

GUIDELINE ON CONTINGENCY PLANNING - CBK/PG/26

CONTENTS

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: Background

PART IV: Specific Requirements

- 4.1 Governance structure and oversight
- 4.2 Board of Directors' responsibilities
- 4.3 Senior Management Responsibilities
- 4.4 Contingency Management Team
- 4.5 Internal Control
- 4.6 Critical Functions and Shared Services
- 4.7 Interconnectedness
- 4.8 Early Warning Mechanism
- 4.9 Quantitative and qualitative early warning indicators
- 4.10 Triggers for actions
- 4.11 Preparatory measures
- 4.12 Management Information System Capabilities
- 4.13 Simulation and Impact Analysis of Actions
- 4.14 Communication and Coordination
- 4.15 Cross-border and other considerations

PART V: Reporting of Contingency Plan to the Central Bank

PART VI: Remedial Measures

PART X: Effective Date

PART I: PRELIMINARY

1.1 Title - Guideline on Contingency Planning.

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 and financial system.

1.3 Application - This Guideline shall apply to all institutions licensed under the Banking Act (cap 488) and Non- Operating Holding Companies (NOHCs) to conduct business in Kenya.

1.4 Definitions

1.4.1 “Contingency plan” involves preparing for major incidents, formulating flexible plans and organising suitable resources that will come into play in the event of major incidents or business disruption.

1.4.2 “Contingency plan simulation” it is a controlled and documented exercise conducted by an institution to test, evaluate and validate the effectiveness, operational readiness and practicality of its contingency plan under hypothetical but plausible adverse scenarios.

1.4.3 “Crisis management team” it is a team that serves as an institution’s central decision-making and coordination body during periods of significant stress or disruption. It comprises of senior management and designated staff responsible for directing, coordinating and overseeing an institution’s response to actual or emerging crisis events.

1.4.4 “Critical functions” these are activities, services, operations and/or business lines performed by an institution whose disruption or failure would materially impair the institution’s ability to continue its core business operations, meet its obligations and threaten its safety and soundness, financial viability and operational resilience.

1.4.5 “Shared services” these are centralized functions, activities, resources, systems, personnel, infrastructure and support services that are utilized by multiple business units, departments and subsidiaries within an institution or a banking group to support efficient delivery of banking services, products and critical functions.

1.4.6 “Interconnectedness” it is the degree and nature of linkages, dependencies, and relationships that exist within an institution, other entities within a group, between institutions and between an institution and external parties such that the distress, disruption, failure or adverse condition of one entity, function, system, market participant or infrastructure may directly or indirectly affect the operations, financial condition, liquidity, solvency, reputation or resilience of another.

1.4.7 “Early warning system” it is a framework of indicators and analytical tools that enables an institution to identify, assess and monitor deteriorating conditions at an early stage.

PART II: STATEMENT OF POLICY

2.1 Purpose

This Guideline outlines the minimum requirements and supervisory expectations for the development, implementation, testing and governance of contingency plans by institutions. The objective is to enhance preparedness, strengthen operational resilience, support effective crisis management, and contribute to the safety, soundness and stability of the banking sector.

A contingency plan describes the actions to take in response to a specific disruption and focuses on ensuring operational resilience. A contingency plan should not be confused with business continuity management (BCM), which is a risk management framework that ensures the organization can continue delivering critical services during and after disruptions. BCM is broader and covers the entire organization and all critical business functions while the contingency plan focuses on a specific incident or risk.

2.2 Scope

This Guideline provides a clear guide to institutions on the minimum requirements for developing an appropriate contingency plan.

2.3 Responsibility

The board of directors is ultimately responsible for the oversight of contingency planning. The board must ensure that there are clear roles and responsibilities at senior management for the preparation, maintenance and execution of the contingency plan. The board must approve and oversee any review of the contingency plan.

PART III: BACKGROUND

The crisis management working group of the Monetary Affairs Committee required that each member state partners' supervisory authority develop a contingency plan for large banks¹. It's on this basis that the contingency plan guideline has been developed.

The Financial Stability Board requires systemically important institutions to maintain robust and actionable contingency plans such as;

- Financial Market Infrastructure plan to maintain essential payment and settlement services;
- Contingency funding plan to deal with sudden, severe disruptions to their cash flow; and
- Recovery and Resolution plan to restore viability under severe stress.

Basel Core Principle 15 mandates supervisors to require banks to have appropriate contingency arrangements, as an integral part of their risk management process, to address risks that may materialize and actions to be taken in stress conditions (including those that will pose a serious risk to their viability).

A contingency plan serves as a structured framework that enables an institution to respond effectively to unexpected adverse events that may threaten its normal operations, financial position and/or heighten risk relating to its reputation. The contingency plan outlines the actions, governance arrangements, communication protocols, and resources required to manage crisis situations, maintain critical functions, minimize losses and facilitate the timely restoration of normal operations.

The primary purpose of a contingency plan is to ensure that an institution can continue delivering critical services to customers during periods of disruption while safeguarding the interests of depositors and preserving market confidence.

PART IV: SPECIFIC REQUIREMENTS

4.1 Governance structure and oversight

4.1.1 An institution shall establish sound governance arrangements to oversee and manage the contingency planning process, which at minimum, shall establish: -

¹ MAC Bank Supervision and Financial Stability sub-committee, Crisis management working group

- (a) well-defined roles, responsibilities and accountabilities of the board, senior management, business units and control functions.
- (b) robust policies, procedures and management information systems to support informed decision making across the institution in order to ensure that the contingency plan is capable of being executed in an effective and efficient manner.

4.2 Board of Directors' responsibilities

- 4.2.1 The board shall exercise effective oversight on all aspects of the development and implementation of the contingency plan and shall, at a minimum:
- (a) Review and approve the contingency planning policies developed by senior management;
 - (b) Designate a senior officer or committee responsible for driving the overall contingency planning process;
 - (c) Ensure sufficient resources are allocated to support the development and implementation of the contingency plan;
 - (d) ensure that the contingency plan is integrated with existing risk appetite and risk management frameworks and is complementary and closely linked to the institution's strategic plan; and
 - (e) receive and review assurance reports of the contingency plan from internal, external or independent party.

4.3 Senior Management Responsibilities

- 4.3.1 The responsibilities of the senior management of an institution shall include but not limited to:
- (a) preparing contingency planning policies, procedures, and strategies for managing stress events.
 - (b) developing contingency plans necessary for the continuity of critical functions and shared services.
 - (c) developing detailed action plans for specific events identified in the contingency plan.
 - (d) ensure that the contingency planning process is undertaken with the appropriate level of involvement of key personnel across core operational areas of the institution.
 - (e) ensure the robust and credible application of expert judgement and critical scrutiny in the development of the risk modelling and quantitative risk

- methodologies used in the contingent plan framework and scenario analysis.
- (f) ensure that well-defined processes and management information systems are developed to provide good quality and granular data for timely risk communication and reporting to the board.
 - (g) regularly update the board on material developments relating to contingency planning, including the early warning indicators and triggers, breaches of regulatory requirements thresholds, activation of the contingency plan, implementation of contingent plan and its progress, and preparatory measures to be undertaken.
 - (h) ensuring that all levels of staff are trained and are fully aware of their roles in the implementation of contingency plan.
 - (i) conducting contingency plan simulations, analyzing results and report to the Board on regular basis.
 - (j) keeping the contingency plan up to date by reviewing it at least annually.
 - (k) ensuring review of the adequacy and effectiveness of the Contingency Plan by internal or external auditor, or any other independent party.
 - (l) ensuring that roles, responsibilities and authority to act, as well as succession plans are clearly articulated in the contingency plan to avoid confusion in the event of financial stress.
 - (m) developing a monitoring mechanism for contingent events and report to the board.

4.4 Contingency Management Team

4.4.1 An institution shall establish a Contingency Management Team, consisting of key executives and functional heads of critical operational areas, which shall be responsible for operationalising the contingency plan during a stressful event. Such a Team shall draw its membership from the following:

- (a) Managing Director or Chief Executive Officer who is the chairperson.
- (b) Senior Management responsible for Treasury, Finance, Operations, Legal Services, Credit, Retail, Risk Management, Information Technology, Human Resources and Communications.
- (c) Line Managers to provide operational leadership within their respective business areas.
- (d) Any person responsible for critical functions or services of the institution.

4.4.2 An institution can utilise members of business continuity management or crisis

management as members of the contingency management team.

- 4.4.3 The roles and responsibilities of each individual member should be clearly defined.
- 4.4.4 The roles and responsibilities of the Contingency Management Committee shall include the following:
- (a) Ensuring the Contingency Plan is in place, frequently updated and effectively implemented;
 - (b) Identifying and assessing stress events and levels of severity and timing for activation of the Contingency Plan;
 - (c) Assessing potential impact on liquidity position, capital adequacy, operational resilience and brand reputation;
 - (d) Identifying market-wide and institution-specific scenarios in developing contingency actions;
 - (e) Describing communication channels for both internal and external stakeholders;
 - (f) Identifying triggers that are appropriate for the institution's risk profile, critical business lines and critical functions and shared services;
 - (g) Coordinating the restoration of critical functions and orderly return to normal operations;
 - (h) Monitoring the impact and effectiveness of contingency actions undertaken during the stress events;
 - (i) Developing, coordinating, conducting and periodically reviewing the training and awareness program to enhance the institution's preparedness, resilience and ability to respond effectively to disruptive events;
 - (j) Perform crisis simulations and testing to assess the effectiveness of the contingency plans and response capabilities.

4.5 Internal Control

- 4.5.1 An institution shall put in place internal controls including effective assurance functions for contingency planning such as internal audit, risk and compliance functions, governance policies and structures which are:
- (a) consistent with the risk profile of the institution and its business model, critical functions and services including those outsourced from third-party service providers.
 - (b) sufficient to ensure effective discharge of responsibilities for stewardship of resources, compliance with legislative and other requirements.
- 4.5.2 The internal audit function or other independent party shall conduct periodic reviews

of the Contingency Plan to determine whether the plan is realistic and remains relevant and whether it adheres to the policies and standards established by the Board.

4.6 Critical Functions and Shared Services

- 4.6.1 Continuity of an institution's critical functions and shared services is essential in preventing potential disruptions that could adversely impact its operations.

4.6.2 Critical Functions

- 4.6.2.1 A contingency plan shall provide an overview of an institution's business model at a high-level, describing its activities, including significant business lines.
- 4.6.2.2 An institution shall identify its critical functions on its operations, activities or services that are provided to the customers or any counterparty. In identifying critical functions, the institution shall consider the following:
- (a) whether a failure or discontinuity of such functions would likely lead to the disruption of services that are essential for the functioning of the entity.
 - (b) contribution of the business line to its profit, assets, capital, liabilities, or risk profile;
 - (c) strategic significance of the business line in relation to:
 - (i) customer base, geographic reach, and branch network;
 - (ii) market potential and growth outlook;
 - (iii) indicative value under the current operating environment, taking into account the provision of market access or international linkages to the bank or financial institution;
 - (iv) operational synergies with other business lines;
 - (v) attractiveness to competitors as a potential acquisition target; and
 - (vi) other factors that contribute to the business line's significance to the institution.
- 4.6.2.3 An institution shall at minimum assess the criticality of functions and identify any additional functions deemed critical.
- 4.6.2.4 Following identification of the critical functions, an institution shall consider in its contingency plan the impact of disruptions on its operations and ability to continue providing services to customers and participation in financial markets infrastructure (local and foreign).
- 4.6.2.5 Assess the impact of disruption of the critical function by applying the indicators as highlighted in 4.9.
- 4.6.2.6 An institution shall, for each critical functions identified, include in the

contingency plan, mitigation measures to ensure continuity of the services.

4.6.3 Critical Shared Services

- 4.6.3.1 Critical shared services refer to the underlying operations, activities or services that are performed for one or more covered unit or entities, where the failure or discontinuance of such services would present a serious impediment or completely impair the performance of one or more critical functions.
- 4.6.3.2 An institution shall identify critical shared services that are performed by an internal unit, a related entity and/or outsourced from external third-party service providers.
- 4.6.3.3 In identifying critical shared services, an institution shall take into consideration at minimum, the following criteria:
 - (a) The impact of discontinuance is likely to have an adverse effect on one or more critical functions; and
 - (b) substitutability of the service, i.e. availability and ease of which the provision of the service can be replaced by other substitute providers with similar quality, at comparable cost.
- 4.6.3.4 An institution shall at minimum, assess the significance of shared critical services and identify any additional shared services deemed critical.
- 4.6.3.5 An institution shall, for each shared critical services identified, include in the Contingency Plan, mitigation measures to minimize disruptions of its operations.

4.7 Interconnectedness

- 4.7.1 An institution shall identify material dependencies, assess key risk transmission channels and the extent of potential adverse effects arising from the disruption or failure of such dependencies which may be financial, operational or legal in nature and determine contingency options. In particular, an institution shall identify and assess:
 - (a) intra-group dependencies covering entities and entities related to the institution that, if disrupted, would significantly affect the funding or operations of institution and/or its performance of critical functions; and
 - (b) external dependencies on third parties services by the institution including management information systems and financial market infrastructures

whereas if disrupted, would significantly affect the funding or operations of the institution and/or its performance of critical functions.

4.7.2 To identify dependencies, an institution shall take into account the following:

- (a) extent of reliance on intra-group capital, funding and liquidity arrangements, off-balance sheet exposures, capital, liquidity, funding, risk transfer, financial support agreements/ guarantees, cross-collateral and intra-group product netting arrangements;
- (b) extent of reliance on external non-related counterparties off-balance sheet exposure, capital, liquidity and funding as well as financial commitments, guarantees, netting arrangements and risk transfers;
- (c) significance of an institution role in providing funding, liquidity or risk transfer to related or third parties;
- (d) extent of reliance on intra-group service providers, shared material operational services (including personnel, facilities and systems) and access to payment systems (local and foreign) as well as reliance on one entity which is a member of a central clearing counterparty; and
- (e) extent of reliance on external service providers including operational services that are outsourced.

4.8 Early Warning Mechanism

4.8.1 Early warning

4.8.1.1 Contingency Plan shall include an early warning mechanism for receiving relevant and timely information in a systematic manner prior to a crisis to facilitate informed decisions and timely corrective actions to:

- (a) minimize disruptions of service to customers;
- (b) minimize financial losses due to business disruptions; and
- (c) ensure timely resumption of normal operations in the event of a realization of crisis.

4.8.1.2 An institution shall establish early warning indicators that set out clearly defined criteria and thresholds to facilitate timely monitoring, escalation, activation and

implementation of the Contingency Plan. Such Indicators shall at minimum:

- (a) facilitate prompt identification and escalation of key vulnerabilities and stress events which could adversely affect the bank or financial institution;
- (b) enable risk monitoring and management across critical functions and mitigation levels in a cohesive manner; and
- (c) ensure timely decision and activation of potential management actions.

4.8.1.3 The early warning indicators shall include, to the extent applicable, thresholds on key internal and external market indicators for monitoring liquidity, capital adequacy, asset quality, earnings, market risk, turnover of board and management, operational risk and any other indicators that facilitate continuity of the critical functions.

4.9 Quantitative and qualitative early warning indicators

4.9.1 An institution shall develop a suite of quantitative and qualitative early warning indicators that are:

- (a) tailored to the size and complexity of its business model/operations, inherent risk drivers and strategy;
- (b) clearly defined, forward-looking and suitable for close monitoring of evolving stress events, taking into consideration the intrinsic characteristics and quality of indicators (e.g. reliability, sensitivity and ease of monitoring);
- (c) aligned with existing indicators used for risk monitoring, escalation and decision-making; and
- (d) diverse to capture an extensive range of stress scenarios of varying nature and severity.

4.9.2 An institution shall establish early warning indicators which are above the regulatory thresholds.

4.9.3 An institution shall supplement the early warning indicators developed at the consolidated level with entity-level indicators specific to subsidiaries, where such indicators serve to capture specific key vulnerabilities faced by the group or subsidiaries.

4.10 Triggers for actions

4.10.1 An institution shall establish thresholds which trigger contingency actions, and at a minimum shall:

- (a) not breach statutory requirements;
 - (b) be at a level before the point of non-viability and able to provide reasonable time based on realistic assumptions that will enable:
 - (i) to implement and realize the benefits of contingency actions; and
 - (ii) to intensify monitoring implementation of contingency actions.
- 4.9.4 An institution shall take contingency actions based on its established procedures.
- 4.9.5 An institution shall ensure that in implementing the contingency actions, it will not negatively affect the continuity of its critical functions and shared services.

4.11 Preparatory measures

- 4.11.1 An institution shall identify preparatory measures to improve the overall efficacy of the Contingency Plan which shall include, but not limited to:
 - (a) measures aimed at overcoming the barriers to the efficacy of identified contingency options and preferred strategies; and
 - (b) the implementation timeline, target completion dates, resources and key personnel responsible for the implementation of these measures.

4.12 Management Information System Capabilities

4.12.1 Access and Availability

- 4.12.1.1 An institution shall ensure that:
 - (a) Its Management Information Systems (MIS) are capable of supporting business continuity for core business lines, critical functions and essential services to its customers and are in compliance with regulatory requirements;
 - (b) Its Contingency Plan explicitly provides details on mitigation measures on how the MIS will continue to support all critical and essential services needed by the institution that depend on MIS prior to, during adverse stress events and after a crisis;
 - (c) Its Contingency Plan identifies and/or explicitly provides for:
 - (i) necessary contingency arrangements to ensure its continuity of participation in interbank payment, clearing and settlement systems and provide an analysis of the potential impact of discontinued or degraded access.

- (ii) necessary contingency arrangements are established for effective business continuity for outsourced and/or third-party information technology providers.

This shall include:

- (a) A list of providers or the critical and essential MIS of the institution including payment, clearing and settlement systems in which it participates;
- (b) Analysis of potential impact of discontinued or degraded access that impairs its ability to undertake its critical function or access to shared services;
- (c) Analysis of the measures that these outsourced and/or third-party technology service providers should take in order to ensure business continuity; and
- (d) The Contingency Plan explicitly provides and covers its MIS capabilities when the parent or group is located in another jurisdiction to ensure that its critical and shared services are not disrupted due to the interconnectedness within the group. The local MIS contingency arrangements should ensure that access prior to, during and after crisis is maintained.

4.12.2 System support

4.12.2.1 An institution shall ensure that MIS is capable of:

- (a) providing functionalities to be invoked for effective crisis management;
- (b) supporting the preparation of regulatory reports and compliance to key financial health indicators by maintaining detailed granular information on proprietary and client exposures/positions and delivery obligations on a daily basis;
- (c) Maintaining a record of, and is able to provide, information prior to or upon entry into adverse financial stress with regard to:
 - (i) The collateral pledged, distinguishing collateral that supports proprietary and client activities by type, aggregate values, from the payment, clearing and settlement systems and/or other financial markets infrastructure intermediaries in which it participates.
 - (ii) The collateral pledged to a jurisdiction in which the security interest of the collateral is enforceable against the institution.

- (iii) A list of the types of collateral and haircuts accepted by a payment, clearing and settlement systems and/or other financial markets infrastructure intermediaries in which it participates.
 - (iv) A list of upcoming settlement and delivery obligations, by value and type of asset, for a specified upcoming period to and/or via the payment, clearing and settlement systems and/or other financial markets infrastructure intermediaries in which it participates.
- (d) Facilitating compliance reporting as required by the institution in respect to the above information or other information generated by the institution incidental to the critical and essential services including real-time reporting; and
 - (e) Facilitating analysis of the liquidity needs that the institution requires to comply with, including any additional collateral requirements, related to the use of payment, clearing and settlement systems services (including on an intraday basis) for all financial markets infrastructure service providers and for each provider individually, which contribute to the bank's preparedness for a potential resolution.

4.13 Simulation and Impact Analysis of Actions

- 4.13.1 An institution shall conduct a simulation of its Contingency Plan to assess the institution's readiness to respond to a stress situation. In doing so, at minimum, it shall:
- (a) Test the viability of the Contingency Plan before its Board's approval;
 - (b) Conduct annual tests of the Contingency Plan to ensure that emergency management capabilities are consistent with the plans, procedures and policies;
 - (c) Require its provider(s) of critical services to participate in the testing process.
 - (d) Apply the test results in reviewing:
 - (i) the Contingency Plan to ensure that the plan remains relevant.
 - (ii) the effectiveness of third-party service providers
 - (a) Assess the impact of the test results provided in subsection (d), on its critical functions and core business lines and devise appropriate remedial actions with specified implementation time frames.

4.14 Communication and Coordination

- 4.14.1 An institution shall ensure that it identifies the roles and responsibilities for communication and coordination during activation of the contingency plan.

- 4.14.2 An institution shall include communication and coordination strategies in the Contingency Plan to ensure relevant stakeholders are adequately informed throughout the activation of the Plan.
- 4.14.3 In developing communication and coordination strategies, an institution shall consider:
- (a) Communication needs of different stakeholders;
 - (b) Communication needs specific to individual contingency actions; and
 - (c) Applicable disclosure requirements such as legal provisions, regulations or listing rules in relation to unpublished information.
- 4.14.4 A communication strategy of an institution shall include, at minimum:
- (a) Identification of key stakeholders, comprising:
 - (i) Internal stakeholders including employees of branches and subsidiaries; and
 - (ii) External stakeholders including shareholders, Central bank, other authorities, customers, counterparties, general public where necessary.
 - (b) Stakeholder engagement strategies to support the implementation of the Contingency Plan, providing:
 - (i) Medium of communication;
 - (ii) Level of detail, timing and frequency of information; and
 - (iii) The parties identified to lead such engagements
 - (c) Plans to mitigate or prevent potential adverse market reactions and maintain public confidence.
- 4.14.5 A coordination strategy of an institution shall include, at minimum:
- (a) a plan for coordinating actions for activating and executing the Contingency Plan;
 - (b) resources including personnel responsible for ensuring effective coordination of Contingency Plan.

4.15 Cross-border and other considerations

- 4.15.1 An institution shall include in its Contingency Plan, comprehensive procedures, in relation to cross-border operations which include at a minimum: -
- (a) communication strategy for financial regulatory authorities and institutions in other jurisdictions; and
 - (b) comprehensive procedures for handling disruptions in its MIS or participation in

the financial market infrastructures.

4.15.2 Other Considerations

4.15.2.1 An institution shall ensure that its Contingency Plan outlines mitigation measures for other risks, which at a minimum shall include:

- (a) fraud risk as the risk to the current or projected financial condition, and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events;
- (b) emerging technological risks emanating from technological innovations for financial services offered by non-traditional players which may disrupt the institution's business model to effectively deliver its critical functions and shared services;
- (c) climate-related financial risks that may require enhanced compliance, adjustments of its service provisions to cater for physical and transition risks including costs of compliance to Environmental, Social and Governance risks and adjustment of its services and products to comply with climate-friendly financial services and products such as increase of credit to green and low carbon sectors; and
- (d) political risks that may emanate from abrupt and drastic policy and regulatory changes, political instability leading to social unrests, fragility, geopolitical tensions, wars and global macro-financial crisis.

PART V: REPORTING OF CONTINGENCY PLAN TO THE CENTRAL BANK

5.1 Institutions are required to prepare on an annual basis contingency plans and submit to the Central Bank by 30th April. The Contingency plan should at a minimum cover the following:

- (a) Governance structure and oversight;
- (b) Identification, assessment and impact of critical functions and shared service including mitigation measures;
- (c) Management Information System capabilities;
- (d) Early Warning Indicators;
- (e) Simulation and Impact Analysis of contingency actions;
- (f) Communication and coordination strategies; and
- (g) Cross-border considerations

PART VI: REMEDIAL MEASURES

Where any provision of this Guideline is breached or not observed, the Central Bank may pursue any or all of the remedial actions and administrative sanctions provided for under the Banking Act.

PART VII: EFFECTIVE DATE:

The effective date of this Guideline shall be 1st January 2027.

ENQUIRIES

Enquiries on any aspect of this Guideline should be referred to:

The Director,
Bank Supervision Department
Central Bank of Kenya
P. O. Box 60000 - 00200
NAIROBI
TEL.2860000 e-mail: fin@centralbank.go.ke

References

1. Australia Prudential Regulation Authority, Prudential Standard CPS 190, Financial Contingency Planning, December 2021
2. Bank of Tanzania, Contingency Planning Guideline for banks and financial institutions, 2023.