

GUIDELINE ON BUSINESS CONTINUITY MANAGEMENT CBK/PG/14

PART I: Preliminary

- 1.1 Title
- 1.2 Authorization
- 1.3 Application
- 1.4 Definitions

PART II: Statement of Policy

- 2.1 Purpose
- 2.2 Scope
- 2.3 Responsibility

PART III: Specific Requirements

- 3.1 Boards and Senior Management
- 3.2 Business Continuity Management Team

PART IV: Remedial Measures

- 4.1 Remedial Measures

PART V: Effective Date

- 5.1 Effective Date
- 5.2 Supersedence

PART I: PRELIMINARY

- 1.1 Title** – Guideline on Business Continuity Management (BCM).
- 1.2 Authorization** – This Guideline is issued under Section 33(4) of the Banking Act, which empowers the Central Bank of Kenya to issue guidelines to be adhered to by institutions in order to maintain a stable and efficient banking system.
- 1.3 Application** – This Guideline applies to all institutions licensed under the Banking Act (Cap. 488) and Non-Operating Holding Companies.
- 1.4 Definitions** – The terms used in this Guideline shall be taken to have the meaning as assigned to them hereunder. Other terms used in the guidelines are as defined in the Banking Act.
- 1.4.1 ‘Alternate Site’** means a site held in readiness for use in the event of a major disruption that maintains an institution’s business continuity.
- 1.4.2 ‘Business Continuity’** is a state of continued, uninterrupted operation of a business.
- 1.4.3 ‘Business Continuity Management’** is a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations 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.
- 1.4.4 ‘Business Continuity Plan’** means a comprehensive, documented plan of action that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an institution in the event of a disruption.
- 1.4.5 ‘Business Impact Analysis’** means the process of identifying and measuring (quantitatively and qualitatively) the business impact loss of business processes in the event of a disruption. It is used to identify recovery priorities, recovery resource requirements and essential staff and to help shape the business continuity plan. All impacts should be measured on financial, regulatory, legal and reputational damage basis.

- 1.4.6 ‘Call Tree’** means a system that enables a list of person/roles organizations to be contacted as part of an information/communication plan.
- 1.4.7 ‘Communication Protocols’** means an established procedure for communication that is agreed in advance between two or more parties internal or external to an institution. Such procedure also includes the nature of the information that should be shared with internal and external parties and how certain types of information should be shared with internal and external parties.
- 1.4.8 ‘Critical Services’** means any activity, function, process or service, the loss of which would be material to the continued operation of an institution.
- 1.4.9 ‘Crisis’** an event, occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an institution.
- 1.4.10 ‘Crisis Management Team’** means a team consisting of key executives, key role players (i.e. legal counsel, facilities manager, disaster recovery coordinator), and the appropriate business owners of critical functions who are responsible for recovery operations during a crisis. Evaluation of capability, training, testing of Crisis Management teams maturity level must be documented.
- 1.4.11 ‘Cyber Incident’** is any malicious act or suspicious event that: compromises, or attempts to compromise, the electronic security perimeter or physical security perimeter of a critical Cyber Asset or disrupts or attempts to disrupt, the operation of a critical Cyber Asset.
- 1.4.12 ‘Disaster’** means a sudden, unplanned catastrophic event that compromises an institution’s ability to provide critical functions, processes, or services for some unacceptable period of time, causing unacceptable damage or loss.
- 1.4.13 ‘Emergency Response Team’** means any organization that is responsible for responding to hazards to the general population (e.g. fire brigades, police services, hospitals)
- 1.4.14 ‘Exercising’** means the process through which business continuity plans are tested, rehearsed in a controlled environment using team members and staff.

- 1.4.15 ‘Major operational disruption’** means high impact disruption of normal business operations, affecting a large geographic area and adjacent communities that are economically integrated to it.
- 1.4.16 ‘Operational Risk’** means the risk of loss from inadequate or failed internal processes, people and systems or from external events.
- 1.4.17 ‘Recovery’** means the rebuilding of a specific business operation following a disruption to a level sufficient to meet outstanding business obligations.
- 1.4.18 ‘Recovery Objective’** means a predefined goal for recovering specific business operations and supporting systems to a specified level of service (recovery level) within a defined period following a disruption. (recovery time).
- 1.4.19 ‘Recovery Time’ (RT)** means the duration of time required to resume a specified business operation. It has two components, the duration of time from activation of the business continuity plan and the recovery of business operations.
- 1.4.20 ‘Recovery Point Objective’ (RPO)** describes a point in time to which data, must be restored from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a disruption.
- 1.4.21 ‘Resilience’** means the ability of an institution, network, activity, process or financial system to absorb the impact of a major operational disruption and continues to maintain critical operations or services.
- 1.4.22 ‘Risk Assessment’** means the probability and impact of specific threats being realized.
- 1.4.23 ‘Single point of failure’** unique source of a service, activity, and/or process where there is no alternative and whose loss could lead to the failure of a critical function.

PART II: STATEMENT OF POLICY

2.1 Purpose

This Guideline outlines the minimum requirements that institutions should implement to ensure that business operations are not adversely affected in the event of a disruption. It is envisaged that by implementing this Guideline, institutions will both reduce the likelihood and impact of operational disruption and ensure business continuity in order to maintain public trust and confidence in the financial system.

2.2 Scope

This Guideline sets the minimum requirements for establishing sound and effective business continuity management practices by institutions.

2.3 Responsibility

The responsibility for business continuity management ultimately rests with the board of directors and the senior management of an institution. They are expected to formulate business continuity policy, procedures, guidelines and set minimum standards for an institution. All of these must be documented and available for review by an external auditor and the Central Bank of Kenya.

PART III SPECIFIC REQUIREMENTS

3.1 Board of Directors and Senior Management

3.1.1 Major duties and responsibilities.

An institution's board and senior management are responsible for the development, implementation and maintenance of policies that ensure the resilience and continuity of an institution, in the event of major operational disruptions. The board fulfills its business continuity planning responsibilities by setting policy, prioritizing critical business functions, allocating sufficient resources and personnel, providing oversight, approving the Business Continuity Plan (BCP), reviewing test results and ensuring maintenance of the current plan. These responsibilities include but are not limited to the following: -

3.1.1.1 Ensure that business continuity planning forms an integral part of the overall risk management of an institution and that business continuity processes are documented and embedded in an organization's operations.

The board of directors and senior management are required to:

- a) Ensure a documented Policy on BCM is put in place.
- b) Define the roles, responsibilities and authority to act in the event of a major disruption, namely:
 - i. At the organizational level, overall management of the business continuity function on a day-to-day basis should be assigned to a Business Continuity Management Team. The selection of the Team should be contingent upon the nature of business activities, size, complexity, and geographical location of an institution.

The basic composition of the Business Continuity Management Team should at a minimum constitute the following:

- Co-coordinator (drawn from the senior management).
 - Functional Department Heads.
 - Line Managers.
 - Risk Management Officer.
- ii. In the event that an institution opts to outsource the business continuity function, it should ensure that accountability for business continuity management ultimately rests with the board of directors and senior management.
- iii. In cases where institutions share a disaster recovery site, there must be service level agreements in place that clearly outline the terms that govern these arrangements between the parties.
- iv. In cases where recovery sites are outsourced to a vendor or supplier, a signed contract must exist with service level agreements that support such an arrangement.

- v. In outsourced solutions that are syndicated, care must be taken not to syndicate services between banks where they have normal business functions close or adjacent to each other i.e. a bank back-office operation in Nairobi which is next to or a few blocks away from another bank and uses the same vendor should not have syndicated solutions utilizing the same syndicated infrastructure. For the above, dedicated options should be taken to ensure recovery in the event of a city-wide incident.
 - vi. Office, data centre or server room recovery must not be in the same building or close to the normal business operation.
 - vii. Distance from the normal business and recovery facility will depend on individual needs but it is proposed that if a bank has its head office or back office function within the city limits, they should have their recovery facilities outside of the city centre. If the recovery site is within the city centre then the head office or back-office function should be located outside the city limits. Care should be taken to look at other factors such as a second power grid and telecommunications infrastructure i.e. a power outage of normal business functions should not be able to affect the recovery facility.
 - viii. Recovery facilities must include all the necessary backup power generation and supply (Generator, UPS and adequate fuel supply).
 - ix. Utilization of alternate sites for recovery within the same organization must be at an adequate distance from the operation based on above criteria. If the alternate site is utilized for normal recovery operations a documented and tested plan must be in place to support such an arrangement.
 - x. Recovery solutions must be based on Business Impact Assessment (BIA) information.
 - xi. Documented pre and post-test reports are to be completed for all recovery testing.
- c) Ensure that employees are trained and made aware of their roles in the implementation of the Business Continuity Plan.

- d) Ensure that sufficient human and financial resources are made available to provide support for Business Continuity Management.
- e) Ensure that the business continuity plans not only consider the business process and technical aspects, but also recognize and address the human element. The overriding consideration in formulating an institution's business continuity plan should be for the preservation of human life.

3.1.1.2 Establish a framework for crisis management.

Establish a Crisis Management Team, consisting of key executives and functional heads of critical operational areas who will be responsible for dealing with crisis management and business continuity during a crisis. This will require the institution to re-prioritize and re-allocate resources in order to expedite recovery. The roles and responsibilities of each individual member/team should be clearly defined. Institutions must take into account all relevant potential scenarios that could result in a crisis for the bank. The term crisis denotes a threatening situation that calls for critical decisions and cannot be handled with or with ordinary management tools and decision-making powers.

The following are examples of crisis management situations:

- Accident like events such as fires or explosions.
- Terrorist attacks and sabotage.
- Natural disasters such as floods and earthquakes.
- Mass absence of personnel due to a pandemic.
- Failure of building technology or energy supply.
- Failure of external suppliers (outsourcing) such as information providers.
- Failure of communication systems or Telecommunication providers.
- Failure of IT systems or infrastructure hardware or software.
- Cyber-security incidences.

Crisis management recommended best practice at a minimum includes:

- A detailed crisis management plan should be in place.
- The crisis management plan contains instructions on how to respond in event of casualties and fatalities. The plan should stipulate that priority is to attend to casualties and fatalities.

- Adjustments to crisis management plan should be made when threats change significantly.
- The senior management team knows who is in the crisis management team and has approved their selection.
- The senior management team understands the crisis management teams terms of reference.
- The crisis management team is responsible for managing all critical internal issues to resolution.
- The core crisis management team may be supplemented by preselected and trained specialists according to incident type scale and severity.
- At least 70 percent of the crisis management team should have been involved in tests and crisis management incidents in the preceding 12 months.
- Once activated the crisis management team has full authority for all decisions including powers to spend during the crisis.
- The primary command centre to support the crisis management team should be fully equipped with necessary facilities e.g. telephones, computers and printers.
- If the command centre is inaccessible the crisis management team may be accommodated in an alternative primary or secondary location.

3.1.1.3 Establish a framework for review and monitoring by the Board of Directors and Senior Management.

- a) Business Continuity Plans should be reviewed and approved by the Board of Directors on an annual basis. Some information such as contact details should be reviewed on a monthly or quarterly basis.

However, certain events may trigger the need for an immediate review of the BCP.

These include significant changes in the following:

- i. Business strategy and risk appetite of an institution.
- ii. Restructuring of an institution, either through expansion or through a merger or acquisition.
- iii. Key technology and telecommunications.
- iv. Service providers.
- v. Regulatory and legislative requirements.

vi. Composition and size of staff.

- b) An institution's business continuity plan should be subject to an independent review at least annually and the findings reported to the board of directors in a timely manner. This is conducted through assurance and business continuity management audits at a predetermined frequency.

3.1.1.4 Ensure compliance with all Prudential Guidelines and all other regulatory and legal requirements related to Business Continuity Management

An institution should comply with the Banking Act, Prudential Guidelines and all other applicable laws and regulations which fall under jurisdiction of other regulatory authorities.

3.2 Business Continuity Management Team

The major roles and responsibilities of the Business Continuity Management Team should be as follows:

3.2.1 To develop and approve a business continuity management process and plan.

An institution's business continuity plan should be developed along the following five levels which reflect the business continuity management life cycle:

- i. Strategic level; Examine the organizational framework taking note of the key business stakeholders, legislative and regulatory requirements in relation to business continuity.
- ii. Process level; - Develop resumption strategies for business processes and activities.
- iii. Resource Recovery; Ensure the deployment of appropriate resources to ensure appropriate continuity across all business processes and activities.
- iv. Awareness and Education; develop a business continuity culture through assessment of business continuity awareness campaigns. Ensure that the BCM Management Team is trained and that appropriate skills are in place.

- v. Testing, Maintenance, Measurement and Audit; Ensure reliability of the business continuity plan of an organization through independent review and testing.

3.2.2 Ensure that the Business Continuity Plan (BCP) is updated to reflect the changes in an institution's risk profile.

The Business Continuity Management Team should ensure that the (BCP) business continuity plan is reviewed annually, though the frequency may be modified to take into account changes in the business strategy, business processes, personnel, location or technology and changes in the external business environment.

3.2.3 Ensure the implementation of the business continuity plan by periodically conducting a business impact analysis, (at least once a year) an enterprise – wide risk assessment, risk management and risk monitoring to identify the mission critical activities and potential for major disruptions.

Business Impact Analysis (BIA's) must be signed off by department or functional heads through a formal functional process stipulating that they understand, accept and verify BIA's are correct.

3.2.3.1 Business Impact Analysis (BIA)

Major operational disruptions pose a substantial risk to the continued operation of an institution. The extent to which an institution incorporates the risk of a major operational disruption in its business continuity plan is dependent upon its risk profile.

Business impact analysis forms the foundation upon which the business continuity plan 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 the urgent functions upon which a risk assessment should be focused. At a minimum, a business impact analysis is expected to;

- i. Provide an understanding of an institution's most critical objectives, the priority, and the timeframes for resumption of each (recovery objective and recovery time).

- ii. Provide information about resource requirements over time to enable each business function within the organization to achieve continuity or resumption of activity within the established timeframes. It should at a minimum identify;
 - a. Staff numbers and key skills.
 - b. Data applications and systems.
 - c. Facilities including alternative location needs, backup strategy policy and schedule.
 - d. Vendors/suppliers of various services.
 - e. Constraints.
 - f. Mission Critical Activities (MCA's) or tasks that need to be recorded to ensure continuity of the process and business.
 - g. Dependencies on people, systems, processes, internal and external parties.
 - h. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for every MCA or business.
 - i. Systems impact assessment.
 - j. Location.
 - k. Department unit owners, system information, commissioning dates.
 - l. Technical person responsible.
 - m. RTO, RPO and dependences.
- iii. Provide a list of recovery options for each business process.
- iv. Methods and techniques

A combination of the following methods and techniques may be used to carry out Business Impact Analysis:

- Questionnaires.
- Interviews.
- Workshops.

Generally, a combination of all the above methods should provide an adequate source of information from which to base the Business Continuity Plan. All relevant information should be stored for reference for at least one year or until the next BIA.

3.2.3.2 Risk Assessment

A risk assessment examines the most urgent business functions identified during business impact analysis. It looks at the probability and impact of a variety of specific threats that could cause a business disruption.

A risk assessment is at a minimum expected to achieve the following:

- i. Identify unacceptable concentrations of risk and what are known as ‘single points of failure’.
- ii. Identify internal and external threats that could cause 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 remediation plan.

3.2.3.3 Methods and Techniques

The methods and techniques to be used to provide a risk assessment may include:

- a. Insurance statistics.
- b. Published disaster frequency statistics.
- c. Scoring systems for impact and probability.
- d. Gap analysis.
- e. Stress testing.

3.2.3.4 Recovery objectives

Institutions should develop recovery objectives that reflect the risk they represent to the operation of the financial system. Institutions should factor in interdependency risks when developing their recovery objectives. Consequently, institution’s business continuity management team should:

- a) Make an assessment of the risks they pose to the financial sector based on critical services they provide and their significance to the financial system.
- b) Identify those business functions and operations to be recovered on a priority basis and establish recovery objectives.

- c) Establish recovery objectives proportional to the risk they pose to the financial system.

When evaluating whether an institution's business continuity plan can accommodate major operational disruptions, an institution should review the adequacy of recovery arrangements in areas such as:

- i. The alternate site should be geographically distant from the main branch of an institution. The site should have alternate power supplies (e.g. alternate power grid, uninterruptible power source, back-up generators).
- ii. The alternate site should be equipped with the necessary equipment and data to maintain critical operations and services. An inventory of assets (backup tapes, communication links, operating systems, hardware) needed for offsite recovery should be generated.
- iii. The business continuity plan should address staff requirements and reallocation to the alternate site in the event of a major disruption. A detailed list of tasks for offsite recovery should be made available to all concerned staff.
- iv. The use of third parties to support the delivery of their critical business services. These arrangements could increase operational risks arising from the failure, delay, or compromise of a third party in providing the service. As such, the Institution should put in place measures that enable third parties to meet the recovery time objectives (RTOs) of its critical business services.

This can be done through among others, the following:

- Establish and regularly review operational level or service level agreements with third parties that set out specific and measurable recovery expectations and support the financial institution's (FI's) BCM.
- Review the BCPs of third parties and verify that the BCPs meet appropriate standards and are regularly tested.
- Establish arrangements with third parties to safeguard the availability of resources, such as requesting for dedicated manpower.
- Conduct audits on the third parties.
- Perform joint tests with third parties.

Financial institutions should also put in place plans and procedures to address any unforeseen disruption, failure or termination of third-party arrangements to minimize the impact of such adverse events on the continuity of critical business services.

3.2.4 IT Disaster Recovery and Cyber Resilience

Financial institutions should implement a robust information and communication technology (ICT) framework (including cyber security) within their operational risk management framework and operational resilience approach.

Institutions should establish appropriate policies and processes to identify, assess, mitigate, monitor and manage ICT risks. These policies and processes also require the board to regularly oversee the effectiveness of the bank's ICT risk management and senior management to routinely evaluate the design, implementation and effectiveness of the bank's ICT risk management.

Institutions should have resilient ICT that is subject to protection, detection, response and recovery processes that are regularly tested, incorporate appropriate situational awareness of vulnerability and convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of the bank's critical operations.

Institutions should identify their critical information assets and the infrastructure upon which they depend. Institutions should also prioritise their cyber security efforts based on their ICT risk assessment and on the significance of the critical information assets to the bank's critical operations, while observing all pertinent legal and regulatory requirements relating to data protection and confidentiality.

Institutions should develop plans and implement controls to maintain the integrity of critical information in the event of a cyber event, such as secure storage and offline backup on immutable media of data supporting critical operations. Institutions should regularly evaluate the threat profile of their critical information assets, test for vulnerabilities and ensure their resilience to ICT-related risks.

3.2.5 Reporting

Report on the status of business continuity management to the board and senior management on a regular basis, highlighting where there are identified gaps. This is

through implementation status reports, incident reports, testing results and related plans for strengthening the business continuity plan.

Institutions should also report activation/invoke of their BCP's to the Central Bank of Kenya within 24 hours of the activation/invoke.

3.2.6 Testing

Facilitate testing of plans to ensure that crisis and recovery teams are aware of their roles and responsibilities in the event of disruption.

Testing the ability of an institution to recover critical operations is an essential component of effective business continuity management.

Though emphasis is made on testing technical recovery, the key element to be examined is human resources, ensuring that skills, knowledge, management and decision-making ability is assessed. An institution should ensure that:

- a) Testing of the overall business continuity management of an institution should at a minimum be conducted at least once a year.

The frequency of testing should be dependent upon the nature, size, risks and complexity of the institution. The number of tests should depend on the criticality of the business process.

- b) The frequency of testing for key functional areas is determined by how critical they are to an institution and any material changes to an institution's internal and external environment.
- c) There are measures for the quality of planning, competency of staff and effectiveness of the business continuity plan.
- d) There is organizational awareness of emergency procedures and team members and staff are familiar with their roles, accountability, responsibilities and authority in response to an incident.
- e) All technological, logistical and administration aspects of the business continuity plan have been tested.

- f) The recovery of infrastructure including command centres and off-site work area is assured.
- g) The opportunity to identify shortcomings and improvements to the institution's business continuity readiness is a continuous process.
- h) The availability and relocation of staff is assessed.
- i) Documentation of testing results for the board of directors, senior management, auditors and regulators.

3.2.7 Methods and Techniques

Management should develop a test plan for each BCP testing method used. An institution is expected to employ various methods of exercising including but not limited to the following:

- a. Technical tests.
- b. Desktop /Orientation/walkthroughs.
- c. Live runs.
- d. Simulations.
- e. Integrated tests for departments that are dependent on each other and also stress testing of recovery facilities.

3.2.8 Communication

Institution's response to a disruption should be communicated internally and externally to applicable parties. External communication to the media should only be through the external communications teams and approved by senior management or the board.

Institutions should include in their business continuity plans procedures for communicating within their institution and with relevant external parties in the event of major disruptions. The communication procedures for an institution should:

- a) Ensure that there is a clear plan identifying staff, for communicating internally (within the organization) and externally (to the public) stakeholders.

- b) Establish communication protocols clearly outlining the chain of command from the board of directors, chief executive, and senior management; Develop a directory for all recovery team members including the crisis management and emergency management teams, local emergency response organisations and critical service providers.
- c) Ensure that the directory/contact lists are made available to all team members.
- d) Address obstacles that may arise due to failure in primary communications systems (electricity, mobile phone network, road network). Ensure that the institution has set up alternative modes of communication.
- e) Ensure regular updating and testing of call trees at least quarterly.
- f) Ensure that copies of business continuity plans are disseminated to the relevant personnel.

3.2.7.1 Cross-Border Communication

Increased globalization of business processes has implications on the impact of a major operational disruption, which can extend across national borders. In this regard, institutions are expected to put in place procedures for communications with financial authorities in other jurisdictions in the event of a major operational disruption. Cross border communications mechanisms for institutions should:

- a) Take into account the implication of disruption of its business operations in one jurisdiction that significantly affects a subsidiary, branch or correspondent operations in other jurisdictions.
- b) Establish communication procedures for sharing information, views and assessments among authorities based in different jurisdictions and at different levels.
- c) Establish a directory of contacts for the various non-domestic financial authorities, supervisory bodies, treasuries, risk management/business continuity specialists.
- d) Ensure contact details are kept up to date on at least a quarterly basis.

PART IV: REMEDIAL MEASURES

- 4.1 Remedial measures – Central Bank may pursue any or all remedial actions as provided in Sections 33,33A, 34 and 55 of the Banking Act.

PART V: EFFECTIVE DATE

- 5.1 Effective date:** The effective date of this guideline shall be 1st January 2027.

- 5.2 Supersedence** - This Guideline supersedes and replaces the guideline on Business Continuity Management CBK/PG/14 issued in March 2013.

ENQUIRIES

Any enquires on this Guideline should be addressed to:

The Director
Bank Supervision Department
Central Bank of Kenya
P.O. Box 60000-00200
NAIROBI

TEL. 2860000 e-mail: *fin@centralbank.go.ke*