BUSINESS CONTINUITY MANAGEMENT GUIDELINES FOR BANKS AND FINANCIAL INSTITUTIONS

DIRECTORATE OF BANKING SUPERVISION

AUGUST 2009

TABLE OF CONTENTS PAGE

1.0 INTRODUCTION

1.1 Background

Banks and financial institutions are susceptible to operational disruptions caused by internal and external threats such as fire, earthquakes, wars, terrorist attacks, system failures, etc. Such disasters may lead to severe operational disruptions and sometimes threaten the solvency and business continuity of institutions, which could adversely impact the financial system as a whole. In today's world, Business Continuity Management (BCM) is becoming increasingly important.

In issuing these Guidelines, Bank of Tanzania recognizes the need for banks and financial institutions to have in place an effective BCM that will ensure their ability to operate on an ongoing basis and limit losses in the event of an operational disruption. The Guidelines set minimum requirements for establishing sound and effective BCM practices in banks and financial institutions.

BCM has to be comprehensive in such a way as to include policies, strategies, plans, procedures and standards for ensuring that specified operations can be maintained or recovered in a timely manner in the event of a disruption and, by extension, ensures that the functionality of the financial system as a whole is preserved. One of the tangible evidence that an institution has embraced BCM is the formulation of an effective and workable Business Continuity Plan (BCP).

A BCP sets out procedures, processes and systems necessary to continue or restore the operation of an organization in the event of a disruption. It provides detailed guidance for implementing the recovery plan and outlines the roles, responsibilities and succession in managing operational disruptions. It also defines triggers for activating the BCP and establishes business resumption teams for core business processes. The resilience of a financial system to major operational disruptions will be determined by the robustness of the BCPs of all participants within the system.

1.2 Citation

These guidelines shall be cited as "*Business Continuity Management Guidelines for Banks and Financial Institutions"*

1.3 Authorization

These Guidelines are issued under Section 71 of the Banking and Financial Institutions Act, 2006, which empowers the Governor of the Bank of Tanzania to issue guidelines in addition to regulations, directives and circulars expressly mentioned under the Act.

1.4 Application of the Guidelines

These guidelines shall apply to all banks and financial institutions licensed by the Bank to carry on banking business.

1.5 Objectives of the Guidelines

The guidelines aim at achieving the following objectives:

(i) Define major elements and highlight the role of business continuity within an institution;

(ii) Outline the duties of the Board, Senior Management, employees and the internal audit function with regard to business continuity;

(iii) Provide guidance to banks and financial institutions on how to develop an effective BCP given the scope and size of their operations;

(iv) Guide banks and financial institutions in making adequate preparations to deal with possible business interruption scenarios; and

(v) Provide guidance to banks and financial institutions on how to evaluate the adequacy of their BCPs.

2.0 BUSINESS CONTINUITY MANAGEMENT GUIDELINES

2.1 Business Continuity Management Policy

Every bank or financial institution shall establish a BCM policy to govern formulation and maintenance of all aspects of business continuity.

The BCM policy of an institution must be approved by the Board and shall be communicated to all relevant levels of the institution in a timely manner. It should take into account appropriate structures including the institution's business continuity objectives, plans, scope, limitations and exclusion. Any significant deviation from the policies must be communicated to Senior Management/Board for corrective measures. The BCM policy should provide for formation of various BCM teams and description of their roles such as BCM Steering Committee, Business Continuity Management Team, Crisis Management Team, Business Recovery Team etc. Furthermore, it should provide for policy reviews at regular intervals and when significant changes occur.

2.2 Major Duties and Responsibilities

Banks and financial institutions should have effective and comprehensive approaches to Business Continuity Management. Board of Directors and Senior Management are responsible for the organization's business continuity. Additionally, Internal Audit and all employees of an organization have a role in business continuity management.

2.2.1 Board of Directors Responsibilities

The responsibility for business continuity management of an institution ultimately lies with the Board of Directors. Specific responsibilities of the Board include approving business continuity management policies, standards and principles developed by Senior Management and ensuring compliance with regulatory and legal requirements for Business Continuity Management.

2.2.2 Senior Management Responsibilities

Senior management is responsible for steering BCM, developing the BCP and strategies necessary for the continuity of critical business functions. They must ensure that at minimum, the necessary administrative support functions in the recovery effort, such as human resources, insurance, legal and security are in place. They should also ensure that all levels of staff are cognizant of the importance of BCPs and the business recovery objectives. Specifically, senior management shall be responsible for the following:

(i) Assigning the overall management of the business continuity function to a Business Continuity Management Team. Such Team shall draw its membership from the following:

1. Senior Management (Coordinator)
2. Functional Departmental Heads
3. Line Managers
4. Risk Management Officer.

(ii) Establishing a Crisis Management Team, consisting of key executives and functional heads of critical operational areas, which will be responsible for dealing with crisis management and business continuity during a crisis. The roles and responsibilities of each individual member should be clearly defined;

(iii) Ensuring that there is a plan for business continuity in line with the institutional business strategy and plan;

(iv) Allocating sufficient human and financial resources for the development and maintenance of the BCP;

(v) Preparing policies by determining how the institution will manage and control business continuity risks;

(vi) Reviewing BCP test results on regular basis;

(vii) Keeping the BCP up to date and reviewing it at least annually;

(viii) Ensuring that employees are trained and are fully aware of their roles in the implementation of BCM;

(ix) Ensure that there is a framework for reporting to the Board and Senior Management on matters related to BCM;

(x) Ensuring that, at least annually, the institution's BCM is subject to review by an independent party, such as internal or external auditor;

(xi) Ensuring that roles as well as responsibilities and authority to act, and succession plans are clearly articulated in institutions' BCM policies to avoid confusion in the event of a disruption;

(xii) Ensuring that the BCP not only consider business processes and technical aspects, but also recognizes and addresses the human element. The overriding consideration in formulating an institution's BCP should be the preservation of human life; and

(xiii) Demonstrating that they have sufficient awareness of the risks, mitigating measures and state of readiness by way of a statement to the Board of Directors. Such statement should be updated at least once a year or more frequently should there be material change within the institution.

2.2.3 Employee Responsibilities

Each employee of a bank or financial institution should be aware of his/her role in the BCP, the importance of having a BCP and the role it plays in ensuring the continuous functioning of the institution and preserving the functionality of the financial system as a whole.

2.2.4 Internal Audit Responsibilities

The internal audit function of a bank or financial institution should conduct periodic reviews of the BCP to determine whether the plan is realistic and remains relevant, and whether it adheres to the policies and standards established by the Board.

2.2.5 Outsourced Business Continuity Management Function

A bank or financial institution may opt to outsource some of the BCM functions. The institution shall take regard of the requirements of Outsourcing Guidelines for Banks and Financial Institutions, 2008. Nevertheless, the following shall be observed:

(i) Accountability for BCM ultimately rests with the Board of Directors of a bank or financial institution;

(ii) In outsourced solutions that are syndicated, care must be taken not to syndicate services between banks or financial institutions, where they have normal business functions close or adjacent to each other. Dedicated options should be taken to ensure recovery in the event of a city wide incidence.

2.2.6 Business Continuity Management Team

A bank or financial institution will constitute a BCM Team for the purpose of the overall management of business continuity. Major roles and responsibilities of the Team shall include the following:

(i) To develop a business continuity management process and plan. Such plan should be developed taking into account five aspects which are in line with the business continuity management life cycle

a. Strategic stage – examine the organizational framework taking note of the key stakeholders, legislative and regulatory requirements in relation to business continuity;

b. Process stage – develop resumption strategies for business processes and activities;

c. Resource Recovery – ensure the deployment of appropriate resources to all business processes and activities;

d. Awareness and Education – develop a business continuity culture through assessment of business continuity awareness campaigns;

e. Testing, Maintenance, Measurement and Audit – ensure reliability of the business continuity plan through independent review and testing.

(ii) To periodically conduct Business Impact Analysis (at least once a year), an institution-wide risk assessment and monitoring to identify the mission critical activities and vulnerability for major disruptions;

(iii) To ensure that the business continuity plan is updated to reflect the changes in the risk profile of the bank or financial institution;

(iv) Report on the status of business continuity management to the Board and Senior Management on a regular basis, highlighting where gaps are identified;

(v) To facilitate testing of plans to ensure that team members are aware of their roles and responsibilities in the event of a disruption;

(vi) To ensure that the institution's response to a disruption is communicated internally and externally to applicable parties.

2.3 Business Impact Analysis (BIA)

Every bank or financial institution shall conduct institution-wide Business Impact Analysis (BIA) to identify business functions that are mission critical and major potential losses (in monetary and non-monetary terms) in case of disruptions

BIA forms the foundation upon which the BCP is developed. It identifies critical business functions and operations that need to be recovered on a priority basis and establishes appropriate recovery objectives for those operations. It should be completed in advance of a risk assessment in order to identify urgent functions upon which risk assessment should be focused. Ultimately, each bank and financial institution should:

(i) Determine their mission critical business functions depending on the nature, scale and complexity of their business and the institutions' obligations to the market, customers and industry;

(ii) Estimate the maximum allowable down time and acceptable levels of data, operations and financial losses;

(iii) identify, those business functions and operations to be recovered on a priority basis;

(iv) Through BIA a bank or financial institution will be able to gather information about resource requirements over time to enable each critical business function within the institution to achieve continuity within the established timeframes. This would at minimum identify:

a. Staff numbers and key skills

b. Data application and systems

c. Constraints

d. Mission Critical Activities (MCA) or tasks that need to be recorded to ensure continuity of the process and business

e. Dependencies on people, systems, processes, internal and external parties

f. Recovery Time Objectives (RTO) and Recovery Point Objective (RPO) for every Mission Critical Activity (MCA)

g. Systems impact assessment highlighting:

i. location;

ii. department unit owners, system information, commissioning dates;

iii. technical person responsible;

iv. RTO and RPO and dependencies; and

h. Provide a list of recovery option for each business process;

2.4 Risk Assessment

Every bank or financial institution shall at least once a year, conduct an institution-wide risk assessment in respect of the identified mission critical functions and ascertain potential for major disruptions.

A risk assessment looks at the probability and impact of a variety of specific threats that could cause a business disruption. It focuses on the critical business functions identified during business impact analysis. Risk assessment is at minimum expected to achieve the following:

(i) Identify unacceptable concentrations of risk and what are known as 'single point of failure'

(ii) Identify internal and external threats that could cause a disruption and assess their probability and impact;

(iii) Prioritize threats according to the institution;

(iv) Provide information for a risk control management strategy and an action plan for risks to be addressed;

(v) Mitigation of risks through a documented remedial plan;

(vi) Ensure BCPs are updated regularly to reflect the changes in the institution's operational risk profile; and

(vii) Specify events that should prompt implementation of the plans;

2.5 Business Continuity Strategies

Every bank or financial institution shall set business continuity strategies to ensure recovery and continuity of its critical operations in the face of a disaster or other major incident or disruption.

An institution shall set up and maintain appropriate strategies in respect of people, premises, technology, information, and relationships. This can be achieved through:

(i) Managing people's core skills and knowledge by:

a. Keeping documentation of working procedures for critical activities;

b. Multi-skill training of staff;

c. Use of third parties; and

d. Succession planning and retention;

(ii) Reducing the impact of unavailability of the primary site by:

a. Setting up alternative site within the location;

b. Arranging for alternative site to be provided by other institutions;

c. Arranging for alternative site to be provided by third party specialists;

d. Working from home or at remote sites.

(iii) Establishing technology strategies, which may include:

a. Replica of the technology at different locations that may not be affected by the same business disruption;

b. Holding older technology asset as fallback position; and

c. Additional risk mitigation for unique or long lead time equipment.

(iv) Establishing strategies to ensure information protection and recoverability according to the timeframes specified within the BIA, considering options such as hardcopies and electronic formats.

(v) Instituting strategies for supplies needed for critical operations, which may include:

a. Storage of additional supplies at another location;

b. Arrangement with suppliers for delivery of stock at short notice;

c. Identification of alternative/substitute supplies;

d. Increasing the number of suppliers;

e. Requiring suppliers to have validated business continuity capability;

f. Contractual/service level agreements with key suppliers.

(vi) Instituting strategies for managing relationships with key stakeholders, such as employees, regulators, auditors, development partners and media.

(vii) Obtaining adequate business continuity assurance on off-shore processing arrangements by:

a. Ensuring reliability of data transfer channels;

b. Keeping adequate documentation of the data processing facilities;

c. Getting into service level agreements for all outsourced elements of data processing;

d. Setting up reliable alternative recovery site preferably locally.

2.6 Recovery Objectives

Banks and financial institutions shall develop recovery objectives that reflect the risks they present to the operations of the financial system.

Recovery objectives provide banks and financial institutions with benchmarks for testing the effectiveness of their BCM. Establishment of recovery objectives involves specification of targets for the level of service and recovery times a bank or financial institution would seek to achieve at various stages during and after an operational disruption. The process needs to also factor in interdependency risks. Specifically, a bank or financial institution shall:

(i) Determine their service level targets and the corresponding recovery time objectives which are commensurate with the nature, scale and complexity of their business and the institutions' obligations to the market, customers and industry;

(ii) Specify in its BCM, appropriate time frames for implementing recovery objectives;

(iii) Provide an assessment of the risks they pose to the financial sector based on critical services they provide and their significance to the financial system; and

(iv) Ensure that recovery objectives are proportionate to the risk they pose to the financial system;

2.7 Business Continuity Plan

Every bank or financial institution shall develop and maintain a comprehensive business continuity plan (BCP) based on their business impact analysis, risk assessment and recovery objectives.

In developing BCP, a bank or financial institution shall ensure that:

(i) The plan is institution-wide and it is disseminated so that the relevant groups of personnel can implement it in a timely manner;

(ii) The business continuity plan addresses the staff requirements and relocation to the alternate site in the event of a major disruption;

(iii) The plan is documented and contains a minimum of the following key elements:

a. A business continuity plan awareness program;

b. a risk management program that includes clearly defined roles and responsibilities for resumption of business processes, including support organization functions;

c. procedures for mitigating interdependency risks between departments within the institution and with other institutions;

d. Trigger points and/or dates to activate the continuity plan;

e. Data back-up and recovery (hard copy and electronic);

f. Processes to deal with the loss of information that are not available from backup data;

g. Manual processes for continuing operations until technology is repaired;

h. Accessible recovery locations and emergency operations centers;

i. A process for automatically switching telephone and data lines;

j. Testing of the business continuity plans on an end-to-end basis;

k. A review process to ensure that the business continuity plan is feasible and up-to-date;

l. Specific incident/emergency management responses that identify assembly areas at a safe distance from the site of the incident;

m. Annual statement by Senior Management on whether the recovery strategies adopted are still valid and whether the documented BCPs are properly tested and maintained; and

n. Regulatory approval.

2.8 Testing, Maintenance and Audit

Every bank or financial institution shall test their business continuity for effectiveness and update on regular basis. An internal auditor or other independent party shall review the BCP to ensure that it is realistic, reliable, and relevant.

Testing is a vital element for implementing effective BCM. Testing is essential for identifying issues that were not apparent during the planning stage and promoting familiarity, awareness and understanding among staff. Testing programmes should therefore involve all personnel who are likely to be involved in responding to major operational disruptions. Furthermore, the testing programme should take into account the key element of human resource, ensuring that skills, knowledge, management and decision making ability is assessed. Changes in technology, business processes and staff roles and responsibilities can affect the appropriateness of the BCP, hence regular updates are necessary.

Banks and financial institutions shall take into account the following in respect of testing, maintenance and audit of their BCPs:

(i) A comprehensive program of testing, which may include desk check, walkthrough, simulation, functions and full plan;

(ii) The tests include measures for the quality of planning, competency of staff and effectiveness of the BCP;

(iii) Ensure that there is institutional awareness of emergency procedures and team members and employees are familiar with their roles, responsibilities and authority in response to an incident.

(iv) Ensure that all technological, logistical and administration aspects of the BCP have been tested;

(v) Ensure that the availability and relocation of staff is assessed;

(vi) Regularly test BCP to determine the ability to recover their operations as provided in their business continuity plans;

(vii) Ensure that test results, reports and resolution path are clearly documented and presented to the Board;

(viii) Ensure that all shortcomings identified in the test lead to the modification of the BCP.

(ix) The frequency of BCP testing shall be dependent upon the nature, size and complexity of an organization, but generally at least once a year;

(x) Define and document a BCM maintenance cycle;

(xi) Review and update BCM arrangements and activities e.g. BIA and RA to reflect all respective internal and external changes, that impact the institution in relation to BCM;

(xii) Review BCM documents e.g. BCM policy, strategies, BCPs to reflect changes in the Institution's business strategies, priorities, aims and objectives

(xiii) Arrange for independent verification of compliance with the institution's BCM policy, strategies, framework, plans, guidelines and standards adopted;

(xiv) Ensure that the audit/self assessment takes verifies / validates the institution's BCM arrangements, BCP, crisis management procedures and BCM exercising and maintenance practices; and

(xv) Ensure that the audit / self assessment ultimately highlights key deficiencies and issues in BCM.

2.9 Recovery Site

Every bank or financial institution shall establish a centre for recovery of data and operations.

The following aspects shall be taken into account:

(i) Office, data centre or server room recovery must not be in the same building or unreasonably close to the normal business operation;

(ii) Put in place an alternate recovery site sufficiently remote from the primary site for recovery and /or resumption of business operations;

(iii) Ensure that the alternate site has sufficient current data, equipment, systems and any other items necessary for recovery;

(iv) Recovery facilities must include all the necessary backup power generation and supply (generator, UPS and adequate fuel supply);

(v) Recovery solutions must be based on Business Impact Assessment (BIA);

(vi) In cases where organizations share disaster recovery site, there must be service level agreements between the parties;

(vii) In the circumstance that recovery sites are outsourced to a vendor or supplier, a signed contract must exist with service level agreements that support such arrangement;

(viii) If the alternate site is utilised for normal and recovery operations, a documented and tested plan must be in place to support such an arrangement.

2.10 Communication

Banks and financial institutions shall include in their business continuity plans comprehensive protocols and procedures for communicating within their institutions and with relevant external parties in the event of a major operational disruption. Such procedures should also provide for communication with financial authorities and institutions in other jurisdictions in the event of a major operational disruption with cross border implications.

Due to the increasing interdependency and interconnectedness among financial institutions within and across jurisdictions, a major operational disruption may extend beyond a bank's or financial institution's national borders and may consequently affect affiliated institutions in other jurisdictions and consequently impact the financial system of the home and other host countries. Therefore, the BCP should outline internal and external communication channels with regulators, investors, customers, counterparties, business partners, service providers, staff, the media and other stakeholders. Specifically, communication procedures for a bank or financial institution shall:

(i) Identify staff responsible for communicating with internal and external stakeholders. This may include senior management, public relations, legal advisors, and staff responsible for business continuity;

(ii) Provide for a communication protocol that include relevant contact lists for emergency management teams, local emergency response organizations, critical service providers and relevant domestic financial authorities;

(iii) Address obstacles that may arise due to failures in primary communications systems;

(iv) External communication to the media must only be through the external communication teams and approved by Senior Management or the Board.

(v) Provide a regular updating and testing of call tree and other contact information at least quarterly, and;

(vi) Ensure that copies of the BCP are disseminated to the relevant personnel.

Cross border communications protocols for institutions should:

(i) Take into account the implications of disruption of its business operations in one jurisdiction that significantly affect subsidiary, branch or correspondent operations in other jurisdictions;

(ii) Identify the circumstance under which it would contact the relevant non - domestic authorities;

(iii) Build relationships and identify contacts at the non domestic financial authority who might need to be informed of such disruptions;

(iv) Establish communication procedures for sharing information, views and assessments among authorities based in different jurisdictions and at different levels, and;

(v) Where applicable, have a memorandum of understanding with the relevant financial authorities in other jurisdictions on a shared understanding of the event that could have significant cross border effects on financial systems and agree on communication procedures.

2.11 BCM Awareness and Culture

Every bank or financial institution shall ensure that BCM is embedded in its organization culture and that all relevant personnel are aware of their business continuity roles.

Achievement of business continuity objectives requires imparting of business continuity awareness and culture to all individual members of the BCM teams, employees and other stakeholders. This requires among other things:

(i) Communicating BCM policy and plans throughout the organization;

(ii) Board's and Senior Management's demonstration of their support and commitment to the organisation's BCM policy and plans;

(iii) Setting up a formal BCM awareness and BCM training programmes for all employees;

(iv) Establishing a formal process of identifying and delivering BCM training requirements;

(v) Setting up a system of monitoring and evaluation of BCP implementation and maintenance; and

(vi) Providing clear definition of roles, accountability, responsibilities and authority within job descriptions at all levels of the organisation.

3.0 APPENDICES

Appendix 1: Definitions

Alternate Site	A site held for readiness for use during a Business Continuity event to maintain the business continuity of an organization. The term applies equally to office or technology requirements. Alternate sites may be cold, warm or hot. This type of site is also known as a Recovery Site.
Assembly Area	The designated area at which employees, visitors, and contractors assemble when evacuated from the primary site.
Backup	A process, by which data, electronic or paper based, is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted.
Business Impact Analysis (BIA)	The process of measuring the business impact or loss (quantitatively and qualitatively) to the institution in an outage. The BIA is useful in identifying the recovery priorities, recovery resources requirements, recovery strategies, and critical staff.
Business Continuity Management (BCM)	Refers to an institution-wide approach that include policies, standards and procedures for ensuring that specific provisions can be maintained or recovered in a timely fashion in the event of disruption. Its purpose is to minimize the operations, financial, legal, reputational and other material consequences arising from disruption.
Business Continuity Management Policy	A BCM policy sets out an organization's aim, principles and approach to BCM, what and how it will be delivered, key roles and responsibilities and how BCM will be governed and reported upon.
Business Continuity Management Program	An ongoing management and governance process supported by senior management and resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products/services through exercising, rehearsal, testing, training, maintenance and assurance.
Business Continuity Plan (BCP)	A comprehensive, written plan of action that sets out the procedures and establishes the processes and systems necessary to restore the orderly and expeditious operation of the institution in the event of disruptions to the operations of the institution.

Business Continuity strategy	Approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption.
Business Recovery	The rebuilding of specific business operations following a disruption to the level sufficient to meet outstanding business obligations.
Business Resumption	The condition of a function, following its recovery, when it is ready to take on tasks and activities to meet new business obligations.
Call Tree	A structured cascade process (system) that enables a list of persons, roles and/or organizations to be contacted as part of information or plan invocation procedure.
Crisis	An occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an organization.
Crisis Management	The process by which an organization manages the wider impact of a Business Continuity E/I/C until it is either ender control or contained without impact to the organization or the BCP is invoked as a part of the Crisis Management process.
Desktop exercise	A paper feedback scenario based method of testing plans, procedures and people.
Incident	An event that may be, or may lead to, a business interruption, disruption, loss and/or crisis.
Information Technology Disaster Recovery (ITDR)	An integral part of the organization's BCM plan by which it intends to recover and restore its IT and telecommunications capabilities after a BCM event.
Mission Critical Activities (MCA)	Critical operational and/or business support activities (either provided internally or outsourced) without which the institution would quickly be unable to achieve its objectives(s).
Recovery Objective	A pre-defined goal for recovering specified business operations and supporting systems to a specified level of service (recovery level) within a defined period following a disruption (recovery time).
Recovery Strategies	Defined, management-approved and tested course of action in response to operational disruptions.
Recovery Time (RTO)	Target duration of time to recover a specific business function. It comprises two components: (1) The duration

	of time from the point of disruption, to the point of declaring the activation of BCP, and (2) The duration of time from the activation of the BCP to the point when the specific business function is recovered. It is the acceptable duration of time that can elapse before the non-continuation of the specific business function would result in severe business impact and losses to the institution.
Recovery level	An element of recovery objective. It is the target level of service that will be provided in respect of a specific business operation after a disruption.
Recovery Point Objective (RPO)	A point in time to which data must be stored from backup storage for normal operations to resume if computer, system, or network goes down as a result of a disruption
Resilience	The ability of an organization, staff, system, network, activity or process to absorb the impact of a business interruption, disruption and/or loss and continue to provide a minimum acceptable level of service.
Scenario	A pre-defined set of Business Continuity E/I/C and conditions that describe an interruption, disruption or loss related to some aspect(s) of an organization's business for purposes of exercising a plan(s) and the people that would manage a business continuity E/I/C.
Single point of failure	A unique source of service, activity, and/or process where, there is no alternative and whose loss could lead to the failure of a critical function
Test Plan	A schedule of work designed to plan for testing a business continuity plan, people, systems and processes.

Appendix 2: Examples of Business Continuity Arrangements

(i) Use of fault-tolerant or duplicated hardware;

(ii) Adequate succession planning and staff orientation;

(iii) Arrangements for the cover and accessibility of key staff members;

(iv) Regular preventative maintenance of all computer and telecommunications components;

(v) On-site supplies of spare hardware and telecommunications components;

(vi) Internally generated or uninterrupted power supplies;

(vii) Fire detection and extinguishing systems;

(viii) Predetermined emergency responses;

(ix) Storage of important documents at both primary and secondary sites;

(x) Use of alternate processes and service providers;

(xi) Insurance coverage against foreseeable disruptions;

(xii) Developed procedures for the exchange of data by physical media (disks, tape, paper) in the event of telecommunications failure; and

(xiii) Capability to revert to old technology when new software, hardware or telecommunications component is implemented.