

GUIDELINE ON OPERATIONAL RISK AND OPERATIONAL RESILIENCE - CBK/PG/27

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

PART III: Principles of Sound Operational Risk Management and Operational Resilience

- 3.1 Introduction
- 3.2 Linkage Between Sound Operational Risk Management and Operational Resilience
- 3.3 Principles of Sound Operational Risk Management
- 3.4 Principles of Operational Resilience
- 3.5 Responsibilities of the Board of Directors
- 3.6 Responsibilities of Senior Management

PART IV: Reporting on Operational Risk and Operational Resilience

- 4.1 Incident Tracking and Reporting
- 4.2 Scenario Testing and Vulnerability Assessment
- 4.3 Operational Resilience Self-Assessment

PART V: Remedial Measures

PART VI: Effective Date

- 6.1 Effective date
- 6.2 Supersedence

PART I: PRELIMINARY

1.1 Title - Guideline on Operational Risk and Operational Resilience

1.2 Authorisation - 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 applies to institutions licensed under the Banking Act and non-operating holding companies.

1.4 Definitions

1.4.1 “Business Continuity Management” is a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that critical operations can be maintained or recovered in a timely manner in the event of disruption. Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from disruption.

1.4.2 “Business Continuity Plan” is a component of business continuity management. A business continuity plan is a comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of an organisation in the event of a disruption.

1.4.3 “Business Impact Analysis” is a component of business continuity management. Business impact analysis is the process of identifying and measuring (quantitatively and qualitatively) the business impact or 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 a business continuity plan.

1.4.4 “Critical Operations” encompasses critical functions and includes activities, processes, services and their relevant supporting assets, the disruption of which would be material to the continued operation of the institution or its role in the financial system. Whether a particular operation is critical depends on the nature of the institution and its role in the financial system.

1.4.5 “Critical Functions” are activities, services, or operations provided by a financial institution to third parties that are so vital that their sudden failure would likely disrupt the real economy or jeopardise financial stability.

1.4.6 “Important Business Service (IBS)” is a service whose disruption could cause intolerable harm to customers, threaten financial stability, or undermine confidence in the financial system.

1.4.6 “Impact Tolerance” is the maximum tolerable level of disruption to an IBS.

1.4.7 “Invocation process” is the procedure an institution follows to officially declare a Business Continuity Plan (BCP) or Disaster Recovery (DR) event. It is an actionable transition from standard operations to emergency measures to sustain or rapidly recover critical services.

1.4.8 “Impact Tolerance” means the maximum level of disruption that an institution can tolerate in the delivery of a critical operation, measured using defined quantitative and qualitative metrics, beyond which the disruption would result in unacceptable harm to customers, compromise the safety and soundness of the institution, or pose a risk to financial stability.

1.4.9 “Impact Tolerance Metrics” means the quantitative and qualitative indicators established by an institution to measure whether the disruption of a critical operation remains within the approved impact tolerance. These metrics should be objective, measurable, and regularly reviewed to ensure they remain appropriate to the institution's operational resilience objectives.

1.4.10 “Material Incident” is an operational disruption with significant customer, financial, regulatory, or systemic impact.

1.4.11 “Operational risk” is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.

1.4.12 “Operational resilience” refers to the ability of an institution to deliver critical operations through disruption. This ability enables an institution to identify and protect itself from threats and potential failures, respond to and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption.

1.4.13 “Respective Functions” refers to the appropriate function(s) within the institution’s three lines of defence. These consist of business unit management, the independent operational risk management function, and the independent internal audit assurance.

1.4.14 “Recovery” means the rebuilding of a specific business operation following a disruption to a level sufficient to meet outstanding business obligations.

1.4.15 “Recovery Objective” is 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).

1.4.16 “Recovery Time” (RT) is 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.

1.4.17 “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.

1.4.18 “Severe but Plausible Scenario” is a realistic but extreme disruption scenario used for resilience testing.

1.4.20 “Single Point of Failure” is a component whose failure would cause significant disruption to an IBS.

1.4.21 “Tolerance for Disruption” is the level of disruption from any operational risk an institution is willing to accept, given a range of severe but plausible scenarios.

PART II: STATEMENT OF POLICY

2.1 Purpose

This Guideline outlines the minimum prudential requirements that an institution should implement to effectively manage operational risk and strengthen operational resilience. It seeks to ensure that institutions can maintain critical operations during severe but plausible disruptions, thereby minimising financial loss and service disruption to customers, preserving public confidence, and promoting the safety, soundness and stability of the financial system. The banking sector is becoming increasingly digital, interconnected and reliant on information and communication technology (ICT), data and third-party service providers. While these developments have improved efficiency, innovation and financial inclusion, they have also increased the frequency and complexity of operational disruptions arising from cyber-attacks, technology failures, fraud, outsourcing arrangements and other external events. These developments have demonstrated that effective operational risk management alone is no longer sufficient. Institutions must also have the capability to anticipate, withstand, respond to, recover from and adapt to operational disruptions while maintaining critical operations.

Recognising this evolving risk landscape, the Basel Committee on Banking Supervision (BCBS) revised the Principles for the Sound Management of Operational Risk (SMOR) in 2021 and, through 2024, revised the Basel Core Principles for Effective Banking Supervision, expanding Core Principle 25 from Operational Risk to Operational Risk and Operational Resilience. This reflects the recognition that operational resilience is founded on

sound operational risk management and has become an integral component of effective prudential supervision.

Accordingly, this Guideline enhances the regulatory framework by integrating operational risk management and operational resilience into a single prudential framework. It requires institutions to strengthen governance, operational risk management, ICT and cyber risk management, business continuity, incident management and third-party risk management to ensure continuity of critical operations and services.

The Central Bank expects the Board of Directors and senior management of every institution to review this Guideline, adopt appropriate governance and risk management measures, and ensure its effective implementation. Institutions should be able to demonstrate that they have considered the supervisory expectations set out in this Guideline and implemented appropriate policies, processes, systems and controls to achieve compliance.

The objectives of this Guideline are to:

- a) Establish a sound framework for the management of operational risk and operational resilience.
- b) Improve institutions' ability to maintain critical operations and services during severe but plausible disruptions.
- c) Strengthen governance, ICT and cyber resilience, business continuity, and third-party risk management.
- d) Enhance incident response, crisis management and recovery capabilities.
- e) Minimise prudential, consumer and systemic risks arising from operational disruptions.
- f) Promote the safety and soundness of institutions and the stability of the financial system.

2.2 Scope

This Guideline sets out the minimum prudential requirements for governance and management of operational risk and operational resilience by institutions and banking groups. It establishes supervisory expectations for identifying, assessing, monitoring, controlling and mitigating operational risk, while strengthening institutions' ability to anticipate, withstand, respond to, recover from and adapt to operational disruptions to maintain critical operations and services.

This Guideline should be read together with the Central Bank's Guidelines on Business Continuity Management, Third Party Service Providers (TPSPs), Stress Testing and Information Communication Technology (ICT) and the Guidance Note on Cyber Security.

PART III: PRINCIPLES OF SOUND OPERATIONAL RISK MANAGEMENT AND OPERATIONAL RESILIENCE

3.1 INTRODUCTION

The principles of operational risk management and operational resilience provide the foundation for institutions to effectively manage operational risk and maintain the continuity of critical operations during severe but plausible disruptions. They require institutions to establish sound governance, a strong risk culture, effective risk management frameworks and internal controls to identify, assess, monitor, control and mitigate operational risks. The principles require institutions to strengthen their operational resilience by enhancing ICT and cyber resilience, business continuity, third-party risk management, incident response and recovery capabilities, enabling them to anticipate, withstand, respond, adapt, recover and learn from disruptions while continuing to deliver critical operations and services.

3.2 THE LINKAGE BETWEEN SOUND OPERATIONAL RISK MANAGEMENT AND OPERATIONAL RESILIENCE

Sound Operational Risk Management (SORM) provides the foundation for operational resilience. SORM focuses on identifying, assessing, monitoring, controlling and mitigating operational risks to reduce the likelihood and impact of operational risk events. Operational Resilience builds on this foundation by ensuring that an institution continues to deliver its critical operations, recover promptly and adapt to future disruptions when they occur. Operational Resilience is therefore an outcome of sound operational risk management rather than a separate risk type. SORM and operational resilience enhance the resilience of institutions and the stability of the financial system.

3.3 PRINCIPLES OF SOUND OPERATIONAL RISK MANAGEMENT

An effective operational risk management framework comprises integrated components that enable institutions to identify, assess, monitor, control and mitigate operational risks while strengthening operational resilience. These components should be proportionate to the institution's nature, size, complexity and risk profile. The key principles of SORM include:

Principle 1: Operational Risk Culture

The board of directors and senior management should establish a corporate culture guided by strong risk management, set standards and incentives for professional and responsible behaviour, and ensure that staff receive appropriate risk management and ethics training.

Institutions that foster a strong risk management culture and uphold high ethical standards are less susceptible to significant operational risk events and are better positioned to manage and mitigate such events when they occur. Effective operational risk management requires active support and oversight from the board and senior management as indicated below:

- a) The Board of Directors should establish and maintain a Code of Conduct or Ethics Policy that shall:
 - i) Apply to all directors, senior management, and employees.
 - ii) Set out the institution's standards of integrity, ethical conduct, and professional behaviour.
 - iii) Define acceptable business practices.
 - iv) Require the identification, disclosure, and management of conflicts of interest, and prohibit inappropriate or unethical conduct.
 - v) Be reviewed periodically and approved by the Board, with directors, senior management, and employees required to acknowledge compliance.
 - vi) Be overseen by a Board committee or designated ethics committee and made publicly available (e.g. on the bank's website).
 - vii) Where appropriate, be supplemented by role-specific codes of conduct for designated positions, such as treasury dealers and senior management.
 - viii) Set clear expectations and accountabilities to ensure bank staff understand their roles and responsibilities for risk management, as well as their authority to act.
- b) Compensation policies should be aligned to the bank's statement of risk appetite and tolerance as well as overall safety and soundness and appropriately balance risk and reward.
- c) Senior management should ensure operational risk training is provided across all levels of the organisation, tailored to employees' roles, responsibilities, and seniority.

d)

Principle 2: Operational Risk Management Framework

Banks should develop, implement and maintain an operational risk management framework that is fully integrated into the bank's overall risk management processes. The operational risk management framework adopted by an individual bank will depend on a range of factors, including the bank's nature, size, complexity and risk profile.

- a) The board of directors and bank management should understand the nature and complexity of the risks inherent in the portfolio of bank products, services, activities, and systems.

- b) The components of the operational risk management framework should be fully integrated into the overall risk management processes of the bank by the first line of defence, adequately reviewed and challenged by the second line of defence, and independently reviewed by the third line of defence.
- c) The operational risk management framework should be embedded across all levels of the organisation, including group and business units as well as new business initiatives' products, activities, processes and systems.
- d) Results of the bank's operational risk assessment should be incorporated into the bank's overall business strategy development process.
- e) The operational risk management framework should be comprehensively and appropriately documented in board-approved policies and include definitions of operational risk and operational loss.
- f) The operational risk management framework should:
 - i) Identify the governance structures used to manage operational risk, including reporting lines and accountabilities, and the mandates and membership of the operational risk governance committees;
 - ii) Reference the relevant operational risk management policies and procedures;
 - iii) Describe the tools for risk and control identification and assessment and the role and responsibilities of the three lines of defence;
 - iv) Describe the bank's accepted operational risk appetite and tolerance; the thresholds, material activity triggers or limits for inherent and residual risk; and the approved risk mitigation strategies and instruments;
 - v) Describe the bank's approach to ensure controls are designed, implemented and operating effectively;
 - vi) Describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;
 - vii) Inventory risks and controls implemented by all business units;
 - viii) Establish risk reporting and Management Information Systems (MIS) producing timely and accurate data;
 - ix) Provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives across all business units. The taxonomy should:
 - Distinguish operational risk exposures by event types, causes, materiality and business units where they occur.
 - Flag those operational exposures that partially or entirely represent legal, conduct, model and ICT (including cyber) risks as well as exposures in the credit or market risk boundary.

- x) Provide for appropriate independent review and challenge of the outcomes of the risk management process; and
- xi) Require the policies to be reviewed and revised as appropriate based on continued assessment of the quality of the control environment addressing internal and external environmental changes or whenever a material change in the operational risk profile of the bank occurs.
- xii)

Principle 3: Responsibilities of Board of Directors

The board of directors should approve and periodically review the operational risk management framework, and ensure that senior management implements the policies, processes and systems of the operational risk management framework effectively at all decision levels.

The board of directors should:

- a) Establish a strong risk management culture and ensure the institution has adequate processes to identify, understand, and assess the operational risks arising from its current and planned strategies.
- b) Ensure operational risk management processes are subject to effective oversight and are fully integrated within the institution's overall risk management framework.
- c) Provide senior management with clear guidance regarding the principles of the operational risk management framework.
- d) Regularly review and approve the operational risk management framework to ensure the institution effectively identifies, manages, and responds to operational risks arising from changes in the operating environment, business activities, products, processes, and systems.
- e) Ensure the operational risk management framework is subject to effective and independent review by the third line of defence (internal audit) or other suitable independent third-party reviewers.
- f) Establish clear management responsibilities and accountability for maintaining a strong control environment. Controls should be regularly reviewed, monitored, and tested for effectiveness, with appropriate segregation of duties between operational risk management, business unit, and support functions.

Principle 4: Risk Appetite and Tolerance Statement

The board of directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk the bank is willing to assume.

- a) The operational risk appetite and tolerance statement should be developed under the authority of the Board of Directors and aligned with the bank's short-term and long-term strategic plans and targets. It should take into account the interests of customers and shareholders, as well as applicable regulatory requirements. In addition, it should:
 - i) Be clearly articulated and easily understood by all stakeholders.
 - ii) Document the key assumptions and background factors underlying the bank's business plans at the time of approval.
 - iii) Clearly state the bank's approach to risk-taking and risk avoidance and establish measurable indicators and limits for monitoring risk exposures.
 - iv) Ensure that the strategies and risk limits of business units and legal entities are aligned with the bank-wide risk appetite statement.
 - v) Be forward-looking and supported by scenario analysis and stress testing to assess potential breaches of risk appetite and tolerance levels.
- b) The board of directors should approve and regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statement.
- c) The board of directors should monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.

Principle 5: Responsibilities of Senior Management

Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the institution's material products, activities, processes and systems consistent with the bank's risk appetite and tolerance statement.

- a) Senior management should implement and maintain effective policies, processes, and systems for managing operational risk across all material products, activities, processes, and systems, in line with the institution's risk appetite and tolerance.
- b) Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue resolution processes. These should include establishing systems for reporting, tracking, and escalating issues to ensure resolution.
- c) Senior management should translate the operational risk management framework approved by the board of directors into specific policies and procedures that can be implemented and verified within the different business units.
- d) Senior management should clearly define roles, responsibilities, and reporting lines, and ensure adequate resources are available to manage operational risk effectively. It should also ensure that oversight is commensurate with the risks of each business unit's activities.

- e) Senior management should ensure effective coordination and communication among staff responsible for operational, credit, market, insurance and other relevant risks, as well as those managing third-party arrangements, to avoid gaps or overlaps in overall risk management.
- f) Managers in charge of operational risk management should be of sufficient stature to enable them to perform their duties effectively. Their positions should be commensurate with those of other senior management in charge of key functions such as credit, finance, treasury, audit and risk.
- g) Senior management should ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should be independent from the units they oversee.
- h) A bank's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, a bank should consider the following:
 - i. Committee structure - depending on the nature, size and complexity of the bank, the enterprise-level risk committee may receive input from operational risk committees by country, business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board's risk management committee.
 - ii. Committee composition – the operational risk committees should include members with a variety of expertise, which should cover expertise in business activities, financial activities, legal, technological and regulatory matters and independent risk management.
 - iii. Committee operation – committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

Principle 6: Risk Identification and Assessment

Senior management should ensure comprehensive identification and assessment of operational risk inherent in all material products, activities, processes and systems to ensure that inherent risks and incentives are well understood.

- a) Risk identification and assessment are fundamental characteristics of an effective operational risk management system and directly contribute to operational resilience capabilities. Effective risk identification considers both internal factors and external factors. Sound risk assessment allows an institution to better understand its risk profile and allocate risk management resources and strategies more effectively.

- b) Operational risk assessment tools contribute to an institution's operational resilience, as they allow banks to identify and monitor threats and vulnerabilities to their critical operations. To strengthen operational resilience and enhance the identification, assessment, and management of operational risks, institutions should use the outputs of the following tools:
- i. Event Management - When banks experience an operational risk event, the process of identification, analysis, end-to-end management and reporting of the event follows a predetermined set of protocols. In addition, event management approaches typically include analysis of events to identify new operational risks, understanding the underlying causes and control weaknesses and formulating an appropriate response to prevent recurrence of similar events. This information is an input to the assessment of control effectiveness.
 - ii. Operational Risk Event Data - Institutions should maintain a comprehensive operational risk event dataset that collects all material events experienced by the institution and serves as a basis for operational risk assessments. The event dataset includes internal loss data classified according to the taxonomy defined in the operational risk management policies. It captures event details, including the occurrence, discovery, and accounting dates, as well as the financial impact of operational loss events. Where feasible, institutions should also gather external operational risk event data and use the data in their internal analysis, as it is often informative of the types of risks that are common across industry.
 - iii. Self-Assessments - institutions should regularly perform self-assessments of their operational risk and controls. The assessment should evaluate inherent risk, effectiveness of the control environment, and residual risk.
The assessments may utilise business process mapping to identify key steps in business processes, activities, and organisational functions, as well as associated risks and areas of control weakness. The assessments should contain sufficiently detailed information on the business environment, operational risks, underlying causes, controls and evaluation of control effectiveness to enable an independent reviewer to determine how the bank reached its ratings.
The risk register should be maintained to form a meaningful view of the overall effectiveness of controls and facilitate oversight by senior management, risk committees, and the board of directors.
 - iv. Control monitoring and Assurance Framework - Institutions should incorporate an appropriate control monitoring and assurance framework to facilitate a structured approach to the evaluation, review and ongoing monitoring and testing of the control environment.

- v. Metrics - Using operational risk event data and risk and control assessments, institutions should develop metrics to assess and monitor their operational risk exposure. These metrics should provide early warning information to monitor ongoing performance of the business and the control environment, and to report the operational risk profile. Institutions should monitor metrics and related trends against agreed thresholds or limits to provide valuable information for risk management and reporting purposes.
 - vi. Scenario Analysis - institutions should use scenario analysis to identify, analyse and measure a range of scenarios, including low probability and high severity events, which could result in severe operational risk losses. The scenario analysis process should be used to develop a range of consequences of potential events, including impact assessments for risk management purposes. Scenario analysis should also be integrated into disaster recovery, and business continuity plans to test operational resilience. Given the subjectivity of the scenario analysis, a robust governance framework and independent review should be conducted to ensure the integrity and consistency of the process.
 - vii. Benchmarking and comparative analysis - Institutions should perform benchmarking and comparative analysis to assess the outcomes of different risk measurement and management tools and compare their risk metrics with those of peer institutions. Such analysis enhances understanding of the institution's operational risk profile, validates the effectiveness of risk assessment processes, and helps identify areas for improvement. For example, comparing internal loss data with self-assessment results can highlight weaknesses in risk assessments, while comparing scenario analysis outcomes with internal and external loss data can provide insights into the potential severity of operational risk exposures.
- c) Institutions should ensure that the operational risk assessment tools' output is based on accurate data, whose integrity is ensured by strong governance and robust verification and validation procedures and subject to corporate operational risk function monitored action plans or remediation plans.

Principle 7: Change Management

Senior management should ensure that the bank's change management process is comprehensive, appropriately resourced and adequately articulated between the three lines of defence.

An institution's operational risk exposure evolves when a bank initiates change, such as engaging in new activities or developing new products or services; entering into unfamiliar markets or jurisdictions; and implementing new or modifying business processes. Change

management should assess and monitor associated risks throughout their lifecycle, from initiation to termination, including across all stages of a product, process, or activity. Sound change management requires the following:

- a) Institutions should have policies and procedures defining the process for identifying, managing, challenging, approving and monitoring change based on agreed objective criteria. Change implementation should be monitored by specific oversight controls. Change management policies and procedures should be subject to independent and regular review and update, and clearly allocate roles and responsibilities in accordance with the three-lines-of-defence model, in particular:
 - i) The first line of defence should perform operational risk and control assessments of new products, activities, processes and systems, including the identification and evaluation of the required change through the decision-making and planning phases to the implementation and post-implementation review.
 - ii) The second line of defence (independent corporate operational risk function) should challenge the operational risk and control assessments of the first line of defence, as well as monitor the implementation of appropriate controls or remediation actions. corporate operational risk function should cover all phases of this process. In addition, the corporate operational risk function should ensure that all relevant control groups (e.g. finance, compliance, legal, business, ICT, risk management) are involved in this process.
- b) A bank should have policies and procedures on the review and approval of new products, activities, processes and systems. The review and approval process should consider:
 - i) Inherent risks including legal, ICT and model risks - in the launch of new products, services, activities, and operations in unfamiliar markets, and in the implementation of new processes, people and systems especially when outsourced.
 - ii) Changes to the bank's operational risk profile, appetite and tolerance, including changes to the risk of existing products or activities.
 - iii) The necessary controls, risk management processes, and risk mitigation strategies.
 - iv) The residual risk.
 - v) Changes to relevant risk thresholds or limits.
 - vi) The procedures and metrics to assess, monitor, and manage the risk of new products, services, activities, markets, jurisdictions, processes and systems.
- c) The review and approval process should ensure that adequate human and technology resources are in place before changes are implemented. Further, all changes should also be monitored during and after implementation to identify and address any material deviations from the expected operational risk profile

- d) Institutions should maintain a central record of their products and services to the extent possible (including the outsourced ones) to facilitate monitoring of changes.

Principle 8: Monitoring and Reporting

Senior management should implement a process to regularly monitor operational risk profiles and material operational exposures. Appropriate reporting mechanisms should be implemented at the board of directors, senior management, and business unit levels to support proactive management of operational risk.

- a) A bank should ensure that its reports are comprehensive, accurate, consistent and actionable across business units and products.
- b) The first line of defence should ensure reporting on any residual operational risks, including operational risk events, control deficiencies, process inadequacies, and non-compliance with operational risk tolerances.
- c) Operational risk reports should be manageable in scope and volume by providing an outlook on the institution's operational risk profile and adherence to the operational risk appetite and tolerance statement.
- d) Reporting should be timely, and an institution should be able to produce reports in both normal and stressed market conditions.
- e) The frequency of reporting should reflect the risks involved and the pace and nature of changes in the operating environment.
- f) The results of monitoring activities should be included in regular management and board reports, as should assessments of the operational risk management framework performed by the internal/external audit and/or risk management functions.
- g) Reports generated by or for supervisory authorities should also be reported internally to senior management and the board of directors, where appropriate.
- h) Operational risk reports should describe the operational risk profile of the institution by providing internal financial, operational, and compliance indicators. It should also include external market or environmental information about events and conditions that are relevant to decision-making. This should include:
 - i) Breaches of the institution's risk appetite and tolerance statement, as well as thresholds, limits or qualitative requirements.
 - ii) A discussion and assessment of key and emerging risks.
 - iii) Details of recent significant internal operational risk events and losses (including root cause analysis).
 - iv) Relevant external events or regulatory changes and any potential impact on the institution.
- i) Data capture and risk reporting processes should be analysed periodically to enhance risk management performance as well as advance risk management policies, procedures and practices.

Principle 9: Control and Mitigation

Institutions should have a strong control environment that utilises policies, processes and systems, appropriate internal controls, and appropriate risk mitigation and/or transfer strategies.

- a) Internal controls should be designed to provide reasonable assurance that an institution will have efficient and effective operations, safeguard its assets, produce reliable financial reports, and comply with applicable laws and regulations.
- b) A sound internal control programme consists of four components that are integral to the risk management process. This includes risk assessment, control activities, information and communication, and monitoring activities.
- c) Control processes and procedures should include a system for ensuring compliance with policies, regulations and laws. Examples of principal elements of a policy compliance assessment are:
 - i) Reviews of progress towards stated objectives.
 - ii) Verification of compliance with management controls.
 - iii) Review of the treatment and resolution of instances of non-compliance.
 - iv) Evaluation of the required approvals and authorisations to ensure accountability to an appropriate level of management.
 - v) Tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy, regulations and laws.
- d) Control processes and procedures should address how an institution ensures operational resilience is maintained in both normal circumstances and in the event of disruption, reflecting respective functions' due diligence, consistent with an institution's operational resilience approach.
- e) An effective control environment also requires appropriate segregation of duties. Areas where conflicts of interest may arise should be identified, minimised, and be subject to careful independent monitoring and review.
- f) In addition to segregation of duties and dual controls, institutions should ensure that the following internal controls are in place:
 - i) Clearly established authorities and/or processes for approval.
 - ii) Close monitoring of adherence to assigned risk thresholds or limits.
 - iii) Safeguards for access to, and use of, the institution's assets and records.
 - iv) Appropriateness of staffing level and training to maintain technical expertise.
 - v) Ongoing processes to identify business units or products where returns appear to be out of line with reasonable expectations.

- vi) Regular verification and reconciliation of transactions and accounts.
 - vii) The vacation policy provides for officers and employees to be absent from their duties for a period of not less than two consecutive weeks.
- g) Institutions should ensure effective use and sound implementation of technology, which can contribute to a robust control environment. Automated processes are less prone to error than manual processes. However, automated processes introduce risks that must be addressed through sound technology governance and infrastructure risk management programmes.
- h) The use of technology-related products, activities, processes and delivery channels exposes an institution to operational risk and the possibility of material financial loss. Consequently, an institution should have an integrated approach to identifying, measuring, monitoring and managing technology risks along the same precepts as operational risk management.
- i) The board of directors and senior management are responsible for understanding the operational risks associated with third-party service providers and outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Amongst others, the concentration of risk and the complexity of outsourcing should be taken into account. Third-party risk policies should comprise the following:
- i) Procedures for determining whether and how activities can be outsourced.
 - ii) Processes for conducting due diligence in the selection of potential service providers.
 - iii) Sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights.
 - iv) Programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider.
 - v) Effective control environment at the institution and the service provider, which should include a register of outsourced activities and metrics and reporting to facilitate oversight of the service provider.
 - vi) Development of viable contingency plans.
 - vii) Execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the institution.
 - viii) Institutions' supervisory and resolution authorities' access to third parties.
- j) In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, the following should be implemented:
- Management should complement controls by seeking to transfer the risk to another party, such as through insurance.

- The board of directors should determine the maximum loss exposure the institution is willing and has the financial capacity to assume and should perform an annual review of the institution's risk and insurance management programme.
 - Institutions should view risk transfer tools as complementary rather than a replacement for thorough internal operational risk control. Having mechanisms in place to quickly identify, recognise and rectify distinct operational risk errors can greatly reduce exposures.
- k) Institutions should have unified classification, methodology, and procedures of operational risk management established by the independent corporate operational risk function.

Principle 10: Information and Communication Technology

Institutions should implement a robust ICT risk management programme in alignment with their operational risk management framework.

- a) Effective ICT performance and security are paramount for an institution to conduct its business properly. The appropriate use and implementation of sound ICT risk management contribute to the effectiveness of the control environment. It is fundamental to the achievement of an institution's strategic objectives.
- b) An institution's ICT risk assessment should ensure that its ICT infrastructure fully supports and facilitates its operations. ICT risk management should reduce an institution's operational risk exposure to direct losses, legal claims, reputational damage, ICT disruption and misuse of technology in alignment with its risk appetite and tolerance statement.
- c) ICT risk management includes:
- i) ICT risk identification and assessment.
 - ii) ICT risk mitigation measures consistent with the assessed risk level (e.g., cybersecurity, response and recovery programmes, ICT change management processes, ICT incident management processes, including relevant information transmission to users on a timely basis).
 - iii) Monitoring of mitigation measures.
- d) The board should oversee the effectiveness of ICT risk management, while senior management should regularly assess the adequacy of ICT controls and processes.

- e) ICT risk and strategies should be aligned with the institution's risk appetite and applicable legal requirements. ICT risks, controls, and incidents should be continuously monitored and regularly reported to the Board and senior management.
- f) ICT risk management together with complementing processes set by the institutions should:
 - i) Be reviewed regularly for completeness against relevant industry standards and best practices as well as against evolving threats (e.g. cyber) and evolving or new technologies;
 - ii) Be regularly tested as part of a programme to identify gaps against stated risk tolerance objectives and facilitate improvement of the ICT risk identification, protection, detection and event management; and
 - iii) Make use of actionable intelligence to continuously enhance their situational awareness of vulnerabilities to ICT systems, networks and applications and facilitate effective decision-making in risk or change management.
- g) Institutions should prepare for ICT disruptions and stress scenarios. This includes supporting remote access, rapid deployment of resources, increased network capacity, and customer data protection. Institutions should ensure that:
 - i) Appropriate risk mitigation strategies are developed for potential risks associated with disruption or compromise of ICT systems, networks and applications. Institutions should evaluate whether the risks taken together with these strategies fall within the institution's risk appetite and risk tolerance;
 - ii) Well-defined processes for the management of privileged users and application development are in place; and
 - iii) Regular updates are made to ICT, including cyber security, to maintain an appropriate security posture.

Principle 11: Business Continuity Planning

Institutions should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption. Business continuity plans should be linked to the institution's operational risk management framework.

- a) Sound and effective governance of Institutions' business continuity policy requires:
 - i) Regular review and approval by the board of directors.
 - ii) The strong involvement of the senior management and business unit leaders in its implementation.
 - iii) The commitment of the first and second lines of defence to its design.

- iv) Regular review by the third line of defence.
- b) Institutions should prepare forward-looking business continuity plans with scenario analyses associated with relevant impact assessments and recovery procedures. In particular:
 - i) An institution should ground its business continuity policy on scenario analyses of potential disruptions that identify and categorise critical business operations and key internal or external dependencies. In doing so, institutions should cover all their business units as well as critical providers and major third parties.
 - ii) Each scenario should be subject to a quantitative and qualitative impact assessment or business impact analysis (BIA) with regard to its financial, operational, legal and reputational consequences.
 - iii) Disruption scenarios should be subject to thresholds or limits, such as maximum tolerable outage, for the activation of a business continuity procedure.
 - iv) The procedure should address resumption aspects, set recovery time objectives (RTO) and recovery point objectives (RPO) as well as communication guidelines for informing management, employees, regulatory authorities, customers, suppliers, and all other relevant stakeholders.
- c) An institution should periodically review its business continuity plans and policies to ensure that contingency strategies remain consistent with current operations, risks and threats.
- d) Training and awareness programmes should be customised based on specific roles to ensure that staff can effectively execute contingency plans.
- e) Business continuity procedures should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, an institution should participate in business continuity testing with key service providers. Results of formal testing and review activities should be reported to senior management and the board of directors.

Principle 12: Role of Disclosure

An institution's public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure.

- a) An institution's public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of an institution's operations, and evolving industry practice.

- b) Institutions should disclose relevant operational risk exposure information to their stakeholders, including significant operational loss events. However, institutions should be careful not to create operational risk through this disclosure, e.g. description of unaddressed control vulnerabilities.
- c) An institution should disclose its independent corporate operational risk function in a manner that allows stakeholders to determine whether the institution identifies, assesses, monitors and controls/mitigates operational risk effectively.
- d) Institutions should have a formal disclosure policy that is subject to regular and independent review and approval by the senior management and the board of directors. The policy should address the institution's approach for determining what operational risk disclosures it will make and internal controls over the disclosure process. In addition, institutions should implement a process for assessing the appropriateness of their disclosures and disclosure policy.

3.4 PRINCIPLES OF OPERATIONAL RESILIENCE

Effective operational resilience requires good governance, robust risk management, robust business continuity management, critical mapping, sound third-party risk management, incident handling, and robust information and communication technology and cybersecurity.

Principle 1: Governance

An Institution should utilise its existing governance structure to establish, oversee and implement an effective operational resilience approach that enables it to respond and adapt to, as well as recover and learn from disruptive events to minimise their impact on delivering critical operations through disruption.

- a) The board of directors should review and approve the institution's operational resilience approach considering the institution's risk appetite and tolerance for disruption to its critical operations.
- b) Senior management, under the Board's oversight, should ensure effective implementation of the institution's operational resilience framework and provide adequate resources to support it.
- c) An institution should provide formal operational resilience management information (MI) to its board on a regular basis and in the event of a disruption. The operational resilience MI should be embedded into the existing reporting structure in an adequate, meaningful and timely manner. An escalation matrix should be established for reporting identified vulnerabilities and unexpected disruptions.

- d) The board is responsible for the approval of the operational resilience framework and approval of critical business services, impact tolerances, business service maps and scenario testing to ascertain the institution's ability to remain within impact tolerances, and communication plans.
- e) The board should oversee senior management assessments of the components of the operational resilience framework.
- f) The board is responsible for review and approval of the assessments of its critical business services, impact tolerances, business service maps and scenario analysis annually and lessons learned from the exercise after a disruption has occurred.
- g) The board should review the components of the operational resilience framework at least annually, through a documented self-assessment to confirm that there are no undetected developing weaknesses.

Principle 2: The Operational Resilience Framework

The Operational Resilience Framework should be embedded within an institution's overall Governance and Risk Management Framework.

- a) An institution should utilise its existing governance and risk management structures when implementing an effective operational resilience framework.
- b) An institution should ensure that its existing governance frameworks and committee structures include responsibilities with respect to operational resilience.
- c) Operational resilience and operational risk are separate disciplines and should be treated as such. Operational resilience is an evolution of operational risk, providing a holistic institution-wide approach to managing disruptions to critical business services.
- d) Institutions should manage operational resilience and operational risk through distinct yet aligned frameworks, where operational resilience focuses on identifying the most critical services and guided response during disruptions, and operational risk focuses on the management and control of risks that could impact operations.
- e) An institution should develop a documented operational resilience framework aligned with its operational risk and business continuity framework.
- f) Since operational resilience draws from elements of business continuity, third-party risk management, ICT risk management, incident management, and wider aspects of

operational risk management, a holistic approach is essential if an institution is to enhance the resilience of its business services.

Principle 3: Operational Risk Management

An institution should leverage its respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with its operational resilience approach.

- a) The institution's operational risk management function should work alongside other relevant functions to manage and address any risks that threaten the delivery of critical operations. An institution should coordinate its business continuity planning, third-party dependency management, recovery and resolution planning and other relevant risk management frameworks to strengthen operational resilience.
- b) An institution should have sufficient controls and procedures to identify and assess threats and vulnerabilities in a timely manner and prevent them from affecting delivery of critical operations. The respective functions should regularly assess the effectiveness of the implemented controls and procedures. Assessments should be conducted following changes to critical operations and after occurrence of incidents, to incorporate lessons learned and address new threats and vulnerabilities.
- c) An institution should use its change management framework to assess how proposed changes may impact critical operations and their interconnections.

Principle 4: Identification of Critical Business Services

The starting point for any institution in enhancing its operational resilience is to set the criteria for defining its critical business services. The Board should review and approve the criteria for critical business services.

- a) It is the responsibility of the Board to approve clearly defined and documented criteria for determining how business services are classified as critical. The criteria should enable an institution to identify its critical business services and prioritise them in the event of disruption. This should be achieved by considering the impact that a disruption to a critical business service would pose to its external end users through three lenses:
 - (i) impact on customer;
 - (ii) impact on the institution's viability, safety and soundness; and
 - (iii) impact on the overall financial stability.
- b) The Board should approve the criteria for identifying critical business services annually and whenever material business changes occur.

- c) Institutions should focus on the end-to-end delivery chain of critical business services, rather than protecting individual systems, processes, or functions.
- d) An institution should implement controls to safeguard its critical business services and ensure their uninterrupted delivery to end users during a disruption.
- e) Critical business services are external-facing and should have an identifiable external end user.
- f) An institution should leverage its existing business functions' knowledge when identifying and prioritising critical business services.
- g) Since critical business services will differ between institutions, institutions should take an outcome-based approach to the identification of these services.
- h) It is the responsibility of the board to review and approve all business services classified as critical at least annually.
- i) Critical business services should be identified to enable an institution to:
 - i. Clearly determine impact tolerances based on maximum acceptable levels of disruption.
 - ii. Perform mapping of the end-to-end delivery of the business service, including any dependence on third parties.
 - iii. Perform tests based on severe but plausible scenarios.
- j) An institution should assess whether the number of critical business services is proportionate to the nature, scale and complexity of its business.

Principle 5: Setting Impact Tolerances and Impact Tolerance Metrics

Impact tolerances and impact tolerance metrics should be set for each critical business service.

An institution should develop impact tolerances and impact tolerance metrics for each of its critical business services on the assumption that disruptive events will happen.

A. Impact Tolerances

- a) The purpose of an impact tolerance is to determine the maximum acceptable level of disruption to a critical business service.
- b) Impact tolerances should be set at the point where a disruption could threaten the institution's viability, cause significant customer harm, or adversely affect the safety and soundness of the financial system.
- c) Breach of impact tolerance indicates that service disruption has reached a point of irreversible damage to customers, the bank, or broader financial stability.
- d) Impact tolerances should be used as a planning tool for an institution rather than as a tool to measure regulatory compliance.
- e) Impact tolerances enable an institution to understand its level of operational resilience in the event of an unplanned disruption.
- f) Impact tolerances are designed to determine the schedule by which an institution should be able to restore delivery of critical business services after a disruption has occurred.
- g) Impact tolerances should be tested against severe but plausible scenarios to ensure they remain appropriate and that the institution can operate within them during a disruption.

- h) The Central Bank expects an institution's board to review and approve impact tolerances at least annually, or following a disruption, to ensure they remain fit for purpose.
- i) Institutions should establish impact tolerances for critical business services using approved criteria and existing resilience measures, such as Business Impact Analysis (BIA), Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and Maximum Tolerable Outage (MTO). These metrics measure the disruption of single points of failure that feed into the delivery of a critical business service.

B. Impact Tolerance Metrics

- a) An institution should set at least one impact tolerance metric for each of its critical business services.
- b) At a minimum, there should be a time-based metric indicating the maximum acceptable duration a critical business service can withstand disruption.
- c) Impact tolerance metrics should be clear and measurable and can be both qualitative and quantitative. To achieve this, they should reference specific outcomes and measurements.
- d) An institution should be able to determine the outcome if the impact tolerances are exceeded.
- e) The metrics should be time-based to ensure that an institution focuses its response to disruption on the continuity of its critical business services.
- f) To be prepared to withstand more than one type of disruption, an institution should also have impact tolerance metrics based on:
 - i. The maximum tolerable number of customers affected by a disruption;
 - ii. The maximum number of transactions affected by a disruption;
 - iii. The maximum value of transactions impacted.
 - iv. Any other metric based on the institution's impact tolerance metrics, based on their specific critical business services, taking into account the nature, scale and complexity of the institution.

Principle 6: Business Continuity Planning and Testing

An institution should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test its ability to deliver critical operations through disruption.

- a) Business Continuity Management (BCM) should be fully integrated into the overarching operational resilience framework and linked to the institution's risk appetite.
- b) Continuity of business services should be forward-looking. While operational resilience is much broader than BCM and recovery, approved business continuity plans should be utilised as part of the holistic response to disruption.
- c) Whereas BCM focuses on single points of failure, such as individual systems, people or processes, operational resilience should go a step further by determining how these single

points of failure have the potential to affect the end-to-end delivery of critical business services.

- d) When a disruption occurs to an institution's critical business services, the Business Continuity Plan (BCP) should be enacted as part of the response process.
- e) For BCM to be aligned with the Operational Resilience Framework, the BCPs should be tested through severe but plausible scenarios and include any third-party interdependencies or interconnections.
- f) To respond effectively to a disruption, an integrated BCP should incorporate invocation processes, impact analyses, recovery strategies, training programmes and crisis management programmes to guide the management of a disruption and limit the impact.
- g) An institution should adopt a holistic approach to BCM by mapping critical business services and developing a recovery plan in line with approved impact tolerances.
- h) Key personnel should be identified and have completed the necessary training. Training and awareness programmes should be customised based on specific roles to ensure that staff can effectively execute contingency plans when responding to a disruption.
- i) Institutions should ensure that third-party arrangements supporting critical business services are resilient, reviewed regularly, and tested at least annually to confirm compliance with impact tolerances.
- j) The institution should consider identifying the dependencies that can be substituted in the event of unexpected disruption.
- k) Institutions should put in place adequate measures to ensure digital resilience in relation to ICT business continuity management.

Principle 7: Mapping Interconnections and Interdependencies

Once an institution has identified its critical operations, it should map the internal and external interconnections and interdependencies that are necessary for the delivery of critical operations consistent with its approach to operational resilience.

- a) An institution should understand and map out how its critical business services are delivered. The respective functions should map the people, technology, processes, information, facilities, and the interconnections and interdependencies required to deliver the institution's critical operations.
- b) To ensure that a critical business service can remain within its impact tolerance(s), an institution should understand how the services are delivered and how each service can be disrupted.
- c) An institution should understand the chain of activities that contribute to the delivery of each of its critical business services in order to be able to identify any critical or single points of failure, dependencies, or key vulnerabilities.
- d) An institution should identify, document and map the necessary people, processes, information, technology, facilities, and third-party service providers required to deliver

each of its critical business services. This exercise should be undertaken collaboratively across business units to ensure comprehensive mapping.

- e) Mapping should be conducted at a level of detail that enables identification of the resources that contribute to the delivery of each stage of the service and their importance. An institution should understand how these resources work in combination to deliver critical business services.
- f) The approach and level of granularity of mapping should be sufficient for an institution to identify vulnerabilities and key dependencies, and to support testing of its ability to stay within the assigned impact tolerances for each critical business service.
- g) Comprehensive mapping of a service should enable an institution to pinpoint vulnerabilities in critical business services and determine where recovery and resolution plans can be leveraged.
- h) Institutions should use their recovery and resolution plans to identify critical operations and ensure that their operational resilience framework is aligned with mapping of critical operations and critical third-party services.
- i) Mapping should be detailed enough to identify vulnerabilities and support testing of critical operations against the institution's risk appetite and tolerance for disruption.

Principle 8: Third-party Dependency Management

An institution should manage its dependencies on relationships with third-party service providers and intragroup entities for delivery of critical operations.

- a) An institution should conduct risk assessments and due diligence before entering into arrangements with third parties or intragroup entities, in line with its operational risk management framework, third-party risk management policy, and operational resilience framework.
- b) An institution should ensure that third-party and intragroup service providers have adequate operational resilience to support critical operations during normal operations and disruptions before entering into any arrangement.
- c) Complex third-party interdependencies should be adequately managed since they expose institutions to external disruptions, even when internal systems are unaffected.
- d) A complicated network of outsourced activities reduces visibility over potential vulnerabilities in the delivery of critical business services. This can hamper an institution in preparing for an operational disruption; therefore, institutions should capture these dependencies as part of the mapping process.
- e) An institution should manage its dependencies on relationships, including those of third parties involved in the delivery of critical business services.
- f) Dependencies should be clearly identified and detailed in the mapping of critical business services. An institution's critical business services should be able to remain within impact tolerances, including when they rely on third-party service providers. The Board and senior management should be cognizant of the fact that when entering into outsourcing

arrangements, they are creating a dependency on a third party for the resilience of their institution.

- g) An institution should undertake due diligence in respect of its third-party service providers prior to entering into an outsourcing arrangement, to ensure that third-party arrangements have appropriate operational resilience conditions that enable the institution to remain within its impact tolerances.
- h) An institution should ensure that legally binding written agreements are in place with third parties that detail how the critical services will be maintained during a disruption, and how an exit strategy, if or when the service cannot be maintained, is executed.
- i) An institution should take into account the geographical location of the third party, which may impact the provision of service depending on the nature or location of the event.
- j) An institution should identify the data and ICT assets that support critical business functions and services. It should understand the related ICT risk dependencies and maintain a register of ICT third-party service providers to support effective mapping and risk management.
- k) Institutions should establish continuity plans, exit strategies, and contingency measures to maintain operational resilience during third-party failures.
- l) Scenario testing must evaluate third-party substitutability and alternative recovery options, including insourcing critical functions.
- m) The Central Bank may assess systemic operational vulnerabilities, concentration risks and sector-wide operational resilience threats.

Principle 9: Incident Management

An institution should develop and implement response and recovery plans to manage incidents that could disrupt delivery of critical operations in line with the institution's risk appetite and tolerance for disruption. An institution should continuously improve its incident response and recovery plans by incorporating the lessons learned from previous incidents.

- a) Incident management is an essential component of being operationally resilient.
- b) Operational resilience requires an institution to have an approach to incidents that covers the full life cycle of an event, from classification of incidents that trigger approved response procedures, to testing the incident management procedures and reflecting on lessons learned from incidents.
- c) Incident management should be aligned with the operational resilience framework. An institution should develop and implement response and recovery plans and procedures to manage incidents that have the potential to disrupt the delivery of critical business services.
- d) Incident management plans should be developed to consider how disruption can affect an institution's risk appetite and impact tolerance metrics.
- e) An institution should maintain an inventory of incident response and recovery, internal and third-party resources to support the institution's response and recovery capabilities.
- f) Incident response and recovery procedures should be reviewed, tested and updated at least annually.

- g) Root causes should be identified and managed to prevent the serial recurrence of incidents.
- h) Lessons learned from previous incidents should be reflected when updating the incident management program, and learnings from incidents should be considered as part of scenario testing.
- i) An institution's incident management program should manage all incidents impacting or potentially impacting the institution.
- j) All operational incidents should be reported to the Central Bank in accordance with the requirements indicated in this Guideline.
- k) An institution should ensure compliance with the Central Bank of Kenya Guidance Note on Cybersecurity, requirements on reporting of cybersecurity and ICT-related incidents to the Central Bank.

Principle 10: Information Communication Technology and Cyber Security Risk Management

An institution should ensure resilient Information Communication Technology (ICT), including cybersecurity, that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant and timely information for risk management and decision-making processes to fully support and facilitate the delivery of the institution's critical operations.

- a) An institution should have a documented ICT and cybersecurity policy covering governance, risk ownership, key security controls (such as access controls, identity management and critical information asset protection), ongoing control monitoring, incident response, and business continuity plans.
- b) An institution should identify its critical information assets and the infrastructure upon which it depends.
- c) An institution should prioritise cybersecurity controls based on its ICT risk assessments and the criticality of assets to its core operations, while ensuring compliance with data protection and confidentiality laws.
- d) Institutions should ensure data integrity during cyber incidents through secure storage and offline, immutable backups for critical operations.
- e) An institution should regularly evaluate the threat profile of its critical information assets, test vulnerabilities and ensure its resilience to ICT-related risks.

Principle 11: Scenario Testing

An institution should document and test its ability to remain within impact tolerances during severe but plausible scenarios.

- a) An institution should test its ability to remain within its impact tolerances for every critical business service through severe but plausible scenarios.
- b) Testing should have clear and detailed maps developed for critical business services.

- c) An institution should identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the potential risks to delivery of the critical business services.
- d) An institution that implements changes more regularly should undertake more frequent testing. This should be done annually for all institutions.
- e) An institution should consider various testing methods, such as paper-based or simulation testing on a number of critical business services.
- f) A scenario test should identify any vulnerabilities or reliance on third parties. The results should focus on resolvability of a vulnerable element, determine alternative channels of delivery or identify the elements that can be substituted if disrupted.
- g) Institutions should develop and document a testing plan, including the scope, procedures, and outcomes of the exercise, and ensure that lessons learned are addressed through appropriate corrective actions. This provides greater assurance that the institution has adequate contingency plans to prepare for, respond to, recover from, and learn from operational disruptions.
- h) An institution's board should review the results of all scenario testing carried out on critical business services.
- i) If the scenario testing indicates that impact tolerances could be breached, the board and senior management should take appropriate action to strengthen the resilience of the affected business service and allocate resources where necessary.
- j) The design and implementation of remediation plans are the responsibility of senior management, and the results of the remediation plans should be reviewed and approved by the board thereafter.

Principle 12: Communication Plans

Internal and External Crisis Communication plans should be fully integrated into the overarching Operational Resilience Framework.

- a) A crisis communication plan should be developed either as part of an institution's Operational Resilience Framework or contained in the Business Continuity Management or recovery plans to communicate effectively during a disruption.
- b) A key part of an effective crisis communications plan is the identification and preparation of key resources and experts that can be leveraged when a disruption occurs. This will aid in the mitigation of the harm caused during disruption.
- c) The institution should develop internal and external communication plans and stakeholder maps that can be implemented during a disruption.
- d) The internal communication plan should contain escalation matrices on communication with key decision-makers, operational staff and third parties if necessary.
- e) The external communication plan should outline how the institution will communicate with its customers, stakeholders and regulators during a disruption.

Principle 13: Lessons Learned Exercise and Continuous Improvement

An institution should conduct a lessons learned exercise after any disruption of a critical business service. This includes any potential material disruption to a third-party service provider that feeds into the delivery of a critical business service.

- a) The lessons learned exercise should utilise the information gathered as part of the incident management or disaster recovery process.
- b) The decisions and recovery processes determined to be appropriate throughout the incident management process should form the basis of the lessons learned exercise.
- c) The lessons learned exercise allows an institution to reflect on the three-pillar approach to operational resilience and allows for feedback into the first two pillars that encourage improvement in how an institution prepares for and recovers from disruptions.
- d) An institution should have predetermined criteria or questions that form the basis of the lessons learned exercise. These questions should identify deficiencies that caused failure in continuity of service.

Specifically, at a minimum, the following should be considered:

- How and why the incident occurred;
 - The identified vulnerabilities;
 - The impact on the delivery of critical business services;
 - Whether the risk controls, decisions, recovery processes and communications were appropriate; and
 - The speed of recovery and whether the impact tolerances are adequate.
- e) The lessons learned exercises should define effective remediation measures to redress deficiencies and failures in the continuity of service. Doing so will allow an institution to agree on remedial actions and adjust any impact tolerances, if determined. This should all be contained within a self-assessment document and presented to the board.
 - f) Continuous improvements to operational resilience require an institution to learn from its experiences. This should not only occur after a disruption has occurred but should form part of ongoing operational resilience governance discussions.
 - g) An institution should promote an effective culture of learning and continuous improvement as operational resilience evolves.

3.5 RESPONSIBILITIES OF THE BOARD OF DIRECTORS

The Board of Directors shall have ultimate responsibility for overseeing the institution's operational risk and operational resilience frameworks and ensuring that the institution remains capable of delivering critical operations through disruption. In carrying out this responsibility, the Board shall:

- i. Approve and periodically review the bank's operational risk management and operational resilience frameworks, strategies, policies, risk appetite and tolerance limits, consistent with the bank's size, complexity, business model and risk profile.
- ii. Approve and periodically review the bank's tolerance for disruption to critical operations, based on a range of severe but plausible operational risk scenarios.
- iii. Require management to put in place a framework for identification of critical operations and appropriate measures to protect the people, processes, technology, information, facilities and third parties necessary for their continued delivery during disruption.
- iv. Receive and review regular reports on operational risk exposures, significant incidents and losses, emerging risks, breaches of risk appetite or tolerance, operational resilience and the effectiveness of key risk mitigants.
- v. Require management to use operational loss data, near misses, key risk indicators and scenario analysis to assess the bank's operational risk profile and strengthen controls.
- vi. Require regular testing and exercising of business continuity, disaster recovery, incident response and operational resilience arrangements, and require timely remediation of material weaknesses identified.
- vii. Hold Senior Management accountable for effective implementation of the approved operational risk and operational resilience frameworks, adequate resourcing and timely remediation of material weaknesses.
- viii. Require timely and accurate reporting to CBK of material operational risk events, significant losses, major ICT or cyber incidents, disruptions to critical operations and other matters required under the regulatory framework.

3.6 RESPONSIBILITIES OF SENIOR MANAGEMENT

Senior management shall be responsible for the effective implementation, administration and continuous enhancement of the institution's operational risk management and operational resilience framework. In particular, senior management should:

- i. Implement the Board-approved operational risk management and operational resilience frameworks, risk appetite and tolerance limits, and establish clear policies, procedures, controls and responsibilities.
- ii. Identify, assess, monitor and manage operational risks arising from people, processes, systems, technology, external events, fraud, legal matters and third-party dependencies across the bank.
- iii. Maintain reliable processes for collecting, validating and analysing operational loss-event data, including significant losses and near misses, and use the findings to identify root causes and strengthen controls.
- iv. Conduct regular scenario analysis and testing under severe but plausible conditions to assess the bank's ability to respond to, adapt to and recover from disruptions affecting critical operations.

- v. Identify and map critical operations and their key dependencies, and maintain appropriate response, continuity, recovery and exit arrangements to support their delivery through disruption.
- vi. Monitor and report to the Board on operational risk exposures, key risk indicators, loss events, major incidents, emerging risks, resilience capabilities, breaches of risk appetite or tolerance and remediation progress.
- vii. Ensure that operational risks associated with new products, processes, technologies, material changes, outsourcing and third-party arrangements are assessed and appropriately managed before implementation.
- viii. Escalate and report material operational risk events, significant losses, major ICT or cyber incidents and disruptions to critical operations to the Board and CBK within the required timelines and ensure timely remediation of identified weaknesses.

PART IV: REPORTING ON OPERATIONAL RISK AND OPERATIONAL RESILIENCE

4.1 Incident Reporting

Institutions shall establish formal processes for the identification, escalation, recording, monitoring and reporting of operational resilience incidents.

The incident management framework shall:

- i. Define incident classification and severity criteria;
- ii. Establish escalation thresholds and reporting timelines;
- iii. Maintain a centralised register of operational resilience incidents;
- iv. Record root causes, business impacts, affected services, corrective actions and recovery outcomes;
- v. Track incidents affecting important business services and breaches of impact tolerances;
- vi. Monitor recurring incidents and emerging trends;
- vii. Ensure lessons learned are incorporated into risk management and resilience enhancement programmes;
- viii. Maintain adequate management information systems to support incident monitoring and reporting;
- ix. Material operational incidents shall be reported promptly to Senior Management, the Board and Central institution;
- x. Reporting to the Central Bank shall be within 24 hours and on a quarterly basis using the format in **Annex 1**. These reports shall be submitted together with the ICT and cybersecurity incident reports in accordance with the requirements of the CBK Guideline Note on Cybersecurity; and
- xi. Institutions shall periodically analyse incident data to identify systemic weaknesses, emerging risks and opportunities for strengthening operational resilience.

4.2 Operational Resilience Self-Assessment

Institutions should conduct periodic self-assessments of their operational resilience capabilities and preparedness and submit a report to senior management and the Board of Directors. The self-assessment shall evaluate:

- i. The effectiveness of governance and accountability arrangements;
- ii. The identification and criticality assessment of Important Business Services;
- iii. Compliance with approved impact tolerances;
- iv. Adequacy of resource mapping and dependency management;
- v. Resilience of ICT systems and critical infrastructure;
- vi. Third-party and outsourcing resilience arrangements;
- vii. Results of scenario testing and lessons learned;
- viii. Incident response and recovery capabilities; and
- ix. Progress in addressing identified vulnerabilities and control weaknesses.

The results of the self-assessment shall be documented, approved by Senior Management, and reported to the Board at least annually. Institutions shall maintain action plans to address gaps identified during self-assessments.

4.3 Operational Stress Testing and Vulnerability Assessment

An institution shall conduct regular operational stress testing and vulnerability assessments to assess its ability to remain within established impact tolerances during severe but plausible disruption events.

Operational stress testing scenarios and vulnerability assessments should be risk-based, forward-looking, proportionate to the institution's nature, size and complexity.

Operational stress testing scenarios and vulnerability assessments shall, at a minimum, include the following:

- i. Cybersecurity incidents, including cyber-attacks and vulnerability exploitation;
- ii. ICT systems and telecommunications outages;
- iii. Cloud service provider disruptions or failures;
- iv. Critical third-party and outsourced service provider failures;
- v. Business continuity disruptions affecting the institution's ability to deliver critical operations;
- vi. Physical infrastructure disruptions, including power, premises, and utility failures; and
- vii. Workforce disruption events, including pandemics, industrial action, loss of key personnel, or other events affecting the availability of critical staff.

Institutions shall also consider other plausible internal and external scenarios that could materially impair their operational resilience, commensurate with the nature, scale, complexity, and risk profile of their operations.

Institutions shall periodically undertake reverse stress testing to identify circumstances that could result in failure to remain within established impact tolerances.

The Central Bank may require institutions to participate in sector-wide resilience exercises and simulations.

All material vulnerabilities identified through testing shall be documented, risk-rated, remediated within defined timelines, and escalated to senior management and the Board where appropriate.

PART V: 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 VI: EFFECTIVE DATE

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

ENQUIRIES

Any enquiries 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*

ANNEX I

Operational Risk Incident Report (Quarterly)

[Insert Name of reporting financial institution][Quarter] [Year]

No.	Date of Incident	Time of Incident	critical	Nature of Incident	Action Taken	Time of Resolution	Impact Assessment	Action Taken to Mitigate Future Incidents
1.								
2.								
3.								
4.								
5.								

Submit this report on the 5th day after the end of every quarter to the Bank Supervision Department at fin@centralbank.go.ke

Prepared by:

Name.....
Designation.....
Contact email address.....
Contact phone number.....
Signature.....
Date.....

Authorised by:

Name.....
Designation.....
Contact email address.....
Contact phone number.....
Signature.....
Date.....

REFERENCES:

This Guideline is benchmarked against and aligned with the following Global best practices and supervisory practices:

1. Basel Committee Paper on Principles for Sound Management of Operational Risk (PSMOR).
2. Basel Committee paper on Principles for Operational Resilience.
3. Basel Core Principles (BCP) No. 25(2024): Essential criteria and additional criteria on operational risk and operational resilience.
4. Cross-Industry Guidance on Operational Resilience by the Central Bank of Ireland;
5. UK PRA/FCA Operational Resilience Framework;
6. Monetary Authority of Singapore (MAS) Operational Resilience and Technology Risk Management Guidelines;
7. South African Prudential Authority and FSCA cyber resilience and operational risk frameworks;
8. European Union Digital Operational Resilience Act (DORA);

9. CPMI-IOSCO Principles for Financial Market Infrastructures;
10. NIST Cybersecurity Framework; and
11. ISO 22301 Business Continuity Management standards.