clients (i.e. customers, depositors or investors) and honour obligations to other financial sector intermediaries,

[1] **Business Continuity** is a state of continued, uninterrupted operation of a business

which may result in significant financial losses and potentially lead to a contagion effect on the financial system.

Business Continuity Management ("*BCM"*) is a comprehensive approach that includes policies, procedures and standards for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption and by extension, ensures that the functionality of the financial system as a whole is preserved. An important tangible evidence that an institution has embraced BCM is the formulation of an effective and workable Business Continuity Plan ("*BCP*"). The resilience[2] of a financial system to major operational disruptions[3] will be determined by the robustness of the BCPs of all participants within the system.

A BCP is a comprehensive written plan of action that sets out the procedures and establishes the processes and systems necessary to continue or restore the operation of an organization in the event of a disaster or major operational disruption. The BCP provides detailed guidance for implementing the recovery plan and outlines the roles and responsibilities in managing operational disruptions. It also defines triggers for activating licensees' BCPs and establishes business resumption teams for each core business process. An effective BCP should set out the decision-making authority in the event of an operational disruption and provide clear guidance regarding the succession of authority under those circumstances.

The Central Bank endorses the Joint Forum's[4] Paper *"High level principles for business continuity"* issued in August 2006 and has adopted the principles recommended by the Joint Forum in the aforesaid document. These Guidelines outline essential principles that the Central Bank will use as a benchmark in assessing the adequacy of its licensees' BCPs. The Central Bank expects all licensees to develop and implement workable and effective BCPs to ensure that specified operations can be maintained or recovered in a timely manner in the event of a disruption, consistent with the nature, size, and scope of their operations and complexity of their business. Additionally, BCPs are by their nature dynamic, evolving and changing as circumstances dictate and hence should be updated regularly. BCPs should also be flexible to address a broad range of potential disruptions.

III. APPLICABILITY

The Business Continuity Guidelines ("*the Guidelines"*) are applicable to all banks and trust companies licensed to do business in and from within The Bahamas. The Guidelines are not intended to be prescriptive, nor does their broad applicability mean a "one-size-

[2] **Resilience** is the ability of an organization, network, activity, process or financial system to absorb the impact of a major operational disruption and continue to maintain *critical operations or services*.

[3] **A major operational disruption** is a high-impact disruption of normal business operations affecting a large metropolitan or geographic area and the adjacent communities that are economically integrated with it; and subsequently affects physical infrastructure.

[4] The **Joint Forum** comprises the **Basel Committee on Banking Supervision**, the **International Organization of Securities Commissions (IOSCO)** and **the International Association of Insurance Supervisors**.

fits-all" approach to business continuity. A licensee's business continuity plan should be flexible, proportionate to its operational risk (arising from both internal and external sources) and tailored to the nature, size, scale and scope of its operations and complexity of its business.

In the case of a licensee that is a branch of a foreign bank, the head office's BCP will suffice, if the plan makes adequate provisions in line with these Guidelines for the licensee. In the case of a licensee that is a subsidiary of a banking group subject to consolidated supervision, the group's BCP will suffice, if the plan makes adequate provisions in line with these Guidelines for the licensee.

With respect to managed licensees, the ultimate responsibility for developing a BCP rests with the parent of the licensee. However, the Central Bank will accept an agreement between such licensees and their managing agents on business continuity and the plans in place to address the same.

Senior management should familiarize themselves with the Guidelines and understand the intent and implications of the principles. Licensees should also read the Guidelines in conjunction with the following documents:

- *Minimum Standards for the Outsourcing of Material Functions*
- *Aide Memoire on Handling Confidential Information Outside The Bahamas*

Licensees are encouraged to conduct a self-assessment of their BCPs against the principles outlined in the Guidelines and rectify deficiencies where applicable.

IV. Board and Senior Management Responsibilities

The Board of Directors of a licensee *("the Board")* is ultimately responsible for risk management and subsequently the BCP and the effectiveness of the same. The Board is also responsible for endorsing policies, standards and principles developed by senior management for business continuity management.

Senior management has ultimate responsibility for developing the BCP and ensuring that sufficient resources are devoted to implementing the plan. They must ensure that the necessary administrative support functions in the recovery effort, such as human resources, insurance, legal, security, etc., are in place. They should also ensure that all levels of staff are cognizant of the importance of BCPs and the role it plays in ensuring the continuous functioning of the institution and preserving the functionality of the financial system as a whole. Further, senior management is to ensure that employees responsible for managing the BCP are adequately trained and aware of their responsibilities.

Senior management should establish clearly which function of the licensee has responsibility for managing the entire process of business continuity planning ("*the BCP function")*. This information should be communicated to the Central Bank and will be the main point of contact between the Central Bank and the licensee with respect to the BCP.

The Board and senior management 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 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 Central Bank will review it as a part of its on-site examinations.

V. DEVELOPMENT AND IMPLEMENTATION OF AN EFFECTIVE BCP

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

1. Business Impact Analysis

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 reputational) arising from the total environment in which the licensee 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 licensee should be able to identify the scope of the critical services to be provided, define the minimum acceptable levels of service/outputs for each core business process and establish time-frames in which the services should be resumed.

2. Business Recovery Strategy

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 licensee 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 a licensee is able to provide at various stages during and after operational disruptions.

In formulating a recovery strategy, a licensee 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 site[5], 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.

3. Testing

The testing of a licensee's ability to recover critical operations and services as intended in the event of a disruption is an important component of an effective BCP. Licensees should test their BCPs, evaluate their effectiveness and update their 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 and procedures. Testing should ideally be undertaken by the team who will operate the BCP to ensure effective team working, preparedness and awareness.

Changes in technology, business processes and staffs' roles and responsibilities can affect the appropriateness of the BCP; and ultimately the business continuity preparedness of licensees. Continuous reviews and meaningful testing of all components of the BCP should be undertaken to reflect the risks faced by the licensee, 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 licensee's testing programme, review test results and report their findings to senior management and the board.

4. 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 cognizant of the importance of the BCP within the licensee's overall risk management framework and emergency contacts in the event of an operational disruption.

5. Communications

[5] An **alternate site** is a site held in readiness for use during a *business continuity* event to maintain an organization's *business continuity*. The term applies equally to work space or technology requirements.

The BCP should outline internal and external communication channels (with regulators, investors, customers, counterparties, 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 licensee'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. Licensees' BCPs should contain communication protocols for contacting relevant non-domestic financial authorities and institutions in these instances.

6. Crisis Management

An effective BCP should set out a crisis management process that serves as documented guidance to assist licensees in identifying potential crisis scenarios and develop procedures for managing these scenarios. Licensees 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.

VI. ALTERNATE SITES FOR BUSINESS CONTINUITY

A useable functional alternate site is an integral component of all BCPs. Where the proposed alternate site is located outside The Bahamas, licensees are advised to assess the appropriateness of the jurisdiction for the temporary relocation of its operations. The First Schedule of the Financial Transactions Reporting Act 2000 (FTRA) provides a list of countries, which the Central Bank regards as being acceptable for this purpose. All other jurisdictions will be assessed by the Central Bank on a case-by-case basis.

In assessing the suitability of an alternate site, emphasis should be placed on location, speed of recovery and adequacy of resources. Alternate 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.

Business resumption very often relies on the recovery of technology resources that include applications, hardware equipment and network infrastructure as well as electronic records. Licensees should ensure that alternate sites are adequately equipped with the technology requirements that are needed for the recovery of individual business and support functions. Alternate 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.

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

VII. CONFIDENTIALITY REQUIREMENTS AND RELOCATION OF OPERATIONS

Licensees are required to ensure that relevant Bahamas statutory requirements relating to client confidentiality continue to be observed, where the BCP will involve the disclosure of customer information to third parties. In this regard, licensees should have controls in place to ensure that the requirements of customer consent and customer data confidentiality are observed and proper safeguards are established to protect the integrity of client information. In the absence of the aforesaid customer consent, the licensee will be expected to enter into an agency agreement subject to the approval of the Central Bank, with the third party prior to the disclosure of customer information to the same.

Where the BCP also requires the temporary physical relocation of Bahamas-based staff and operations to another jurisdiction, licensees should take care in advance to ensure that the operations of those staff are not in breach of local law in that jurisdiction. The Central Bank, for its part, will do everything it can to seek the co-operation of local regulators, particularly in neighbouring jurisdictions; to do all they can to facilitate the smooth temporary transfer of business. Nevertheless, the Central Bank must be in a position continue its regulation/supervision of temporarily relocated functions outside The Bahamas.

VIII. APPROVAL/REPORTING REQUIREMENTS

Licensees are required to confirm to the Central Bank that they have a BCP in place, which should include the name and contact information for the BCP function. Furthermore, licensees are strongly encouraged to seek and obtain legal advice that their BCPs are in compliance with Bahamian legal requirements, particularly with respect to the preservation of client confidentiality. Central Bank approval is not required for activation of BCPs; however, licensees should inform the Inspector of Banks and Trust Companies as soon as possible after activation of the BCP.

In addition, the Board is required to include a statement in the Annual Corporate Governance Certificate confirming that the Board is satisfied that the recovery strategies adopted in the BCP are still valid, and that the licensee's BCP management team and/or an independent party have properly tested the BCP during the period.

The Central Bank will, in the course of its on-site examinations, review the BCP implemented, taking into consideration the extent to which a licensee has observed the Guidelines and its risk profile.

*****End*****

Appendix 1

Examples of Business Continuity Arrangements

- Use of fault-tolerant or duplicated hardware;
- Adequate succession planning and staff orientation;
- Arrangements for the cover and accessibility of key staff members;
- Regular preventative maintenance of all computer and telecommunications components;
- On-site supplies of spare hardware and telecommunications components;
- Internally generated or uninterrupted power supplies;
- Fire detection and extinguishing systems;
- Predetermined emergency responses;
- Storage of important documents at both primary and secondary sites;
- Use of alternate processes and service providers;
- Insurance coverage against foreseeable disruptions;
- Developed procedures for the exchange of data by physical media (disks, tape, paper) in the event of telecommunications failure; and
- Capability to revert to old technology when new software, hardware or telecommunications component is implemented.

Appendix 2

Components of an Effective Business Continuity Plan

Institutions should ensure that its business continuity plans are comprehensive, having been based on the business impact analysis and recovery strategies of the institution. Business continuity plans must be documented and should contain a series of key elements:-

- a business continuity plan awareness program;
- a risk management program that includes clearly defined roles and responsibilities for resumption of business processes, including support organization functions;
- continuity plans for each core business process;
- procedures for mitigating interdependency risks between departments within the institution and with other institutions;
- trigger points and/or dates to activate the continuity plan;
- data back-up and recovery (hard copy and electronic);
- processes to deal with the loss of information that are not available from backup data;
- manual processes for continuing operations until technology is repaired;
- accessible recovery locations and emergency operations centres;
- a process for automatically switching telephone and date lines;
- testing of the business continuity plans on an end-to-end basis;
- a review process to ensure that the business continuity plan is feasible and up-to-date; and
- specific incident/ emergency management responses that identify assembly areas at a safe distance from the site of the incident; and
- annual statement by senior management on whether the recovery strategies adopted are still valid and whether the documented BCPs are properly tested and maintained.