



**BUSINESS CONTINUITY MANAGEMENT GUIDELINES FOR  
BANKS AND FINANCIAL INSTITUTIONS, 2021**

**BANK OF TANZANIA**

- |                                       |  |
|---------------------------------------|--|
| Citation                              | 1. These guidelines shall be cited as “ <i>Business Continuity Management Guidelines for Banks and Financial Institutions, 2021</i> ”  |
| Authorization                         | 2. These guidelines are issued under Section 71 of the Banking and Financial Institutions Act, 2006.   |
| Application                           | 3. These guidelines shall apply to all banks and financial institutions.   |
| Objectives                            | <p>4. These guidelines aim at achieving the following objectives:</p> <ul style="list-style-type: none"> <li>(a) Define major elements and highlight the role of business continuity within a bank or financial institution;</li> <li>(b) Outline the duties of the Board, Senior Management, employees and the internal audit function with regard to business continuity;</li> <li>(c) Provide guidance to banks and financial institutions on how to develop an effective BCP given the scope and size of their operations;</li> <li>(d) Guide banks and financial institutions in making adequate preparations to deal with possible business interruption scenarios; and</li> <li>(e) Provide guidance to banks and financial institutions on how to evaluate the adequacy of their BCPs.</li> </ul>  |
| Business Continuity Management Policy | <p>5. Every bank or financial institution shall establish a BCM policy to govern formulation and maintenance of all aspects of business continuity. The policy shall be approved by the Board and shall be communicated to all relevant levels of the institution in a timely manner. At minimum the policy shall include:</p> <ul style="list-style-type: none"> <li>(a) business continuity objectives, plans, scope, limitations and exclusion;</li> <li>(b) reporting arrangement for any significant deviation from the policy to Senior Management/Board for corrective measures;</li> <li>(c) formation of various BCM teams and description of their roles such as BCM Steering Committee, Business Continuity Management Team, Crisis Management Team and Business Recovery Team;</li> <li>(d) provision for policy reviews at regular intervals and when significant changes occur; and</li> <li>(e) definition of roles and responsibilities of all parties who may be involved.</li> </ul> |

- Major Duties and Responsibilities
6. Banks and financial institutions shall have effective and comprehensive approaches to Business Continuity Management. Board of Directors and Senior Management are responsible for the bank's or financial institution's business continuity. Additionally, Internal Audit and all employees of an organization have a role in business continuity management.
- Board of Directors Responsibilities
7. The responsibility for business continuity management of a bank or financial institution ultimately lies with the Board of Directors. Specific responsibilities of the Board include:
- (a) approving business continuity management policy, strategy, plans, standards and principles developed by Senior Management;
  - (b) allocating sufficient human and financial resources for the development and maintenance of the BCP; and
  - (c) ensuring compliance with legal and regulatory requirements for Business Continuity Management.
- Senior Management Responsibilities
8. Senior management shall be responsible for:
- (a) preparing policies by determining how the institution will manage and control business continuity risks;
  - (b) developing BCPs and strategies necessary for the continuity of critical business functions;
  - (c) ensuring that the necessary administrative support functions in the recovery effort, such as human resources, insurance, legal and security are in place;
  - (d) ensuring that all levels of staff are cognizant of the importance of BCPs and the business recovery objectives;
  - (e) formation and assigning the overall management of the business continuity function to a Business Continuity Management Team;
  - (f) 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;
  - (g) reviewing BCP test results on regular basis;
  - (h) keeping the BCP up to date and reviewing it at least annually;
  - (i) ensuring that employees are trained and are fully aware of their roles in the implementation of BCM;
  - (j) ensuring that there is a framework for reporting to the Board and Senior Management on matters related to BCM;

- (k) ensuring that, at least annually, the bank's or financial institution's BCM is subject to review by an independent party, such as internal or external auditor;
- (l) ensuring that roles as well as responsibilities and authority to act, and succession plans are clearly articulated in the bank's or financial institutions' BCM policies to avoid confusion in the event of a disruption;
- (m) ensuring that the BCP not only considers business processes and technical aspects, but also recognizes and addresses the human element. The overriding consideration in formulating a bank or financial institution's BCP should be the preservation of human life; and
- (n) 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.

Employee  
Responsibilities

9. Each employee of a bank or financial institution shall 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.

Internal Audit  
Responsibilities

10. The internal audit function of a bank or financial institution shall 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.

Outsourced  
Business  
Continuity  
Management  
Function

11. A bank or financial institution may opt to outsource some of the BCM functions. The bank or financial institution shall take regard of the requirements of Outsourcing Guidelines for Banks and Financial Institutions issued by the Bank. Nevertheless, the following shall be observed:
- (a) Accountability for BCM ultimately rests with the Board of Directors of a bank or financial institution;
  - (b) In cases where recovery sites are outsourced from vendors or suppliers, a signed contract must exist with service level agreement that supports such an arrangement;
  - (c) In cases where institutions share disaster recovery site, there must be service level agreements in place that clearly outline the terms that govern these arrangements between the parties; and
  - (d) 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.

Business  
Continuity  
Management  
Team

12. (1) A bank or financial institution shall constitute a BCM Team for the purpose of the overall management of business continuity. Such Team shall draw its membership from the following:
  - (i) Senior Management (Coordinator)
  - (ii) Functional Departmental Heads
  - (iii) Line Managers
  - (iv) Risk Management Officer.
- (2) Major roles and responsibilities of the Team shall include the following:
  - (a) 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:
    - (i) Strategic stage – examine the organizational framework taking note of the key stakeholders, legislative and regulatory requirements in relation to business continuity;
    - (ii) Process stage – develop resumption strategies for business processes and activities;
    - (iii) Resource Recovery – ensure the deployment of appropriate resources to all business processes and activities;
  - (iv) Awareness and Education – develop a business continuity culture through assessment of business continuity awareness campaigns; and
  - (v) Testing, Maintenance, Measurement and Audit – ensure reliability of the business continuity plan through independent review and testing.
  - (b) 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;
  - (c) To ensure that the business continuity plan is updated to reflect the changes in the risk profile of the bank or financial institution;
  - (d) Report on the status of business continuity management to the Board and Senior Management on a regular basis, highlighting where gaps are identified;

- (e) To facilitate testing of plans to ensure that team members are aware of their roles and responsibilities in the event of a disruption; and
- (f) To ensure that the institution's response to a disruption is communicated internally and externally to applicable parties.

Business Impact Analysis (BIA)

13. (1) 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.

(2) 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:

- (a) 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;
- (b) Estimate the maximum allowable down time and acceptable levels of data, operations and financial losses;
- (c) identify, those business functions and operations to be recovered on a priority basis;
- (d) 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:
  - (i) Staff numbers and key skills
  - (ii) Data application and systems
  - (iii) Constraints
  - (iv) Mission Critical Activities (MCA) or tasks that need to be recorded to ensure continuity of the process and business
  - (v) Dependencies on people, systems, processes, internal and external parties
  - (vi) Recovery Time Objectives (RTO) and Recovery Point Objective (RPO) for every Mission Critical Activity (MCA)
  - (vii) Systems impact assessment highlighting:
    - location;

- department unit owners, system information, commissioning dates;
  - technical person responsible;
  - RTO and RPO and dependencies.
- (viii) Provide a list of recovery option for each business process; and
- (e) Review BIA at least once a year.

- Risk Assessment 14. 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:
- (a) Identify unacceptable concentrations of risk and what are known as ‘single point of failure’
  - (b) Identify internal and external threats that could cause a disruption and assess their probability and impact;
  - (c) Prioritize threats;
  - (d) Provide information for a risk control management strategy and an action plan for risks to be addressed;
  - (e) Mitigation of risks through a documented remedial plan;
  - (f) Ensure BCPs are updated regularly to reflect the changes in the institution’s operational risk profile; and
  - (g) Specify events that should prompt implementation of the plans.

- Business Continuity Strategies 15. (1) 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.
- (2) A bank or financial institution shall set up and maintain appropriate strategies in respect of people, premises, technology, information, and relationships. This can be achieved through:
- (a) Managing people’s core skills and knowledge by:
    - (i) Keeping documentation of working procedures for critical activities;
    - (ii) Multi-skill training of staff;
    - (iii) Use of third parties; and
    - (iv) Succession planning and retention;

- (b) Reducing the impact of unavailability of the primary site by:
  - (i) Setting up alternative site within the location;
  - (ii) Arranging for alternative site to be provided by other institutions;
  - (iii) Arranging for alternative site to be provided by third party specialists;
  - (iv) Working from home or at remote sites.
- (c) Establishing technology strategies, which may include:
  - (i) Replica of the technology at different locations that may not be affected by the same business disruption;
  - (ii) Holding older technology asset as fallback position; and
  - (iii) Additional risk mitigation for unique or long lead time equipment.
- (d) Establishing strategies to ensure information protection and recoverability according to the timeframes specified within the BIA, considering options such as hardcopies and electronic formats.
- (e) Instituting strategies for supplies needed for critical operations, which may include:
  - (i) Storage of additional supplies at another location;
  - (ii) Arrangement with suppliers for delivery of stock at short notice;
  - (iii) Identification of alternative/substitute supplies;
  - (iv) Increasing the number of suppliers;
  - (v) Requiring suppliers to have validated business continuity capability;
  - (vi) Contractual/service level agreements with key suppliers.
- (f) Instituting strategies for managing relationships with key stakeholders, such as employees, regulators, auditors, development partners and media.
- (g) Obtaining adequate business continuity assurance on off-shore processing arrangements by:
  - (i) Ensuring reliability of data transfer channels;
  - (ii) Keeping adequate documentation of the data processing facilities;
  - (iii) Getting into service level agreements for all outsourced elements of data processing; and
  - (iv) Setting up reliable alternative recovery site preferably locally.

Recovery Objectives

16. (1) Banks and financial institutions shall develop recovery objectives that reflect the risks they present to the operations of the financial system.
- (2) 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:

- (a) 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;
- (b) Specify in its BCM, appropriate time frames for implementing recovery objectives;
- (c) 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
- (d) Ensure that recovery objectives are proportionate to the risk they pose to the financial system.

Business  
Continuity Plan

17. 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:

- (a) The plan is institution-wide and it is disseminated so that the relevant groups of personnel can implement it in a timely manner;
- (b) The business continuity plan addresses the staff requirements and relocation to the alternate site in the event of a major disruption;
- (c) The plan is documented and contains at minimum the following key elements:
  - (i) a risk management program that includes clearly defined roles and responsibilities for resumption of business processes, including support organization functions;
  - (ii) procedures for mitigating interdependency risks between departments within the bank or financial institution and with other institutions;
  - (iii) Trigger points and/or incidences to activate the continuity plan;
  - (iv) Data back-up and recovery (hard copy and electronic);
  - (v) Processes to deal with the loss of information that are not available from backup data;
  - (vi) Manual processes for continuing operations until technology is repaired;
  - (vii) Accessible recovery locations and emergency operations centers;

- (viii) A process for automatically switching telephone and data lines;
- (ix) Testing of the business continuity plans on an end-to end basis;
- (x) A review process to ensure that the business continuity plan is feasible and up-to-date;
- (xi) Specific incident/emergency management responses that identify assembly areas at a safe distance from the site of the incident;
- (xii) Annual statement by Senior Management on whether the recovery strategies adopted are still valid and whether the documented BCPs are properly tested and maintained;
- (xiii) A business continuity plan awareness program; and
- (xiv) Regulatory approval.

Testing,  
Maintenance and  
Audit

18. 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. In that regard:

- (a) Every bank or financial institution shall test its business continuity plan for effectiveness and update its BCM on regular basis.
- (b) 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
  - (xii) respective internal and external changes, that impact the institution in relation to BCM;
  - (xiii) Review BCM documents e.g. BCM policy, strategies, BCPs to reflect changes in the bank's or financial institution's business strategies, priorities, aims and objectives;
  - (xiv) Arrange for independent verification of compliance with the institution's BCM policy, strategies, framework, plans, guidelines and standards adopted;
  - (xv) Ensure that the audit/self-assessment verifies / validates the bank's or financial institution's BCM arrangements, BCP, crisis management procedures and BCM exercising and maintenance practices; and
  - (xvi) Ensure that the audit / self-assessment ultimately highlights key deficiencies and issues in BCM.
- (c) The internal auditor or other independent party shall review the BCP to ensure that it is realistic, reliable, and relevant.

Recovery Site

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

The following aspects shall be taken into account:

- (a) Office, data centre or server room recovery must not be in the same building or unreasonably close to the normal business operation;
- (b) Put in place an alternate recovery site sufficiently remote from the primary site for recovery and /or resumption of business operations;
- (c) Ensure that the alternate site has sufficient current data, equipment, systems and any other items necessary for recovery;

- (d) Recovery facilities must include all the necessary backup power generation and supply (generator, UPS and adequate fuel supply);
- (e) Recovery solutions must be based on Business Impact Assessment (BIA);
- (f) In cases where organizations share disaster recovery site, there must be service level agreements between the parties;
- (g) 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.

Data Centre

20. (1) Every bank or financial institution shall establish its primary data center in Tanzania.
- (2) Every bank or financial institution shall build capacity of its Information and Communication Technology (ICT) personnel to be able to run its data center independently.
- (3) A banks or financial institution may outsource activities related to data center operations within the country, provided they comply with outsourcing requirements stipulated under outsourcing guidelines issued by the Bank.

Communication

21. (1) 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.
- (2) 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.
- (3) 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:

- (a) 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;
  - (b) 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;
  - (c) Address obstacles that may arise due to failures in primary communications systems;
  - (d) External communication to the media must only be through the external communication teams and approved by Senior Management or the Board;
  - (e) Ensure that the directory or contact lists are made available to all team members;
  - (f) Provide a regular updating and testing of call tree and other contact information at least quarterly, and;
  - (g) Ensure that copies of the BCP are disseminated to the relevant personnel.
- (4) Cross border communications protocols for banks and financial institutions shall:
- (a) 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;
  - (b) Identify the circumstance under which it would contact the relevant non-domestic authorities;
  - (c) Build relationships and identify contacts at the non-domestic financial authority;
  - (d) Identify who might need to be informed of such disruptions;
  - (e) Establish communication procedures for sharing information, views and assessments among authorities based in different jurisdictions and at different levels; and
  - (f) 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.

BCM Awareness  
and Culture

22. 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:

- (a) Communicating BCM policy and plans throughout the organization;
- (b) Board's and Senior Management's demonstration of their support and commitment to the organisation's BCM policy and plans;
- (c) Setting up a formal BCM awareness and BCM training programmes for all employees;
- (d) Establishing a formal process of identifying and delivering BCM training requirements;
- (e) Setting up a system of monitoring and evaluation of BCP implementation and maintenance; and
- (f) Providing clear definition of roles, accountability, responsibilities and authority within job descriptions at all levels of the organization.

Administrative  
Sanctions and  
Penalties

23. Without prejudice to other penalties and actions prescribed by the Act, the Bank may impose one or more of the following sanctions where any of the provisions herein are contravened: -

- (a) civil money penalty on the banking institution or directors, officers or employees responsible for non-compliance in such amounts as may be determined by the Bank;
- (b) suspension of access to the credit facilities of the Bank;
- (c) suspension of lending and investment operations;
- (d) suspension of capital expenditure;
- (e) suspension of the privilege to accept new deposits;
- (f) suspension from office of the defaulting director, officer or employee; and
- (g) disqualification from holding any position or office in any banking institution in Tanzania; and revocation of banking license.

## **APPENDICES    Appendix 1: Definitions**

<i>Alternate Site</i>	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.
<i>Assembly Area</i>	The designated area at which employees, visitors, and contractors assemble when evacuated from the primary site.
<i>Backup</i>	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.
<i>Business Impact Analysis (BIA)</i>	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.
<i>Business Continuity Management (BCM)</i>	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.
<i>Business Continuity Management Policy</i>	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.
<i>Business Continuity Management Program</i>	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.
<i>Business Continuity Plan (BCP)</i>	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.
<i>Business Continuity strategy</i>	Approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption.

<i>Business Recovery</i>	The rebuilding of specific business operations following a disruption to the level sufficient to meet outstanding business obligations.
<i>Business Resumption</i>	The condition of a function, following its recovery, when it is ready to take on tasks and activities to meet new business obligations.
<i>Call Tree</i>	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.
<i>Crisis</i>	An occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an organization.
<i>Crisis Management</i>	The process by which an organization manages the wider impact of a Business Continuity E/I/C until it is either under control or contained without impact to the organization or the BCP is invoked as a part of the Crisis Management process.
<i>Desktop exercise</i>	A paper feedback scenario based method of testing plans, procedures and people.
<i>Financial authority</i>	A financial sector regulatory or supervisory organization having some level of responsibility for safeguarding and maintaining public confidence in the financial system.
<i>Incident</i>	An event that may be, or may lead to, a business interruption, disruption, loss and/or crisis.
<i>Information Technology Disaster Recovery (ITDR)</i>	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.
<i>Mission Critical Activities (MCA)</i>	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).
<i>Recovery Objective</i>	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).
<i>Recovery Strategies</i>	Defined, management-approved and tested course of action in response to operational disruptions.

<i>Recovery Time (RTO)</i>	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.
<i>Recovery level</i>	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.
<i>Recovery Point Objective (RPO)</i>	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
<i>Resilience</i>	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.
<i>Scenario</i>	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.
<i>Single point of failure</i>	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
<i>Test Plan</i>	A schedule of work designed to plan for testing a business continuity plan, people, systems and processes.

## **Appendix 2:**

Examples of Business Continuity Arrangements	<ul style="list-style-type: none"> <li>(a) Use of fault-tolerant or duplicated hardware;</li> <li>(b) Adequate succession planning and staff orientation;</li> <li>(c) Arrangements for the cover and accessibility of key staff members;</li> <li>(d) Regular preventative maintenance of all computer and telecommunications components;</li> <li>(e) On-site supplies of spare hardware and telecommunications components;</li> <li>(f) Internally generated or uninterrupted power supplies;</li> <li>(g) Fire detection and extinguishing systems;</li> </ul>
--	--

- (h) Predetermined emergency responses;
- (i) Storage of important documents at both primary and secondary sites;
- (j) Use of alternate processes and service providers;
- (k) Insurance coverage against foreseeable disruptions;
- (l) Developed procedures for the exchange of data by physical media (disks, tape, paper) in the event of telecommunications failure; and
- (m) Capability to revert to old technology when new software, hardware or telecommunications component is implemented.

Dar Es Salaam,  
17<sup>th</sup> June 2021

**FLORENS D. A. M. LUOGA**  
Governor