DRAFT CENTRAL BANK OF KENYA RISK MANAGEMENT GUIDELINES 2026

1.0 OVERVIEW OF RISK MANAGEMENT FRAMEWORK

1.1 Introduction

The Central Bank of Kenya issues these guidelines to provide institutions with minimum requirements for establishing and maintaining risk management systems and frameworks. These guidelines adopt an Enterprise Risk Management (ERM) approach, promoting a holistic, forward looking and integrated management of risks in line with the best global practices.

For the purposes of these Guidelines, financial risk in a banking institution refers to the possibility that the outcome of an action or event could adversely affect the institution's capital, earnings, or overall financial condition. This includes both existing and emerging risks, including those arising from technological innovation, environmental and climate related factors, digital transformation, and cross-border operations. Such risks may result in direct financial losses or impose constraints on the institution's ability to achieve its strategic and business objectives.

1.2 Objective

The objective of these guidelines is to provide financial institutions with a structured framework for identifying, assessing, monitoring, and mitigating risks within financial institutions.

The Guidelines are intended to strengthen institutional resilience, enhance governance and risk culture, safeguard depositors' funds, promote financial stability, and support the sustainable development of the financial sector.

1.3 Scope

These Guidelines shall apply to all institutions licensed under the Banking Act. Institutions with cross-border operations shall ensure that their group wide risk management frameworks align with these Guidelines, and are appropriately applied across subsidiaries, branches and affiliated entities.

1.4 Risk Governance Structure: The Three Lines of Defense

Institutions should establish and maintain a robust risk governance structure based on the Three Lines of Defense (3LoD) model. This model ensures clear allocation of roles, responsibilities, and accountability for risk management, consistent with Basel Committee on Banking Supervision (BCBS) standards on governance and internal control frameworks.

(a) First Line of Defense – Business and Operational Management

The first line of defense shall comprise business units, operational management, and all staff responsible for day-to-day activities. The first line shall be responsible for:

- Identifying, assessing, and managing risks arising from business activities on a continuous basis;
- Designing and implementing effective internal controls within their processes;
- Ensuring compliance with approved policies, procedures, risk limits, and regulatory requirements;
- Maintaining accurate and timely risk and operational data; and
- Escalating risk issues, breaches, and control deficiencies in a timely manner.

Business units should remain primarily accountable for the risks they originate.

(b) Second Line of Defense – Risk Management and Compliance Functions

The second line of defense consists of independent risk management and compliance functions.

These functions shall be responsible for:

- Developing and maintaining risk management frameworks, policies, and methodologies;
- Providing oversight, monitoring, and independent challenge of risk-taking activities;
- Establishing risk measurement tools, limits, and reporting frameworks;
- Monitoring compliance with laws, regulations, and internal policies;
- Consolidating and reporting risk exposures to senior management and the Board; and
- Providing guidance and advisory support to business units on risk and compliance matters.

The second line shall operate independently from business units and shall have adequate authority, stature, and resources to discharge its responsibilities effectively.

(c) Third Line of Defense – Internal Audit

The third line comprises an independent internal audit function that provides objective assurance to the Board and senior management on the effectiveness of governance, risk management, and internal control systems. Its responsibilities include:

- Conducting independent reviews of risk management and control processes;
- Assessing the adequacy and effectiveness of the first and second lines;
- Providing assurance on governance, risk, and control frameworks; and
- Reporting findings directly to the Board Audit Committee.

Internal audit operates independently from management and provides the highest level of assurance.

Governance Alignment

This structure shall be implemented in a manner consistent with global best practices on sound corporate governance, ensuring independence of control functions, clear escalation pathways, and effective board oversight. Institutions should ensure that the three lines operate in a coordinated but independent manner to support robust risk identification, measurement, monitoring, and control across all risk types.

1.5 Risk Categories

The nature, scale, and severity of risks an institution is exposed are influenced by various factors including its size, complexity, interconnectedness, business model, technological adoption, and operating environment. Institutions are increasingly exposed to emerging risks arising from technological, data governance requirements, environmental and climate related developments, and evolving regulatory and geopolitical landscapes.

While the types and degree of risks an institution may be exposed to depend upon a number of factors, these guidelines highlight the following categories of risks as critical for financial institutions:-

1. Strategic Risk
2. Credit Risk
3. Liquidity Risk
4. Market Risk
5. Operational Risk
6. Information and Communication Technology (ICT)
7. Cybersecurity Risk
8. Data Governance Risk
9. Reputational Risk
10. Legal and Compliance Risk
11. Country and Transfer Risk
12. Transfer Pricing Risk
13. Environmental, Social and Governance Risk

14. Model Risk
15. Third Party Risk
16. Digital Financial Services/Fintech Risk
17. Money Laundering/Financing of Terrorism/Proliferation Financing (ML/FT/PF) Risk

1.6 Risk Management Function

In accordance with the Basel Core Principles for Effective Banking Supervision, Risk Management Processes, *banks and banking groups are required to maintain comprehensive risk management processes subject to Board and senior management oversight, to identify, measure, evaluate, monitor, report and control or mitigate all material risks. These processes should also incorporate the assessment of overall capital adequacy relative to the institution's risk profile and be commensurate with the size, complexity and types of risks of the institution.*

It is therefore a requirement that each institution prepare a comprehensive Risk Management Programme (RMP) tailored to its needs and circumstances under which it establishes and operates a Risk Management Function that supervises overall risk management. The function should be independent from those who take or accept risks on behalf of the institution and should report directly to the board or a committee of the board.

The risk management function is responsible for ensuring that effective processes are in place for:

i. Identifying current and emerging risks;
ii. Developing risk assessment and measurement systems;
iii. Establishing policies, practices and control mechanisms to manage risks;
iv. Developing risk tolerance limits for Senior Management and board approval;
v. Monitoring exposures against approved risk tolerance limits; and
vi. Reporting results of risk monitoring to Senior Management and the board.

1.7 Risk Management Process

A robust Risk Management Programme, regardless of its design, should at a minimum incorporate the following core components:

1.7.1 Risk Identification: Every product and service offered by financial institutions carries a unique risk profile composed of multiple types of risks. For instance, most loan products present at least four types of risks: credit risk, interest rate risk, liquidity risk and operational risk. Risk identification should be a

continuing process and should be understood at both the transaction and portfolio levels.

1.7.2 Risk Measurement: Once the risks associated with a particular activity have been identified, the next step is to measure the significance of each risk. Each risk should be evaluated across three dimensions: size, duration and probability of adverse occurrences. Accurate and timely measurement of risk is essential to effective risk management systems.

1.7.3 Risk Control: Once risks have been identified and measured for significance, institutions can manage the risks, or at least minimize their adverse consequences through the following three primary approaches:

- Avoiding or placing limits on certain activities/risks.
- Mitigating risks.
- Offsetting risks

It is a primary management function to balance expected rewards against risks and the expenses associated with controlling risks. Institutions should establish and communicate risk limits through policies, standards and procedures that define responsibility and authority.

1.7.4 Risk Monitoring: Institutions need to establish an MIS that accurately identifies and measures risks at the inception of transactions and activities. It is equally important for management to establish an MIS to monitor significant changes in risk profiles over time. A loan payment delinquency report reflecting loans that are not being repaid as agreed is one report that indicates possible changes in perceived risk profiles. Since many institutions depend heavily on their net interest margins for survival, an MIS that reflects the impact of changes in interest rate risk is very important., Risk monitoring involves developing reporting systems that:-

- Identify adverse changes in the risk profiles of key products, services and activities.
- Monitoring the effectiveness of control measures that have been put in place to minimize/mitigate adverse consequences.

1.8 Basic Elements of a Sound Risk Management System

A risk management program defines the scope of risks to be managed, as well as the processes, systems, and procedures established to manage risks effectively. It also outlines the roles and responsibilities of individuals involved in risk management. The

framework should be comprehensive enough to capture all risks, while remaining flexible enough to adapt to changes in business activities, products and operating environment. The risk management program of each institution should at least contain the following elements of a sound risk management system:

1.8.1 Active Board and Senior Management Oversight

The Board of Directors bears ultimate responsibility for the level of types of risk assumed by the institution. Accordingly, the Board should approve the institution's overall business strategy, risk appetite, and all significant policies including those relating to risk management. These policies should, among others, address key risk areas such as Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF), Environmental, Social, and Governance (ESG) and climate-related financial risks.

The Board is also responsible for ensuring that senior management possesses the requisite competence, experience, and integrity to effectively manage the institution's activities in a manner consistent with the approved strategy and risk appetite. Additionally, the Boards understand the nature of the material risks facing the institution and ensure that senior management takes appropriate steps to identify, measure, monitor and control these risks.

While the level of technical knowledge required of directors may vary depending on the institution's complexity, it is essential that the directors have a clear understanding of the key risks to which their institutions are exposed to. This should be supported by regular timely and meaningful reporting that enables informed decision making. Directors may take steps to develop an appropriate understanding of the risks their institution face, through briefings from internal and external experts, including auditors, specialists in areas of compliance, financial crime prevention and sustainability.

Based on this understanding, the Board should provide clear guidance acceptable risk exposures and ensure that senior management implements appropriate policies, procedures and controls necessary to comply with approved strategies, regulatory requirements and sustainability commitments.

Senior management is responsible for effective implementation of board approved strategies and for managing the risks associated with the institution's activities. Management should therefore be fully involved in the activities of their institutions and possess sufficient knowledge of all major business lines to ensure that appropriate policies, risk management systems, internal controls and risk monitoring systems are in place, and that accountability and lines of authority are clearly delineated.

Senior management is also responsible for fostering a strong risk management and compliance culture, supported by effective internal controls and high ethical standards. This requires a thorough understanding of developments in the financial sector, and the institution's activities, including the nature of the internal controls necessary to limit the related risks

1.8.2 Adequate Policies Procedures and Limits

The board of directors and senior management should tailor their risk management policies and procedures to the types of risks that arise from the activities the institution conducts. Once the risks are properly identified, the institution's policies and procedures should provide detailed guidance for the day-to-day implementation of broad business strategies and should include limits designed to shield the organization from excessive and imprudent risks.

A bank's policies, procedures and limits should:

- Provide for adequate and timely identification, measurement, monitoring, control and mitigation of the risks posed by its lending, investing, trading, securitisation, off balance sheet, fiduciary and other significant activities at the business line and firm-wide levels;
- Ensure that the economic substance of a bank's risk exposures are fully recognised and incorporated into the bank's risk management systems;
- Be consistent with the bank's stated goals and objectives, as well as its overall financial strength;
- Clearly delineate accountability and lines of authority across the bank's various business activities, and ensure there is a clear separation between business lines and the risk function;
- Escalate and address breaches of internal position limits;
- Provide for the review of new businesses and products by bringing together all relevant risk management, control and business lines to ensure that the bank is able to manage and control the activity prior to it being initiated; and
- Include a schedule and process for reviewing the policies, procedures and limits and for updating them as appropriate.

1.8.3 Adequate Risk Monitoring and Management Information Systems (MIS)

Effective risk monitoring requires institutions to identify and measure all material risk exposures. Consequently, risk-monitoring activities must be supported by information systems that provide senior managers and directors with timely reports on the financial condition, operating performance and risk exposure of the institution. The

sophistication of risk monitoring and MIS should be consistent with the complexity and diversity of the institution's operations. Every institution shall require a set of management and board reports to support risk-monitoring activities. These reports may include daily or weekly balance sheets and income statements, a watch list for potentially troubled loans, a report of overdue loans, simple interest rate risk report and other relevant reports.

In order to ensure effective measurement and monitoring of risk and management information systems, the following should be observed:

a) the institution's risk monitoring practices and reports address all of its material risks;
b) key assumptions, data sources, and procedures used in measuring and monitoring risk are appropriate and adequately documented and tested for reliability on an ongoing basis;
c) As an integral component of an institution's risk management framework appropriate periodic stress testing should be conducted and management action plans to mitigate the risks identified in the Stress Tests are put in place.
d) reports and other forms of communication are consistent with the institution's activities, structured to monitor exposures and compliance with established limits, goals, or objectives and, as appropriate, compare actual versus expected performance and;
e) reports to management or to the institution's directors are accurate and timely and contain sufficient information for decision-makers to identify any adverse trends and to evaluate adequately the level of risk faced by the institution.

1.8.4 Adequate Internal Controls

An institution's internal control structure is critical to the safe and sound functioning of the organization, in general and to its risk management, in particular. Establishing and maintaining an effective system of controls, including the enforcement of official lines of authority and the appropriate separation of duties is one of management's important responsibilities.

When properly structured, a system of internal controls promotes effective operations and reliable financial and regulatory reporting, safeguards assets and helps to ensure compliance with relevant laws, regulations and institutional policies, and mitigates both financial and non-financial risks.

Internal controls should be tested by an independent and suitably qualified internal auditor who reports directly to the board's Audit Committee. Given the importance of appropriate internal controls for institutions, the results of audits or reviews, conducted

by an internal auditor or other persons, should be adequately documented, as should management's responses to them.

In addition, communication channels should exist that allow negative or sensitive findings, including those related to operational, technological, or Environmental, Social, and Governance (ESG) risks to be reported directly to the board's Audit Committee.

In order to ensure the adequacy of an institution's internal controls and audit procedures, the following should be observed:-

- The system of internal controls should be appropriate to the type and level of risks posed by the nature and scope of the institution's activities, including financial, operational, technological, third-party, ESG, and emerging risks.
- The institution's organisational structure should establish clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits across all risk categories.
- Reporting lines should provide sufficient independence of the control areas from the business lines and appropriate segregation of duties throughout the institution such as those relating to trading, custodial, and back-office, technology, and vendor management activities.
- Official institutional structures should reflect actual operating practices, including operational resilience protocols and cybersecurity governance.
- Financial, operational, technological, and regulatory reports should be reliable, accurate and timely; wherever applicable, exceptions are noted and promptly investigated.
- Adequate procedures for ensuring compliance with applicable laws and regulations, ESG commitments should be in place.
- Internal audit or other control review practices should provide for independence and objectivity and should explicitly cover non-financial risk areas, including cybersecurity, third-party arrangements, operational resilience, ESG, and emerging risks such as AI-driven fraud.
- Institutions should ensure that internal controls and information systems are subject to regular testing and review. The scope, procedures, findings, and management responses should be adequately documented. Material weaknesses identified should receive timely attention from senior management and the Board, as appropriate, and corrective actions should be independently verified to ensure their effective implementation.
- Institutions should implement controls for operational resilience, including business continuity and disaster recovery planning, incident response, and crisis management, with periodic testing to validate effectiveness.

- Institutions should implement cybersecurity controls that include threat and vulnerability assessments, access controls, network security, data protection, and real-time monitoring. Cybersecurity controls must be reviewed regularly to address evolving threats, including AI-driven attacks, ransomware, and other technology-enabled risks.
- Institutions should implement controls to manage third-party risks, including risk-based due diligence, ongoing monitoring of service providers, and contractual obligations that support operational and reputational risk mitigation.
- ESG-related risks should be identified, monitored, and mitigated through controls that address environmental, social, and governance exposures, aligned with recognized frameworks and best practices.
- The institution's audit committee or board of directors should review the effectiveness of internal audits and other control review activities covering both financial and non-financial risk areas on a regular basis.

2.0 STRATEGIC RISK MANAGEMENT

2.1 Introduction

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. It is a risk that could significantly impact on the achievement of the institution's vision and strategic objectives as documented in the strategic plan.

Strategic risk management is the process of identifying, assessing, measuring, monitoring and managing the risk in the institution's business strategy. Strategic risk management involves evaluating how a wide range of possible events and scenarios will affect the strategy and its execution and the ultimate impact on the institution's value.

2.2 Board and Senior Management Oversight

2.2.1 Specific responsibilities for the Board

The Board has specific responsibilities for overseeing an institution's strategic risk management process. These includes:-

- Ensuring that the institution has in place an appropriate strategic risk management framework which suits its own circumstances, business needs and risk tolerance.
- Ensuring that the institution's strategic goals and objectives are clear and are set in line with its corporate mission and values, culture, business direction and risk tolerance.
- Approving the institution's strategic plan (including strategies contained therein) and any subsequent changes and reviewing the plan (at least annually) to ensure its appropriateness.
- Ensuring that the institution's organisation structure, culture, infrastructure, financial means, managerial resources and capabilities, as well as systems and controls are appropriate and adequate to support the implementation of its strategies; Reviewing high-level reports periodically submitted to the Board on the institution's overall strategic risk profile.
- ensuring that any material risks and strategic implications identified from those reports are properly addressed.
- Ensuring that senior management is competent in implementing strategic decisions approved by the Board and supervising such performance on a continuing basis.
- Ensuring that the risk appetite of the institution is aligned with strategy and capital.
- Ensuring that the institution has robust risk management and modeling including stress testing, backtesting and scenario analysis. The results can be linked to decisions such as capital planning and dividend policies.
- Ensure that the institution has recovery planning to prepare for extreme scenarios.

- Ensuring that the institution moves towards forward looking risk management systems including embedding artificial intelligence driven early warning systems.
- Integrating Environmental, Social, and Governance and climate related risks Frameworks within the overall Enterprise Risk Management.

2.2.2 Specific responsibilities of senior management

In ensuring effective strategic risk management within an institution, senior management should, among other things:–

- Establish and implement the institution's strategic risk management framework based on criteria and standards set by the Board;
- Assist the Board in developing strategies to meet the institution's strategic goals and objectives;
- Formulate the institution's strategic plan and related implementation plans (such as business, development and operating plans);
- Ensure adequate implementation of the institution's strategic plan, as approved by the Board;
- Implement an effective performance evaluation system;
- Ensure that any strategic issues and material risks arising from environmental changes or implementation of the institution's strategies are reported to the Board on a timely basis.

2.3 Policies and Procedures and Limits

Effective management of strategic risk requires that policies, procedures and limits be established to ensure objective evaluation of and responsiveness to a bank's business environment. Policies on business strategy are critical in defining the business segments that the institution will focus on, both in the short and long run. There should be clear guideline on frequency and procedure for review of the institution's business strategy.
Procedures for defining and reviewing the institutions' business strategy are intended to ensure that the following aspects are given adequate consideration:

- The institution's inherent strengths.
- It's identified weaknesses.
- Opportunities external to the institution.
- External factors that pose threats to the institution.

Limits are necessary in defining*:*

- Exposure to different sectors.
- Growth of business and staff strength.
- Network expansion programmes.

2.3.1 Strategic risk management process

An effective strategic management process should include the following:

2.3.1.1 Strategic Planning

Strategic planning is the process whereby an institution determines the overall direction and focus of their organisation, establish medium and long term priorities in line with their corporate mission and goals, and translate those priorities into appropriate strategies for achieving stated goals and objectives. This process culminates in the development of a strategic plan. Strategic planning provides a process for institutions to identify and assess potential risks posed by their strategic plan, and consider whether they have adequate capacity to withstand the risks. It also facilitates institutions in responding on a timely basis to any adverse changes in circumstances (whether internal or external) that may undermine the achievement of their plan or affect their future development.

A strategic planning process has three basic elements:-

- A process to set strategic goals and objectives,
- A process to evaluate the institutions strategic position and develop appropriate strategies, and
- A process to translate those strategies into action plans.

2.3.1.2 Setting of Strategic goals and objectives

In setting strategic goals and objectives, institutions should be guided by their corporate mission which outlines the broad directions that the institution is to follow, and reflect the vision and values upheld by the institution. Strategic goals generally reflect an institution's aspirations in relation to achieving growth and return, efficiency, and competitive advantage within the environment it operates.

In setting strategic goals and objectives, institutions should identify and take into account the needs and aspirations of their major stakeholders and changes in operating environment (eg. political, legal, economic, social and technological changes).

2.3.1.3 Development of strategies

Institutions should have a process for evaluating their strategic position and developing appropriate strategies to achieve their strategic goals and objectives. The process requires

comprehensive assessment of the prevailing banking, business, and economic environment alongside an internal analysis of its institutional strengths, weaknesses and risk tolerance.

2.3.1.4 Formulation of strategic plan

Institutions should have a process for formulating and approving the strategic plan. This process and all related procedures must be clearly documented and approved by the Board. Similarly, the responsibilities of the Board, senior management and other staff concerned should be clearly documented. The Board and senior management should also be subject to periodic review to ensure ongoing appropriateness.

Strategic decisions agreed upon during the planning process should form the basis of the strategic plan. Beyond defining execution strategies, the plan should articulate the institution's business philosophy, growth targets, and financial risk tolerance. It must also incorporate critical internal and external factors influencing long-term growth and development. The depth and coverage of the strategic plan should be commensurate with the institution’s scale and complexity of business.

In the case of a local banking group with regional presence, the strategic plan should be prepared on a consolidated basis (i.e. including the positions of subsidiaries and overseas branches).

Branches or subsidiaries of foreign banks should develop their own strategic plan for managing strategic risk if the group’s plan does not adequately reflect their local situation, needs and activities. This ensures their specific needs and activities are properly addressed.

2.3.2 Alignment and change management

Institutions should align internal resources and processes before implementing their strategies. Institutions must also manage change dynamics, including those arising from organizational or cultural shifts. This preparation helps facilitate the achievement of desired outcomes. Interdependencies between processes across departments should be addressed in advance so that they can be properly understood and accounted for during implementation.

Ensuring proper alignment of internal resources and processes means, for example, checking to see whether: –

- sufficient resources (financial and non-financial) have been allocated to undertake the necessary tasks;
- the right people have been put in the right place; and

- the organisation and risk management structure, systems, infrastructure and technology are in the right shape to support the new initiatives.

2.4 Measuring and monitoring

The success or failure of a strategy depends on whether an institution has sufficient resources and capabilities to implement it. It also relies on the institution's ability to effectively monitor and control the progress of implementation. As such, in addition to strategic planning, institutions should have a process to facilitate the monitoring and control of strategies being implemented.

Active Board and senior management oversight with the support of the strategic risk management function will help ensure effective implementation and control of strategies. In addition, there should be adequate management guidelines and written procedures for implementing strategies and monitoring and reporting the progress of implementation.

Institutions should report strategic issues from anticipated operational or market changes to senior management and subsequently to the Board promptly. These issues may have a significant adverse impact on business or financial conditions. Reports should include an assessment of the strategic risk implications. They should also outline the need for remedial actions. These remedial actions may involve modifying strategies or implementing risk-mitigating and contingency measures.

In order to ensure an effective strategic risk management process, every institution should deploy a management information system that will enable management to monitor:

- Current and forecasted economic conditions, e.g. economic growth, inflation, foreign exchange trends, etc..
- Current and forecasted industry and market conditions, such as:
  - Increasing competition by new market entrants.
  - Number and size of mergers and acquisitions.
  - Changing customer behaviour.
  - New products/substitutes.
- Exposure to different sectors, and associated sector risks.

2.4.1 Performance evaluation and feedback

Comparing actual performance with desired outcomes is an essential check on strategy implementation. It shows whether approved strategies are succeeding. This comparison also highlights significant deviations from set targets. Management can then take timely remedial actions to keep implementation on track. Therefore, institutions are expected to develop a

performance evaluation system that tracks progress towards achieving both financial and non-financial targets.

To ensure efficient and continuous performance evaluation, long-term strategic goals should be broken down into short-term, measurable targets. Ideally, these should be set on a yearly basis.

2.4.2 Other Supporting Processes

2.4.2.1 Planning and Management of Capital and Funding needs

Inadequate planning of capital and funding needs hinders the implementation of strategic decisions. It can disrupt an institution's operations. Poor planning also weakens its ability to meet strategic goals thus creating obstacles to achieve objectives. Effective capital and funding planning is therefore essential. As such, institutions should view such planning as a crucial element of the strategic planning process.

Capital planning should be risk-based and forward-looking. It must consider current and future capital needs, anticipated expenditures, dividend forecasts, desirable capital levels, and external sources such as available supply and capital-raising options among others.

2.4.2.2 Management Information System

In a competitive banking environment, the ability to effectively manage information is crucial to an institution's ability to remain competitive, introduce new products and services, and achieve desired goals. Institutions should therefore ensure that they have sufficient and robust MIS to support their strategic planning and decision making processes.

2.4.2.3 Human resources management and development

Human resources management has a strategic focus in that it is involved in gaining commitments to an institution's goals and shaping its corporate culture. By developing policies to meet future needs, human resources management enables the adoption of a forward-looking approach to deal with change and growth and to anticipate future problems.

2.4.2.4 Succession Planning

The institutions' management should develop management succession plans to cater for staff turnover and retirement. This is particularly essential for institutions to cater for major turnover in senior and middle management, whether due to transfer, resignation or retirement.

The institutions' board of directors should also maintain succession plans for critical positions such as Chairman of the Board and the institution's Chief Executive Officer.

2.4.3 Stress-Testing and Contingency Strategies

Institutions should employ stress-testing techniques in their strategic planning and management processes to assess any potential threats to the implementation of their strategies. Stress-testing generally involves identifying possible events or changes in the external environment that could have unfavourable effects on an institution and assessing the institution's ability to withstand those effects.

Stress-testing does not require sophisticated financial modeling tools. Its purpose is to ensure institutions evaluate the potential impact of different stress scenarios. These impacts may be both financial and non-financial. The focus is therefore on understanding how such scenarios could affect the institution. This evaluation strengthens preparedness and resilience. The level of resources devoted to this effort should be commensurate with the nature, scale and complexity of institutions' business activities.

2.5 Three Lines of Defence

The understanding of strategic risks within institutions requires a collaborative approach that encompasses the following functions: Business line, Risk Management and Internal Audit.

The first line of defence is the business unit, which is accountable for identifying, measuring, taking and mitigating the risks of its business.

The second line of defence, which includes risk management and compliance functions, work with the business units to ensure that the first line has properly identified, measured and reported their business risks. Collectively, all elements of this line of defence are responsible for developing a bank-wide view of risk. Therefore, the Risk Management Function comprises risk, control, and compliance oversight functions which ultimately ensure that an institution's management of strategic risks and controls are effectively operating. Risk management has a duty to ensure that the strategic risks are managed within the enterprise risk management portfolio.

The third line of defence, namely internal audit, independently and systematically reviews the efficiency and effectiveness of the first two lines of defence and contributes to improving their effectiveness.

Institutions therefore need strong internal control systems to ensure that they are not unduly exposed to strategic risks. Internal controls are required to ensure that:

- The organization structure establishes clear lines of authority.
- The institution’s systems and structures provide for business continuity planning.
- The process of setting up and reviewing strategic plans is comprehensive and is adhered to.

Finally, the third line of defence should be supported more generally by the external auditors and the board's audit committee. External auditors play a crucial role by providing independent assurance, validating risk governance frameworks, and highlighting weaknesses in capital planning, controls, and reporting. Their oversight ensures that board and senior management receive unbiased insights into whether strategies align with risk appetite and regulatory expectations.

3.0 CREDIT RISK MANAGEMENT

3.1 Introduction

Credit risk is the current or prospective risk to earnings and capital arising from an obligor's failure to meet the terms of any contract with the bank or if an obligor otherwise fails to perform as agreed.

Banks need to manage the credit risk inherent in the entire portfolio as well as the risk in individual credits or transactions. Banks should also consider the relationships between credit risk and other risks. The effective management of credit risk is a critical component of a comprehensive approach to risk management and essential to the long-term success of any banking organization.

For most banks, loans are the largest and most obvious source of credit risk; however, other sources of credit risk exist throughout the activities of a bank, including in the banking book and in the trading book, and both on and off the balance sheet. Banks are increasingly facing credit risk (or counterparty risk) in various financial instruments other than loans, including acceptances, interbank transactions, trade financing, foreign exchange transactions, financial futures, swaps, bonds, equities, options, and in the extension of commitments and guarantees, and the settlement of transactions.

3.2 Board and Senior Management Oversight

3.2.1 The Board of Directors

The board of directors carries the ultimate responsibility of approving and periodically reviewing the credit risk strategy and credit risk policies of the bank. This role is part of the board's ultimate responsibility of offering overall strategic direction to the bank. The credit risk strategy should reflect the bank's tolerance for risk and the level of sustainable returns the bank expects to achieve for incurring various credit risks, taking into account market conditions, macroeconomic factors and forward-looking information.

The credit policies should be adequate and must cover all the activities in which credit exposure is a significant risk. The credit risk strategy and policies should be communicated throughout the organisation. The board oversees senior management to ensure that the approved credit risk policies are effectively implemented and fully integrated within the bank's overall risk management process. The board should ensure that:

- The credit strategy has a statement on acceptable levels of exposure to the various economic sectors, currencies and maturities. It should also include the target markets, diversification and concentration of the credit portfolio.

- The credit risk strategy and policies are effectively communicated throughout the bank.

- The financial results of the bank are periodically reviewed to determine if changes need to be made to the credit risk strategy.

- The recruitment procedure ensures that the senior management team is fully capable of managing the credit risk.

- There is an internal audit function capable of assessing compliance with the credit policies and management of the entire credit portfolio.

- The delegation authority and approval levels are clearly defined.

- The management provides periodic reports on the insiders, provisioning and write-off on credit loan losses and audit findings on the credit granting and monitoring processes.

- To avoid conflicts of interest, board members do not override the credit-granting and monitoring processes of the bank. Board members with conflicts of interest should be excluded from the approval process for granting and managing related party transactions.

- The bank's remuneration policies do not contradict its credit risk strategy. Remuneration policies that reward unacceptable behaviour such as generating short-term profits while deviating from credit policies or exceeding established limits, weaken the bank's credit processes.

3.2.2 Senior Management

Senior management should have responsibility for implementing the credit risk strategy and policies approved by the board of directors, and for developing procedures for identifying, measuring, evaluating, monitoring, reporting and controlling or mitigating credit risk (including counterparty credit risk). Such policies and procedures should address credit risk in all of the bank's activities and at both the individual credit and portfolio levels. The senior management should ensure the following:

- The credit granting activities conform to the established credit risk strategy.

- The bank has implemented written policies and sound procedures related to identifying, measuring, evaluating, monitoring, reporting and controlling or mitigating credit risk (including counterparty credit risk).The bank has implemented credit risk policies and procedures to ensure that the credit portfolio is adequately diversified given the bank's target markets and overall credit risk strategy.

- That loan approval and review responsibilities are clearly and properly assigned.

- Banks that engage in granting credit internationally undertake, in addition to standard credit risk, risks associated with conditions in the home country of a foreign borrower or counterparty, including country risk and transfer risk.

- Compliance with internal exposure limits, prudential limits and regulatory requirements.

- The credit policies must be communicated throughout the bank, implemented, monitored and revised periodically to address any changes.

- Internal audit reviews of the credit risk management system and credit portfolio are undertaken regularly.

- Adequate research is undertaken for any new products or activities to ensure the risks are appropriately identified and managed. These products must receive prior board approval.

3.3 Policies, Procedures and Limits

Banks should establish overall credit limits at the level of individual borrowers and counterparties, and groups of connected counterparties that aggregate in a comparable and
meaningful manner different types of exposures, both in the banking and trading book and on and off the balance sheet.

Exposure limits are needed in all areas of the bank's activities that involve credit risk. These limits help to ensure that the bank's credit-granting activities are adequately diversified. Much of the credit exposure faced by some banks comes from activities and instruments
in the trading book and off the balance sheet. Limits on such transactions are particularly effective in managing the overall credit risk profile or counterparty risk of

a bank. In order to be effective, limits should generally be binding and not driven by customer demand.

Effective measures of future exposure, such as potential future exposure (PFE) or alternative metrics, are essential for establishing meaningful exposure limits for different activities. PFE is an estimate that captures the potential increase in exposure if a counterparty were to default today on a derivative contract until all exposures to this counterparty are closed (including by liquidation, closing out, realisation of collateral, netting or guarantees). It is determined by simulating market scenarios and assessing the potential worst-case loss at a specific future point in time. Measures of future exposures should t be calculated over multiple time horizons.

3.3.1 Policies Relating to Limits

Establishment of sound and well-defined policies, procedures and limits is vital in the management of credit risk. These should be well documented, duly approved by the board and strictly implemented by management. Credit policies establish the framework for lending and guide the credit-granting activities of the bank

An effective credit policy should outline the following:-

- Defines the credit concentrations, limits and exposures the organization is willing to assume. These limits will ensure that credit activities are adequately diversified. The policy on large exposures should be well documented to enable banks to take adequate measures to ensure concentration risk is mitigated. The policy will stipulate clearly the percentage of the bank's capital and reserves that the bank can grant as loans or extend as other credit facilities to any individual entity or related group of entities.

- In the exposure limit, contingent liabilities should be included – for example guarantees, acceptances and letters of credit. In the case of large exposures, banks must pay attention to the completeness and adequacy of information about the debtor. Credit staff should ensure they monitor events affecting large debtors and their performance on an on-going basis. Where external events present a cause for concern, credit officers should request for additional information from the debtor. If there are signs that the debtor might have difficulties in meeting its obligations to the bank, the concerns should be raised with the credit management and a contingency plan developed to address the issues.

- The policy should require that the board approve all loans to related or connected parties. These credits should be based on market terms and should

not be more favourable with regard to amount, maturity, rate and collateral than those provided to other customers.

3.3.1.1 Limits

Banks should monitor actual exposures against established limits. It is important that banks have a management information system in place to ensure that exposures approaching risk limits are brought to the attention of senior management. All exposures should be included in a risk limit measurement system. The bank's information system should be able to aggregate credit exposures to individual borrowers and counterparties and report on exceptions to credit risk limits on a meaningful and timely basis.

On exposure limits, the policies should include the following:

- Acceptable exposure to individual borrowers.
- Maximum exposure to connected groups and insider dealings.
- The total overall limit on the credit portfolio in relation to capital, assets or liabilities.
- Limits in relation to geographical location.
- Maximum exposure to individual economic sectors (for example commercial, consumer, real estate, agricultural).
- Acceptable limits on specific products.

Banks should ensure that their own internal exposure limits comply with any requirement made by the Central Bank under the Banking Act. In order to be effective, credit policies must be communicated throughout the organization, implemented through appropriate procedures, and periodically revised to take into account changing internal and external circumstances.

3.3.2 Policies Relating to Credit Concentration Risk

Banks should have policies and processes that provide a comprehensive bank-wide view of significant sources of concentration risk. Exposures (including counterparty credit risk exposure) arising from off-balance sheet as well as on-balance sheet items included in both the banking book and trading book are captured.

Concentration risk may result from credit, market and other risk where a bank is overly exposed to particular asset classes, products, collateral, currencies or funding sources, and is broader than exposures subject to large exposure requirements. Credit concentrations include exposures to: single counterparties (including collateral credit protection and other commitments provided); groups of connected counterparties;

counterparties in the same industry, economic sector or geographic region; and counterparties whose financial performance is dependent on the same activity or commodity

3.3.3 Segregation of Duties

Credit policy formulation, credit limit setting, monitoring of credit exposures and review and monitoring of documentation are functions that should be performed independent of the loan origination function. For small banks, where it might not be feasible to establish such structural hierarchy, there should be adequate compensating measures to maintain credit discipline, introduce adequate checks and balances and standards to address potential conflicts of interest.

3.3.4 Policies Relating to Credit Products

The various types of loan products and credit instruments the bank intends to offer should be documented. Management must have a good understanding of all the products on offer and a careful review of the existing and potential risks must be undertaken. The products should also have a maturity profile and the pricing of these products should be included and periodically reviewed. Any new products should be fully researched and prior board approval obtained before introduction to the customers.

Credit exposure for all off balance sheet commitments should be well documented. These main off balance sheet items include letters of credit, guarantees, futures, options, swaps etc. The policy will stipulate the credit risk analysis procedures and the administration of these credit instruments. The key objective of the review is to assess the ability of the client to meet particular financial commitments in a timely manner.

3.3.5 Policies Relating to Credit Assessment and Granting Process

Banks must operate within sound, well-defined credit-granting criteria. These criteria should include a clear indication of the bank’s target market and a thorough understanding of the risk profile and characteristics of the borrower or counterparty, as well as the purpose and structure of the credit, and its source of repayment.

Banks must operate under sound, well-defined credit-granting criteria. These criteria should include a thorough understanding of the borrower or counterparty, as well as the purpose and structure of the credit, and its source of repayment.

Banks must receive sufficient information to enable a comprehensive assessment of the true risk profile of the borrower or counterparty. At a minimum, the factors to be considered and documented in approving credits must include:

- the purpose of the credit and sources of repayment;
- the integrity and reputation of the borrower or counterparty;
- collateral and its sensitivity to economic and market developments
- the current risk profile (including the nature and aggregate amounts of risks) of the borrower or counterparty and its sensitivity to economic and market developments;
- the borrower's repayment history and current capacity to repay, based on historical financial trends and cash flow projections;
- The borrower credit rating/report from licensed Credit Reference Bureau;
- a forward-looking analysis of the capacity to repay based on various scenarios;
- the legal capacity of the borrower or counterparty to assume the liability;
- for commercial credits, the borrower's business expertise and the status of the borrower's economic sector and its position within that sector;
- the proposed terms and conditions of the credit, including covenants designed to limit changes in the future risk profile of the borrower; and
- where applicable, the adequacy and enforceability of collateral or guarantees, including under various scenarios.

Banks should have procedures to identify situations where, in considering credits, it is appropriate to classify a group of obligors as connected counterparties and, thus, as a single obligor. This would include aggregating exposures to groups of accounts exhibiting financial interdependence, including corporate or non-corporate, where they are under common ownership or control or with strong connecting links (for example, common management, familial ties). Banks should also have procedures for aggregating exposures to individual clients across business activities.

For banks that participate in loan syndications or other such loan consortia, all syndicate participants should perform their own due diligence, including independent credit risk analysis and review of syndicate terms prior to committing to the syndication. Each bank should analyse the risk and return on syndicated loans in the same manner as directly sourced loans.

In granting credit, collateral cannot be a substitute for a comprehensive assessment of the borrower or counterparty. The bank should primarily assess the borrower's capacity to repay and should not use collateral to compensate for insufficient information.

Arm's-length Lending Practices

Banks should have checks and balances to ensure credit is granted on arms-length basis. Extensions of credit to directors, senior management and other influential parties, for example shareholders, should not override the established credit granting and monitoring processes of the bank.

Transactions with related parties must not be undertaken on more favourable terms than corresponding transactions with non-related counterparties. For instance, more favourable terms should not be applied to credit assessment, tenor, interest rates, fees, amortisation schedules and requirements for collateral. This guards against conflicts of interest and protects the integrity of the bank's lending process.

Process for Approving Credits

Banks should have a clearly established process in place for approving new credits as well as amending, renewing and refinancing existing credits and ensuring a thorough understanding of the risk profile and characteristics of the borrowers or counterparties.

The following should be observed in the approval process:

- Approvals should be made in accordance with the bank's written guidelines and granted by the appropriate level of management.
- There should be a clear audit trail documenting that the approval process was complied with and identifying the individual(s) and/or committee(s) providing input as well as making the credit decision.
- Banks should invest in adequate credit decision resources so that they are able to make sound credit decisions consistent with their credit strategy and meet competitive time, pricing and structuring demands.
- Each credit proposal should be subject to careful analysis by a qualified credit analyst with expertise commensurate with the size and complexity of the transaction
- An effective evaluation process establishes minimum requirements for the information on which the analysis is to be based.
- There should be policies in place regarding the information and documentation needed to approve new credits, renew existing credits and/or change the terms and conditions of previously approved credits. The information received will be the basis for any internal evaluation or rating assigned to the credit, and its accuracy and adequacy is critical to management making appropriate judgments about the acceptability of the credit.
- Banks should maintain a team of credit risk officers who have the experience, knowledge and background to exercise prudent judgment in assessing, approving and managing credit risks.

- A bank's credit-granting approval process should establish accountability for decisions taken and designate who has the absolute authority to approve credits or changes in credit terms. Banks typically utilise a combination of individual signature authority, dual or joint authorities, and a credit approval group or committee, depending upon the size and nature of the credit. Approval authorities should be commensurate with the expertise of the individuals involved.
- There should be a clear audit trail documenting that the approval process was complied with. The trail should identify the individual(s) and/or committee(s) providing input, as well as those making the credit decision to ensure accountability and consistency.

3.3.6 Credit Risk Mitigation Techniques

Banks use various techniques of mitigating credit risk including collateral, guarantees and netting off of loans against deposits of the same counter-party. While the use of these techniques will reduce or transfer credit risk, other risks may arise which include legal, operational, liquidity and market risks. Therefore, there is a need for a bank to have stringent procedures and processes to control these risks and have them well documented in the policies. At present, in this jurisdiction, the common credit risk mitigation technique used is collateral.

Banks should have policies covering the acceptability of various forms of collateral, procedures for the ongoing valuation of such collateral, and a process to ensure that collateral is, and continues to be, enforceable and realisable. With regard to guarantees, banks should evaluate the level of coverage being provided in relation to the credit-quality and legal capacity of the guarantor. Banks should be careful when making assumptions about implied support from third parties such as the government.

A collateralized transaction is one in which banks have a credit exposure or potential credit exposure and the exposure is reduced in whole or in part by collateral. The following is essential:

- There must be legal certainty. All documentation used for collateralized transactions must be binding to all parties and also be legally enforceable.
- The legal environment must provide for right of liquidation or right of possession in a timely manner in the event of default.
- Necessary steps must be taken for obtaining and maintaining an enforceable security, for example registration, right of set-off or transfer of title must meet all the legal requirements.
- Procedures for timely liquidation of collateral should be in place.

- Policies covering the various acceptable forms of collateral. With regard to guarantees, banks should evaluate the level of coverage being provided in relation to the credit-quality and legal capacity of the guarantor.
- Policies covering ongoing valuations of the collateral to confirm that it remains realisable.

3.3.7 Internal Risk Rating Systems

Internal risk ratings are an important tool in monitoring credit risk. Internal risk ratings should be adequate to support the identification and measurement of risk from all credit exposures and should be integrated into an bank's overall analysis of credit risk and capital adequacy.

A well-structured internal risk rating system is a good means of differentiating the degree of credit risk in the different credit exposures of a bank. This will allow more accurate determination of the overall characteristics of the credit portfolio, concentrations, problem credits and the adequacy of loan loss reserves. In determining loan loss reserves, banks should ensure that the Central Bank of Kenya classification criteria are the minimum.

Typically, an internal risk rating system categorises credits into various classes designed to take into account the gradations in risk. Simpler systems might be based on several categories ranging from satisfactory to unsatisfactory; however, more meaningful systems will have numerous ratings for credits considered satisfactory in order to truly differentiate the relative credit risk they pose.

While developing their systems, banks must decide whether to rate the riskiness of the borrower or counterparty, the risks associated with a specific transaction, or both. Internal risk ratings are an important tool in monitoring and controlling credit risk. In order to facilitate early identification, bank's internal risk rating system should be responsive to indicators of potential or actual deterioration in credit risk e.g. financial position and business condition of the borrower, conduct of the borrower's accounts, adherence to loan covenants and value of collateral.

Credits with deteriorating ratings should be subject to additional oversight and monitoring, for example, through more frequent visits from credit officers and inclusion on a watch list that is regularly reviewed by senior management. The internal risk ratings can be used by line management in different departments to track the current characteristics of the credit portfolio and help determine necessary changes to the credit strategy. Consequently, it is important that the board of directors and senior management also receive periodic reports on the condition of the credit portfolios based on such ratings.

The ratings assigned to individual borrowers or counterparties at the time the credit is granted must be reviewed on a periodic basis and individual credits should be assigned a new rating when conditions either improve or deteriorate. Because of the importance of ensuring that internal ratings are consistent and accurately reflect the quality of individual credits, responsibility for setting or confirming such ratings should rest with a credit review function independent of that which originated the credit concerned. It is also important that the consistency and accuracy of ratings is examined periodically by a function such as an independent credit review group.

3.3.8 Policies on Management of Problem Credits

The credit policy should establish the procedures for dealing with deteriorating and managing problem credits. Early recognition of weaknesses in the credit portfolio is important and allows alternative action and for an effective determination of loan loss potential.

An bank must have clearly articulated and documented policies in respect of the counting of days past due. In particular, policies should cover granting extensions, deferrals, renewals and additional credits to existing accounts. At a minimum, it must have approval levels and reporting requirements in respect of the above.

The policy should define a follow-up procedure for all loans and the various reports to be submitted both to management and board of directors. It should also include the internal rating for loan classification and provisioning.

When a bank has credit-related problems, it is important to segregate the credit remedial function from the area that originated the credit.

3.3.9 Policies on Inter-Bank Transactions

Inter-bank transactions also portend significant credit risk. These transactions are essentially for facilitation of fund transfers, settlement of securities transactions or because certain services are more economically performed by other banks due to their size or geographical location. An bank's lending policy should typically focus on the following:

- The establishment and observation of counter party credit limits.
- Any inter-bank transaction for which specific provisions should be made.
- The method and accuracy of reconciliation of the nostro and vostro accounts.
- Any inter-bank credit with terms of pricing that is not a market norm.

- The concentration of inter–bank exposure with a detailed listing of banks and amounts outstanding as well as lending limits.

3.3.10 Credit Classification and Provisioning Policy

Banks must have comprehensive policies, processes and methodologies for grading, classifying and monitoring all credit exposures (including off-balance sheet and forborne exposures) of individual credits and single obligors across the bank's various portfolios or at a portfolio level for credit exposures with homogeneous characteristics. These processes, policies and methodologies need to define criteria for identifying and reporting potential problem exposures in a timely manner to ensure that they are subject to more frequent monitoring as well as possible corrective action, classification and/or provisioning.

The credit policy must clearly outline the provisioning procedures for all credits and the capital charge to be held. This should comply at a minimum to the International Financial Reporting Standards, regulatory requirements and provisioning guidelines already issued by the Central Bank of Kenya.

3.4 Measuring and Monitoring Credit Risk

3.4.1 Measuring Credit risk

An bank should have procedures for measuring its overall exposure to credit risk as well as exposure to connected groups, products, customers, market segments and industries for appropriate risk management decisions to be made.

Internationally, the direction has been for banks to put in place stringent internal systems and models, which allow them to effectively measure credit risk. This risk measurement system assists banks to make provisions for credit risk and assign adequate capital. The effectiveness of the bank's credit risk measurement process is dependent on the quality of management information systems and the underlying assumptions supporting the models. The quality, detail and timeliness of the information is of paramount importance in determining the effectiveness of the credit risk management.

The measurement of credit risk should take account of:

(i) The specific nature of the credit (loan, derivative, facility, etc) and its contractual and financial conditions (maturity, reference rate, etc);
(ii) The exposure profile until maturity in relation to potential market movements;
(iii) The existence of collateral or guarantees; and

(iv) the potential for default based on the internal risk rating.

The analysis of credit risk data should be undertaken monthly with the results reviewed against relevant limits. Banks should use measurement techniques that are appropriate to the complexity and level of the risks involved in their activities, based on robust data and subject to periodic validation.

The bank should also undertake an analysis of the whole economy or in particular sectors to ensure contingency plans are developed for higher than expected levels of delinquencies and defaults.

An important tool in monitoring the quality of individual credits, as well as the total portfolio, is the use of an internal risk rating system. A well-structured internal risk rating system is a good means of differentiating the degree of credit risk in the different credit exposures of a bank. This will allow more accurate determination of the overall characteristics of the credit portfolio, concentrations, problem credits, and the adequacy of loan loss reserves. More detailed and sophisticated internal risk rating systems, used primarily at larger banks, can also be used to determine internal capital allocation, pricing of credits, and profitability of transactions and relationships.

Typically, an internal risk rating system categorizes credits into various classes designed to take into account the graduations in risk. Simpler systems might be based on five categories which include Normal, Watch, Substandard, Doubtful and Loss; however, more detailed systems with numerous ratings for credits may be considered.

3.4.2 Monitoring Credit Risk

An bank should have in place a system for monitoring the condition of individual credits. Key indicators of credit condition should be specified and monitored to identify and report potential problem credits. These would include indicators from the following areas:-

Financial Position and Business Conditions

Key financial performance indicators on profitability, equity, leverage and liquidity should be analysed as well as the operating environment of the obligor. When monitoring companies dependent on key management personnel or shareholders, such as small and medium enterprises, an bank should pay particular attention to assessing the status of these parties.

Conduct of Accounts

An bank should monitor the borrower’s principal and interest repayments, account activity, as well as instances of excesses over credit limits.

Loan Covenants
The borrower's ability to adhere to pledges and financial covenants stated in the loan agreement should be assessed and breaches detected should trigger prompt action.

Status and Valuation of Collateral
The value of collateral should be updated periodically to account for changes in market conditions. For example, where the collateral is property or shares, an bank should undertake more frequent valuations in adverse market conditions. If the facility is backed by an inventory or goods purportedly on the obligor's premises, appropriate inspections should be conducted to verify the existence and valuation of the collateral.

External Rating and Market Price
Changes in an obligor's external credit rating and market prices of its debt or equity issues could indicate potential credit concerns

Force Majeure Situation
The bank should consider any unforeseen circumstances that have come into play which might affect the borrower's ability to repay a facility.

In addition to monitoring the above risk indicators, an bank should also monitor the use of funds to determine whether credit facilities are drawn down for their intended purposes. Where a borrower has utilised funds for purposes not shown in the original proposal, the bank should determine the implications on the creditworthiness of the obligor. Exceptions noted during the monitoring process should be promptly acted upon and reported to management

An effective credit monitoring system should also include measures to identify contractual payment delinquencies and classify potential problem exposures on a timely basis and promptly direct problems for remedial management.

3.4.3 Credit Administration

Credit administration is critical in ensuring the soundness of the credit portfolio. It is the responsibility of management to set up a credit administration team to ensure that once a credit is granted it is properly maintained and administered. This will include record keeping, preparation of the terms and conditions as well as perfection and safe custody of the securities. Credit files of banks should contain the following information:

- Credit application.
- Evidence of approval.

- loan agreements, legal covenants and collateral.
- Latest financial information and statements from the borrower.
- Record and date of all credit reviews.
- Record of all guarantees and securities.
- Record of terms and conditions of facility.
- Evidence of securities validation function that should include legal validity, existence, valuation, registration of charge and safekeeping.
- Financial analyses and risk rating documentation.
- Internal memos and correspondence

The loan review function should determine that the credit files are complete and that all loan approvals and other necessary documents have been obtained.

While developing the credit administration process, banks should develop controls to ensure compliance with the applicable laws and regulations and internal policy. Adequate segregation of duties between approval and administration process should be maintained.

Ongoing administration of the credit portfolio is an essential part of the credit process. The credit administration function is basically a back office activity that supports and control extension and maintenance of credit. A typical credit administration unit performs the following functions:-

a. **Documentation -** It is the responsibility of credit administration to ensure completeness of documentation (loan agreements, guarantees, transfer of title of collaterals etc) in accordance with approved terms and conditions. Outstanding documents should be tracked and followed up to ensure execution and receipt.

b. **Credit Disbursement -** The credit administration function should ensure that the loan application has proper approval before entering facility limits into computer systems. Disbursement should be effected only after completion of covenants, and receipt of collateral holdings. In case of exceptions necessary approval should be obtained from competent authorities.

c. **Credit monitoring -** After the loan is approved and draw down allowed, the loan should be continuously monitored. These include keeping track of borrowers' compliance with credit terms, identifying early signs of irregularity, conducting periodic valuation of collateral and monitoring timely repayments.

d. **Loan Repayment -** The obligors should be communicated to ahead of time as and when the principal/markup installment becomes due. Any exceptions such as non-

payment or late payment should be tagged and communicated to the management. Proper records and updates should also be made after receipt.

e. **Maintenance of Credit Files -** Banks should devise procedural guidelines and standards for maintenance of credit files. The credit files should not only include all correspondence with the borrower but should also contain sufficient information necessary to assess the financial health of the borrower and its repayment performance.

f. **Collateral and Security Documents -** Banks should ensure that all security documents are kept in a fireproof safe under dual control. Registers for documents should be maintained to keep track of their movement.

Procedures should also be established to track and review relevant insurance coverage for certain facilities/collateral. Physical checks on security documents should be conducted on a regular basis.

Given the wide range of responsibilities of the credit administration function, its organisational structure varies with the size and sophistication of the bank. In larger banks, responsibilities for the various components of credit administration are mostly assigned to different departments. In smaller banks, a few individuals might handle several of the functional areas. Where individuals perform such sensitive functions as custody of key documents, wiring out funds or entering limits into the computer database, they should report to managers who are independent of the business origination and credit approval processes.

3.4.4 Credit Exposure and Risk Reporting

Credit risk information should be provided to the board and management with sufficient frequency, timelines and should be reliable. Reports should be generated on the credit activities both on and off balance sheet for example:

- Credit exposures by business line such as commercial, industrial sector, real estate, construction, credit cards, mortgage and leasing.
- Credit exposures relating to the composition of on and off balance sheet credits by major types of counterparties, including government, foreign corporate, domestic corporate, consumer and other financial institutions.
- Significant credit exposure in relation to individual borrowers or counterparties, related borrowers or groups of borrowers.
- Credit exposures by major asset category showing impaired and past due amounts relating to each category.

- Credit exposures restructured during a certain period and credits for which special conditions have been granted.

3.5 Management Information System

Banks must have information systems and analytical techniques that enable management to measure the credit risk inherent in all on- and off-balance sheet activities. The management information system should provide adequate information on the composition of the credit portfolio, including identification of any concentrations of risk.

The effectiveness of the bank's credit risk management is highly dependent on the quality, detail and timeliness of the information provided by its MIS. The information it generates should enable the board and all levels of management to fulfil their oversight roles. Information on the composition and quality of the bank's portfolios should allow management to assess the level of credit risk and the alignment with the credit risk strategy.
Management should review the existing scope of information periodically to ensure that it is sufficient for the complexity of the business. The MIS should also be able to provide information necessary for scenario analyses that capture evolving market and stressed conditions.

Banks should monitor actual exposures against established limits. Banks' MIS should ensure that exposures approaching risk limit are brought to the attention of senior management. All exposures should be included in a risk limit measurement system. Moreover, the MIS should allow the aggregation of credit exposures to individual borrowers and counterparties in a timely and comprehensive manner. The MIS should also report on exceptions to credit risk limits on a meaningful and timely basis.

3.6 Stress Testing

Banks should take into consideration current and forward-looking market and macroeconomic factors when assessing individual credits and their credit portfolios and should assess their credit risk exposures under stressful conditions.

There is a distinct difference in the nature and magnitude of credit risks faced by an bank under normal business conditions and under stress conditions, such as financial crises. Under stress conditions, asset values and credit quality may deteriorate by a magnitude not predicted by analysis of normal business conditions.

Stress testing is a tool that can be used to assess the impact of market dislocations on an bank's credit portfolio. It can aid the bank in estimating the range of losses that it could incur in stress conditions, and in planning appropriate remedial actions.

An important component of stress testing is the identification and simulation of stress conditions or scenarios an bank could encounter. The stress events and scenarios postulated should be plausible and relevant to the bank's portfolio. These scenarios could include economic or industry changes, market – risk events and liquidity conditions.

Banks must be in a position of analyzing the various situations in the economy or certain sectors to determine the event that could lead to substantial losses or liquidity problem. Whatever methods are used for stress testing, the output of these should be reviewed periodically and appropriate action taken by senior management in cases where results exceed agreed tolerance.

Stress test results should be reported to the board and senior management on a regular basis, at relevant levels of aggregation. Results of stress tests should, where appropriate, inform banks' calibration of limits.

3.7 Internal Controls and Audit

Banks must establish a system of independent, ongoing assessment of the bank's credit risk management processes, and the results of such reviews should be communicated directly to the Board of directors and senior management.

Banks' should have an efficient internal review and reporting system in order to manage effectively the bank's various portfolios. This system should provide the Board of directors and senior management with sufficient information to evaluate the performance of account officers and approval officers and the condition of the credit portfolio.

This function is necessary in order to independently enable the board determine whether the risk management process is working effectively, assessment of individual credits and the overall quality of the credit portfolio. The results of these audits should be communicated promptly to the directors and senior management. The review should provide sufficient information to the board and management to enable them evaluate accurately performance and condition of the portfolio. The credit review function should report directly to the board of directors or a board audit committee.

A review of the lending process should include analysis of the credit manuals and other written guidelines applied by various departments of a bank, and the capacity and

actual performance of all departments involved in the credit function. It should also cover origination, appraisal, approval, disbursement, monitoring, collection and handling procedures for the various credit functions provided by the bank.

The internal audit review team should ensure the following:-

- The credit granting function is carried out effectively.
- Credits are authorised within the guidelines established by the bank's board of directors.
- existence, quality and value of individual credits are accurately being reported to senior management
- The credit exposures are within the prudential and internal limits set by the board.
- Validation of significant change in the risk management process.
- Verification of the consistency, timeliness and reliability of data used for internal risk rating system.
- Credit activities are in compliance with the bank's credit policies and procedures.
- Adherence to internal risk rating system.
- Identification of areas of weaknesses in the credit risk management process.
- Exceptions to the policies, procedures and limits.

The internal audit should be conducted on a periodic basis and ideally not less than once a year. The audits should also identify weaknesses in the credit risk management process and any deficiencies in the policies and procedures.

4.0 LIQUIDITY RISK MANAGEMENT

4.1. Introduction

Liquidity risk is defined as the risk to an institution's earnings or capital arising from its inability to meet its obligations as they fall due, without incurring significant costs or losses.

Liquidity stress can lead to financial distress or even insolvency. More importantly, if not dealt with adequately and in a timely manner, the liquidity stress of an individual bank may trigger a crisis of confidence in the banking sector as a whole.

Liquidity risk management systems involve forecasting a bank's future cash flows by analyzing its on- and off-balance sheet positions, assessing its funding needs, and evaluating the availability, accessibility, and reliability of its funding sources and access to funding markets. This includes:

- identifying the funding markets to which the bank has access;
- understanding the nature of those markets;
- evaluating the bank's current and future use of those markets; and
- monitoring signs of erosion of market confidence.

4.2. Board and Senior Management Oversight

The prerequisites for effective liquidity risk management include an informed board, capable management, staff with relevant expertise and efficient systems and procedures. It is the responsibility of an institution's board and management to ensure that the institution has sufficient liquidity to meet its obligations as they fall due. It is primarily the duty of the board of directors to understand the liquidity risk profile of the institution and the tools used to manage liquidity risk.

The board has to ensure that the institution has necessary liquidity risk management framework, and that the institution is capable of confronting liquidity stress scenarios. The board should:

- Approve the institution's strategic direction and tolerance level for liquidity risk;
- Regularly review (at least annually) the institution's liquidity strategies, key policies, procedures, processes and practices (e.g., liquidity stress test framework and contingency funding plan).

- Appoint senior managers who have the ability to manage liquidity risk and delegate to them the required authority to accomplish the job;
- Continuously monitor the institution's performance and overall liquidity risk profile;
- Ensure that liquidity risk is identified, measured, monitored and controlled.

Senior management is responsible for the implementation of sound policies and procedures, keeping in mind the strategic direction and risk appetite specified by the board. To effectively oversee the daily and long-term management of liquidity risk, senior managers should:-

- Develop and implement liquidity strategy, policies, procedures and practices that translate the board's goals, objectives and risk tolerance into operating standards that are well understood by the bank staff;
- Adhere to the lines of authority and responsibility that the board has established for managing liquidity risk;
- Oversee the implementation and maintenance of management information and other systems that identify, measure, monitor, and control the bank's liquidity risk;
- Establish effective internal controls over the liquidity risk management process; and
- Ensure and review the contingency plans of the institution for handling disruptions to its ability to fund some or all of its activities in a timely manner and at a reasonable cost.
- Oversee the implementation of the stress testing process, regularly review scenarios, assumptions, and results, and use stress tests to inform liquidity management.

The responsibility for managing daily liquidity assessment resides with the Treasurer. However, the balance sheet liquidity management resides with the Asset and Liabilities Committee (ALCO). The ALCO should comprise senior management from key areas of the institution who identify/manage liquidity risk. It is important that these members have clear authority over the units responsible for executing liquidity-related transactions so that ALCO directives reach these line units unimpeded. The ALCO should meet monthly, if not more frequently.

A sound framework for managing liquidity risk has three dimensions:

- maintaining a stock of liquid assets that is appropriate to the institution's cash flow profile and that can be readily converted into cash without incurring undue capital losses;
- measuring, controlling and scenario testing of funding requirements; and
- Managing access to funding sources.

4.3. Liquidity Management Strategy

Institutions should have a liquidity management strategy that sets out their overall approach to managing liquidity on a day-to-day basis. The strategy should articulate the institution's longer-term approach to liquidity management, including the management of liquidity risk and maturity mismatch positions.

The strategy should;

a) Consider liquidity needs under normal and stressed conditions (considering institution-specific, market-wide, and combined scenarios).
b) Align with risk profile, business lines, balance sheet size, and risk appetite.
c) Be suitable for the institution's nature, size, and complexity.
d) Be regularly updated as market and macroeconomic conditions change.
e) Take into account legal structure, key business areas, and range of markets/products.
f) Consider jurisdictions in which it operates, and home and host regulatory requirements.

The liquidity strategy should be clearly documented and should include;

a) goals and objectives underlying the strategy;
b) composition and maturity of assets and liabilities;
c) management of liquidity across currencies, borders, business lines and legal entities;
d) intraday liquidity management;
e) an analysis of funding requirements under alternative scenarios;
f) the maintenance of a cushion of high-quality, unencumbered, liquid assets that can be used, without impediment, to obtain funding in times of stress;
g) diversification in the sources (including counterparties, instruments, currencies and markets) and tenor of funding, and regular review of concentration limits;
h) regular efforts to establish and maintain relationships with liability holders;
i) and regular assessment of the capacity to monetise assets.

An institution's liquidity risk management strategy should take into consideration the interdependencies between the various members of the same group in terms of liquidity. This includes the impacts of these interdependencies on the financial institution's liquidity risk.

4.4. Policies, Procedures and Limits

4.4.1. Policies

Institutions should formulate a comprehensive and responsive liquidity policy statement that takes into account all on- and off-balance sheet activities. The policy should be recommended by senior management and approved by the board of directors. While specific details vary across institutions according to the nature of their business, the key elements of any liquidity policy should include:

- General liquidity strategy (short and long-term), specific goals and objectives in relation to liquidity risk management, process for strategy formulation and the level of approval within the institution;
- Roles and responsibilities of individuals performing liquidity risk management functions, including structural balance sheet management, pricing, marketing, contingency planning, management reporting, lines of authority and responsibility for liquidity decisions;
- Liquidity risk management structure for monitoring, reporting and reviewing liquidity;
- Liquidity risk management tools for identifying, measuring, monitoring and controlling liquidity risk (including the types of liquidity limits and ratios in place and rationale for establishing limits and ratios);
- Where an institution is actively involved in multiple currencies and/or where positions in specific foreign currencies are significant to its business, its liquidity policy should address the measurement and management of liquidity in these individual currencies;
- The currencies should include a back-up liquidity strategy for circumstances in which its normal access to funding in individual foreign currencies is disrupted;
- Contingency plan for handling liquidity crisis; and
- Consideration of how other risks (e.g. credit, market, operational and reputational risks) may impact the bank's overall liquidity strategy.

To be effective, the liquidity policy must be communicated down the line throughout the organization. It is important that the board and senior management review these policies at least annually and when there are any material changes in the institution's current and prospective liquidity risk profile.

4.4.2. Procedures

Institutions should establish appropriate procedures and processes to implement their liquidity policies and include the following features:

- A procedures manual which should explicitly narrate the necessary operational steps and processes to execute the relevant liquidity risk controls;
- Periodic review and updating of the manual to take into account new activities, changes in risk management approaches and systems;
- Management should be able to accurately identify and quantify the primary sources of an institution's liquidity risk in a timely manner;
- To properly identify the sources, management should understand both existing as well as future risk that the institution can be exposed to; and
- Management should always be alert for new sources of liquidity risk at both the transaction and portfolio levels.

4.4.3. Limits

The Board of Directors and senior management shall establish limits for the nature and amount of liquidity risk that the institution is willing to assume.

i. Institutions may use a variety of ratios to quantify liquidity and create limits for liquidity management. To obtain a forward-looking view of liquidity risk exposures, a bank shall use metrics that assess the structure of the balance sheet, as well as metrics that project cash flows and future liquidity positions, considering off-balance sheet risks.
ii. Limits should take into account the following:

    a. the size, complexity and financial condition of the financial institution. Balance sheet complexity will determine how much and what types of limits a bank should establish over daily and long-term horizons.
    b. nature of the institution's strategies and activities, its past performance, the level of earnings, capital available to absorb potential losses, and the board's tolerance for risk.

iii. The limits should be periodically reviewed and adjusted -at least annually and when conditions or risk tolerances change.
iv. The responsibility for monitoring limits shall be assigned to a function independent of the funding areas.
v. A defined procedure for reporting limits exceptions to management shall be in place. Limit exceptions can be early indicators of excess risk or inadequate liquidity risk management.

While limits will not prevent liquidity crisis, limit exceptions can be early indicators of excessive risk or inadequate liquidity risk management.

4.5. Measuring and Monitoring Liquidity Risk

Liquidity measurement involves assessing an institution's cash inflows against its outflows and the liquidity value of its assets to identify the potential for future net funding shortfalls. An institution should be able to measure and forecast its prospective cash flows for assets, liabilities, off-balance sheet commitments and derivatives over a variety of time horizons, under normal conditions and a range of stress scenarios, including scenarios of severe stress.

An effective measurement and monitoring system is essential for adequate management of liquidity risk. Consequently, institutions should institute systems that enable them to capture liquidity risk ahead of time, so that appropriate remedial measures could be prompted to avoid any significant losses. An effective liquidity risk measurement and monitoring system not only helps in managing liquidity in times of crisis but also optimize return through efficient utilization of available funds.

4.5.1. Measurement of liquidity position

An institution should have a sound process for accurately measuring liquidity risk. The following are the tools that a bank should utilise at a minimum, in addition to the minimum liquidity standards, to measure its liquidity position. Liquidity position measurements tools provide a basis for monitoring the institution's liquidity risk and assessing its ability to meet funding obligations as they fall due. A bank must establish appropriate internal guidelines to ensure prompt corrective actions are undertaken to address any liquidity shortfall.

The Minimum Liquidity Ratio (MLR), Liquidity Coverage Ratio (LCR), and Net Stable Funding Ratio (NSFR) together provide a comprehensive and forward-looking assessment of liquidity adequacy and funding resilience. The MLR establishes the statutory minimum level of liquid assets, the LCR assesses an institution's ability to withstand a 30-day liquidity stress scenario, and the NSFR promotes a stable funding profile over a one-year horizon. The liquidity measurement standards with specific requirements are as detailed below:

4.5.1.1. Minimum Liquidity Ratio

Section 19 of the Banking Act requires that 'an institution shall maintain such minimum holding of liquid assets as the Central Bank may from time to time determine'. Currently an institution is required to maintain a statutory minimum of twenty per cent (20%) of all its deposit liabilities, matured and short term liabilities in liquid assets. The institution can however develop its own higher minimum liquidity ratio based on size, complexity and the risk appetite.

4.5.1.2. Liquidity Coverage Ratio

Liquidity Coverage Ratio (LCR) is intended to promote resilience to potential liquidity disruptions over a thirty-day horizon. The ratio ensures that institutions have sufficient unencumbered, high-quality liquid assets to offset the net cash outflows it could encounter under an acute short-term stress scenario. The value of the LCR must not be less than 100 percent.

$$LCR = \frac{Stock\ of\ High-Quality\ Liquid\ Assets}{Total\ Net\ Cash\ Outflow\ Over\ 30\ Day\ Period} \geq 100\ percent$$

4.5.1.3. Net Stable Funding Ratio (NSFR)

Net Stable Funding Ratio (NSFR) is defined as the amount of available stable funding relative to the amount of required stable funding. This ratio should be equal to at least 100 percent on an ongoing basis. "Available stable funding" is defined as the portion of capital and liabilities expected to be reliable over the time horizon considered by the NSFR, which extends to one year. The amount of such stable funding required ("Required stable funding") of a specific institution is a function of the liquidity characteristics and residual maturities of the various assets held by that institution as well as those of its off-balance sheet (OBS) exposures.

$$NSFR = \frac{Available\ amount\ of\ stable\ funding}{Required\ amount\ of\ stable\ funding} \geq 100\ percent$$

Additional tools for measuring and monitoring liquidity position

4.5.1.4. Loan to Deposit Ratio

Institutions should compute at month end, a loan to deposit ratio. Such ratio provides a simplified indication of the extent to which a bank is funding illiquid assets by stable liabilities. Institutions should set a trigger loan-deposit ratio above which liquidity risk management should be enhanced.

4.5.1.5. Contractual Maturity Mismatch

This is defined as the contractual cash and security inflows and outflows from all on- and off-balance sheet items, mapped to defined time bands based on their respective maturities. These maturity gaps indicate how much liquidity an institution would potentially need to raise in each of these time bands if all outflows occurred at the earliest possible date.

4.5.1.6. Cashflow Projections

Analyzing funding requirements involves the development of a maturity profile. Cash flow projections estimate a bank's inflows and outflows and identify net funding surpluses or deficits (gap) over various time horizons. These projections take into account the institution's funding requirements arising out of different sources and obligations across different time bands. Maturity profiles depend significantly on assumptions regarding future cash flows associated with assets, liabilities and off-balance sheet items. Institutions should document and review the assumptions utilized in managing liquidity frequently to determine that they continue to be valid, since an institution's future liquidity position will be affected by factors that cannot always be forecast with precision given the rapidity of change in financial markets.

4.5.1.7. Concentration of Funding

The more diversified an institution's funding structure (with respect to counterparties, products/instruments and currencies), the less likely it is that a substantial portion of funding will be withdrawn at the same time. This metric is meant to identify those sources of wholesale funding that are of such significance that withdrawal of this funding could trigger liquidity problems.

Institutions are required to:

a. diversify available funding sources in the short, medium and long term;
b. consider correlations between sources of funds and market conditions;
c. include limits by counterparty, secured versus unsecured market funding, instrument type, securitisation vehicle, currency and geographic market.

Counterparties and instruments/products that account for more than 1 percent of a bank's total balance sheet are considered significant. In addition, any currency for which aggregate liabilities represent 5 percent or more of the bank's total liabilities is considered a significant currency and should be monitored across the following time horizons: less than one month, one to three months, three to six months, six to twelve months, and beyond twelve months.

4.5.1.8. Liquidity Coverage Ratio by significant currency

While the LCR is required to be met in one single currency, in order to better capture potential currency mismatches, institutions should monitor the LCR in significant currencies.

The definition of the stock of high-quality foreign exchange assets and total net foreign exchange cash outflows should mirror those of the LCR for common currencies.

$$Foreign\ Currency\ LCR = \frac{Stock\ of\ HQLA\ in\ each\ significant\ currency}{Total\ net\ cash\ outflows\ over\ a\ 30\ day\ time\ period\ in\ each\ significant\ currency}$$

Institutions should establish internal limits and monitoring thresholds for significant-currency LCRs, taking into account the availability of HQLA and funding sources in each currency under both normal and stressed conditions.

4.5.2. Monitoring Liquidity

4.5.2.1. Management Information System

Key elements of an effective risk management process include an efficient Management Information System (MIS) and systems to identify, measure, monitor and control risks. The MIS should be integrated into the overall MIS of the institution across the institution to provide timely, accurate and reliable information for liquidity risk management. It should link all functions involved in treasury activities, i.e. the dealing room, treasury operations, finance and risk management function, to facilitate effective monitoring, reporting and decision-making.

A strong MIS that is flexible enough to deal with various contingencies that may arise is central to making sound decisions related to liquidity. It should provide the board of directors, senior management and other appropriate personnel with timely and forward-looking information on the liquidity position of the bank.

To effectively manage and monitor its net funding requirements, an institution should have the ability to calculate its liquidity positions across a range of time horizons. This should include the calculation of liquidity positions on an intraday basis, on a day-to-day basis for shorter time horizons, and over longer-term time horizons.

The MIS should have the ability to calculate liquidity positions in all of the currencies in which the bank conducts business; both individually and on an aggregate basis. The MIS should be used in day-to-day liquidity risk management to monitor compliance with the bank's established policies, procedures and limits.

4.5.2.2. Early Warning Indicators

An institution should establish and monitor early warning indicators (EWIs). These provide insights into the institution's risk profile and flag potential deterioration in its liquidity position. An institution should implement formalized processes to monitor these indicators, including clearly defined triggers or thresholds and escalation and reporting procedures.

Frequency of monitoring and parties responsible for monitoring should also be clearly laid out. When indicators suggest increased risk, prompt assessment and, if necessary, management action should be taken to mitigate emerging risks. EWIs can be qualitative or quantitative in nature and may include, but are not limited to, the following:

Relating to an institution's liquidity profile;

a) rapid asset growth, especially when funded by unstable funding sources, which could lead to asset and liability mismatches;
b) rapid deposit growth, which could be vulnerable to sudden reversals;
c) growing concentrations in assets or liabilities (e.g., concentration to a specific sector or single borrower/depositor);
d) increases in currency mismatches;
e) repeated incidents of positions approaching or breaching internal limits;
f) deterioration in regulatory metrics, e.g., LCR, NSFR, LR;
g) increasing retail and wholesale deposit outflows (e.g., increasing outflows from high value retail deposits and wholesale fund providers);
h) a decrease of weighted average maturity of liabilities;
i) increasing redemptions of certificates of deposit before maturity;
j) difficulty accessing longer-term funding;
k) worsening intraday liquidity indicators (e.g., nostro accounts balances falling below the institution's pre-set internal threshold, operational problems in payment and settlement systems);
l) deterioration in internal stress test results relating to an institution's financial conditions; and
m) negative trends or heightened risk associated with a particular product line, such as rising delinquencies.

Relating to counterparties' responses;

n) counterparties request increased margins and additional collateral for credit granted or resist entering into new transactions; and

o) correspondent banks eliminate or decrease the bank's credit lines.

With the increased use of digital banking, customers can now transfer funds instantaneously without the friction of requiring in-person withdrawals. Coupled with the speed of information (and misinformation) dissemination through social media, institutions are more vulnerable to rapid deposit outflows when customer confidence is impacted. To address these developments and enable swift responses, an institution should:

a) strengthen its MIS capabilities and tools to allow rapid assessment of its liquidity positions (e.g., in real-time), including beyond normal business hours; and
b) enhance its monitoring capabilities to analyse trends from both news and social media platforms, enabling timely intervention when necessary.

4.5.2.3. Key Liquidity Factors

The following key liquidity factors should be monitored closely:

- The maturity profile of cash flows under varying scenarios;
- The stock of liquid assets available to the institution and their market values;
- The ability of an institution to execute assets sales in various markets (notably under adverse conditions) and to borrow in markets;
- Potential sources of volatility in assets and liabilities (and claims and obligations arising from off-balance sheet business);
- The impact of adverse trends in asset quality on future cash flows and market confidence in the bank;
- Credit standing and capacity of providers of standby facilities to meet their obligations;
- The impact of market disruptions on cash flows and on customers;
- Intra-group cash flows and the accessibility of intra-group funding; and
- The type of new deposits being obtained, as well as its source, maturity, and price.

4.5.2.4. Asset and Liability Committee (ALCO)

In order to effectively monitor its liquidity risk, an institution is supposed to establish an Asset and Liability Committee (ALCO) with the following roles:

a) Management of the overall liquidity of the institution;
b) ALCO must report directly to the Board or in the case of a foreign incorporated bank, to senior management of the institution in the country;

c) ALCO must facilitate, coordinate, communicate and control balance sheet planning with regards to risks inherent in managing liquidity and convergences in interest rates; and
d) ALCO is responsible for ensuring that a bank's operations lies within the parameters set by its Board of Directors. However, the ALCO is not responsible for formulating the in-house liquidity risk management policy.

In determining the composition, size and various roles of the ALCO, the Board is required to consider the size of the institution, the risks inherent in the institution's operations and the organizational complexity.

All institutions are required to maintain written report of the deliberations, decisions and roles of the ALCO with regards to liquidity risk management.

4.5.3. Intragroup liquidity monitoring

i. An effective liquidity risk management requires a good understanding of the funding positions of all entities in the bank's group that could affect the bank's liquidity.
ii. Intragroup liquidity management arrangements may significantly influence the risk profile, profitability, capitalization and reputation of an institution. On one hand, an institution may be required to provide liquidity to the other members of the group and, on the other hand, funds provided to the institution by other members of the group may be withdrawn or cancelled, particularly in the event of a crisis.
iii. Regardless of its organizational structure and degree of centralized or decentralized liquidity risk management, an institution should actively monitor and control liquidity risks at the level of individual legal entities, and foreign branches and subsidiaries, and the group as a whole.
iv. Institutions should incorporate processes that aggregate data across multiple systems in order to develop a group-wide view of liquidity risk exposures and identify constraints on the transfer of liquidity within the group.
v. An institution should consider establishing internal limits on intragroup liquidity risk to mitigate the risk of contagion under stress.
vi. An institution may also establish limits at the subsidiary and branch level to restrict the reliance of related entities on funding.

4.5.4. Management of Intraday Liquidity

i. An institution should actively manage its intraday liquidity positions and risks to meet payment and settlement obligations on a timely basis under both normal and stressed conditions.

ii. An institution's failure to manage intraday liquidity effectively could leave it unable to meet its payment obligations at the time expected, thereby affecting its own liquidity position and that of other parties.

iii. An institution's strategy to achieve its intraday liquidity management objectives shall have at least the following six operational elements:

a) the capacity to measure expected daily gross liquidity inflows and outflows;
b) monitor intraday liquidity positions against expected activities and available resources;
c) arrange to acquire sufficient intraday funding to meet its intraday objectives;
d) manage and mobilize collateral as necessary to obtain intraday funds;
e) manage the timing of its liquidity outflows in line with its intraday objectives; and
f) be prepared to deal with unexpected disruptions to its intraday liquidity flows.

4.5.5. Foreign Currency Liquidity Management

Where an institution's foreign currency business is significant, or the institution has significant exposure in a given currency, the bank is required to undertake separate analysis of its strategy and monitor its liquidity needs separately for each such significant currency. This includes the use of stress testing to determine the appropriateness of mismatches in that currency and, where appropriate, setting regular review of limits on the size of its cash flow mismatches for foreign currencies in aggregate and for each significant currency individually.

4.5.6. Contingency Funding Planning

In order to develop a comprehensive liquidity risk management framework, institutions should have way out plans for stress scenarios. A Contingency Funding Plan (CFP) is a set of formally articulated and adequately documented policies, procedures and action plans that serve as a blueprint for a bank to meet its funding needs in a timely manner and at a reasonable cost. It is a projection of future cash flows sources of a bank under market scenarios including aggressive asset growth or rapid liability erosion. To be effective it is important that a CFP represent management's best estimate of balance sheet changes that may result from liquidity or credit events. Effective CFP should consist of several components:

- Provide specific procedures to ensure timely and uninterrupted information flows to senior management. Clear division of responsibility within management in a crisis, including the authority to invoke the CFP.

- Names and contact details of members of the team responsible for implementing the CFP and the locations of team members; and the designation of alternates for key roles.
- Action plans for altering asset and liability behaviors (i.e., market assets more aggressively, sell assets intended to hold, raise interest rates on deposits).
- An indication of the priority of alternative sources of funds (i.e., designating primary and secondary sources of liquidity).
- A classification of borrowers and trading customers according to their importance to the institution in order to maintain customer relationships; and
- Plans and procedures for communicating with the media. Astute public relations management can help a bank to avoid the spread of rumors that could result in a significant run-off of funds.

4.5.7. Stress Testing

An institution should conduct stress tests on a regular basis for a variety of short-term and protracted institution-specific and market-wide stress scenarios (individually and in combination) to identify sources of potential liquidity strain and to ensure that current exposures remain in accordance with a bank's established liquidity risk tolerance. A bank should use stress test outcomes to adjust its liquidity risk management strategies, policies, and positions and to develop effective contingency plans.

Stress testing involves subjecting institution's liquidity position to several scenarios and assessing whether the institution can withstand liquidity shocks. In designing stress scenarios, the nature of the institution's business, activities and vulnerabilities should be taken into consideration so that the scenarios incorporate the major funding and market liquidity risks to which the bank is exposed. These include risks associated with its business activities, products (including complex financial instruments and off-balance sheet items) and funding sources. The assumptions should be reasonable, supported by sufficient evidence, and documented.

The scenario entails significant stress, albeit not a worst-case scenario, and assumes the following:

- a significant downgrade of the institution's public credit rating;
- loss of major depositor funds and significant withdrawal of retail deposits:
- a significant change in market interest rates;
- a significant increase in demand for loans and other funding;

- increases off-balance sheet exposures, including committed credit and liquidity facilities.
- unavailability/impaired unsecured/secured wholesale funding sources;
- shortening of funding tenors;
- heightened liquidity drains associated with complex products/transactions;
- accelerated balance sheet growth;
- surge in intraday liquidity demands; and
- constraints on liquidity transfer across entities, sectors and borders taking into account legal, regulatory, operational and time zone restrictions and constraints.

Banking groups should ensure that a set of consistent scenarios and assumptions is run on a groupwide basis to assess group liquidity conditions. However, circumstances may warrant a differentiated treatment (e.g., a particular outflow assumption) more reflective of local locations and these can be factored in after careful consideration by head office/parent/group.

In addition, liquidity transferability, particularly in cross-border operations, should be assessed under stress. Institutions shall:

a) Evaluate impediments to liquidity transfer in stressful conditions.
b) Identify and document appropriate contingency measures.

Stress test results (along with key scenario assumptions) and vulnerabilities, along with any recommended actions should be reported to and discussed with the board and senior management. To the extent that the stress test outcomes exceed an institution's liquidity risk appetite, senior management should adjust liquidity positions and contingency funding plans in consultation with the board.

4.5.8. Internal Controls and Audit

In order to have effective implementation of policies and procedures, institutions should institute review processes that should ensure the compliance of various procedures and limits prescribed by senior management. Institutions should have an adequate system of internal controls over the liquidity risk management process. There should be regular, independent reviews and evaluations of the effectiveness of the system. A fundamental component of the internal control system should include:

- A strong control environment;
- An adequate process for identifying and evaluating liquidity risk;

- The establishment of control activities such as policies and procedures and adequate information systems with regular independent reviews and evaluations of the effectiveness of the system; and
- Ensuring that appropriate revisions or enhancements to internal controls are made.

Institutions should ensure that all aspects of the internal control systems are effective, including those that are not directly part of the risk management process. Periodic reviews should be conducted to verify the level of liquidity risk and management's compliance with limits and operating procedures. Any exceptions should be reported immediately to senior management/board for necessary action to be taken.

5.0 MARKET RISK MANAGEMENT

5.1 Introduction

Market risk is the risk that the value of on and off-balance sheet positions of a financial institution will be adversely affected by movements in market rates or prices such as interest rates, foreign exchange rates, equity prices, credit spreads and/or commodity prices resulting in a loss to earnings and capital.

Institutions may be exposed to Market Risk in a variety of ways. Market risk exposure may be explicit in portfolios of securities / equities and instruments that are actively traded. It may also arise in form of interest rate risk due to mismatch of loans and deposits and from activities categorized as off-balance sheet items. Therefore, market risk is potential for loss resulting from adverse movement in market risk factors such as interest rates, foreign exchange rates, equity and commodity prices.

What constitutes adequate market risk management practices can vary considerably from one institution to the other. For example, less complex institutions whose senior managers are actively involved in the details of day-to-day operations may be able to rely on relatively basic market risk management processes. However, institutions that have more complex and wide-ranging activities are likely to require more elaborate and formal market risk management processes, to address their broad range of financial activities and to provide senior management with the information they need to monitor and direct day-to-day activities.

The risk arising from market risk factors can be categorized into the following categories:

- Interest rate risk
- Price Risk
- Foreign Exchange risk

5.1.1 Interest rate risk

Interest rate risk is the current or prospective risk to earnings and capital arising from adverse movements in interest rates.

This risk appears when monetary flows of assets, with respect to capital and interest, do not correspond to the monetary flows of liabilities, with respect to capital, interest and services.

The monetary flows of an institution can be uncertain. This uncertainty results, among other factors, from the existence of inherent variations in the asset and liability elements, as well as inherent options.

The sources of interest rate risk are thus mainly three fundamental factors:

- basis risk: the imperfect correlation in the adjustment of borrowing and lending rates on various instruments;
- the yield curve risk for rates resulting from different instrument pricing;
- the rate repricing risk;

Excessive interest rate risk can pose a significant threat to an institution's earnings and capital base. Changes in interest rates affect an institution's earnings by changing its net interest income and the level of other interest-sensitive income and operating expenses. Changes in interest rates thus can have adverse effects both on an institution's earnings, capital and its economic value.

5.1.2 Price Risk

Price risk is the risk that an institution may experience loss due to unfavorable movements in market prices. It arises from the volatility of positions taken in the four fundamental economic markets: interest-sensitive debt securities, equities, currencies and commodities. The volatility of each of these markets exposes institutions to fluctuations in the price or value of on- and off- balance sheet marketable financial instruments.

5.1.3 Equity Risk

Equity risk is the potential for reduced income or losses in on- and off-balance sheet positions arising from adverse changes in equity prices.

5.1.4 Commodity Risk

Commodity risk is the risk that on- or off-balance sheet positions will be adversely affected by movements in commodity prices. Commodities include agricultural products, minerals and precious metals. In addition to directional risk arising from changes in their spot prices, institutions should also take into account basis risk while they measure their commodity risk (basis risk is the risk that the relationship between prices of similar commodities alters through time).

Likewise other risks, the concern for management of the equity and commodity risks must start from the top management. Effective board and senior management oversight of the institution's overall equity and commodity risk exposure is cornerstone of risk management process.

5.1.5 Foreign Exchange risk

Foreign exchange risk is the current or prospective risk to earnings and capital arising from adverse movements in currency exchange rates. The potential for loss arises from the process of revaluing foreign currency positions on both on- and off- balance sheet items.

The amount of the risk depends on the scale of the possible fluctuations of rates and the degree and duration of the exposure to the currency risk.

As with the other categories of risk, management of exchange rate risk includes oversight by the Board of Directors, development of exchange rate risk management program, policies, limits and delegations of powers.

5.2 Market Risk Management Framework

An Institution should establish a sound, comprehensive, reliable and forward-looking market risk management framework. At a minimum it should incorporate:-

- effective oversight and management by the board of directors and senior management, respectively;
- comprehensive policies, procedures, systems and controls for identifying, measuring, monitoring and controlling market risk, including but not limited to stress testing or scenario/sensitivity analysis;
- robust reporting systems and processes that provides sufficient information to the Board and senior management on market risk;
- sound internal controls and independent review procedures; and
- effective mechanisms for market risk capital allocation.

An Institution should incorporate its market risk management framework into its overall risk management system. This would enable the institution to understand and manage its consolidated risk exposure more effectively. In addition, where the institution is part of a

group, the market risk management processes should, as far as possible, be integrated across the group.

The market risk management framework should align with the institution's risk appetite and risk tolerance. It should also be commensurate with the nature, scale, risk, complexity of the institution's trading, other financial activities and market risk exposures.

The framework should reflect an understanding of the potential market risk implications of the institution's business activities, products and strategies.

The market risk management framework (along with any changes) must be documented and approved by the institution's Board.

5.2.1 Board and Senior Management Oversight

5.2.1.1 The Board of Directors

Effective Board and senior management oversight is critical to sound risk management and should therefore be an integral part of the institution's market risk management infrastructure.

The Board of an institution has ultimate responsibility for the governance of market risk and should ensure that an overarching enterprise-wide risk management framework is in place. The enterprise-wide risk management framework should adequately addresses market risk proportionate to its size, complexity and risks. The Board should, at a minimum: -

a) establish an enterprise-wide market risk appetite and tolerance that is forward looking and takes into account, inter alia, the institution's short and long term strategic goals, business model, available resources and internal and regulatory capital targets and other regulatory requirements;

b) understand the nature and level of the institution's market risk exposure and the extent to which these exposures affect enterprise-wide operations and strategic plans. The Board should understand how market risk is managed and appreciate how this risk may affect the financial institution's soundness. The Board should also have an understanding of the methodologies used by senior management to evaluate the institution's market risk profile;

c) formulate and approve broad business strategies and policies that govern the market risk of the institution. Accordingly, the board of directors is responsible for approving

the overall policies with respect to interest rate risk, price risk and foreign exchange risk.

d) review the overall objectives of the institution with respect to market risk and ensure the
provision of clear guidance regarding the level of market risk acceptable to the institution.

e) review and approve the procedures to measure, manage and control price risk within which foreign exchange transactions shall be conducted.

f) identify and have a clear understanding of the price risks inherent in the institution's investment portfolio and make appropriate efforts to remain informed about these risks as the institution's activities evolve.

g) define senior management's authority and responsibilities and oversee senior management's compliance with Board approved policies and limits. The Board should also ensure that senior management implements market risk strategies, policies and processes that are aligned with the institution's risk appetite and tolerance and fully integrated into the institution's overall risk management process;.

h) review and approve the institution's market risk management framework, including the risk appetite, risk tolerance, strategies, policies and procedures at least annually or more frequently where, for example, there are changes in financial performance, changes to business strategy or activities, or changes in market conditions that may impact the institution's market risk profile; and

i) periodically review information that is sufficient in detail and timeliness to allow it to understand and assess the performance of senior management in monitoring and controlling risks in compliance with the institution's board-approved policies.

5.2.1.2 Senior Management

The senior management has the responsibility of implementing all approved policies that govern market risk and develop procedures for effective management of the risks. Management should be sufficiently competent and able to respond to price risks, interest risks and foreign exchange risks that may arise from changes in the competitive environment or from innovations in markets in which the institution is active.

The senior management of a financial institution should ensure that the Board approved market risk management framework is effectively implemented throughout the institution. At a minimum, senior management should:-

a) develop policies, procedures and strategies for managing and controlling market risk (including limits and controls) that are documented and accord with the Board's market risk goals, objectives, risk appetite and tolerance ensuring that these are appropriately communicated throughout the institution;

b) adhere to the lines of authority and market risk policies and limits established and approved by the Board;

c) establish a market risk measurement system and document standards, procedures and methodologies for measuring market risk, valuing positions and assessing performance, including, for example, procedures for updating stress scenarios and key underlying assumptions driving the institution's market risk analysis;

d) monitor compliance of relevant business units with the prescribed market risk lines of authority and responsibilities and ensure that staff responsible for analysis and market risk management are knowledgeable, capable and experienced given the characteristics and sophistication of the market risk exposures undertaken by the financial institution;

e) implement and maintain systems that allow for monitoring market risk institution wide and facilitate accurate and timely reporting to the Board, the Central Bank and other relevant stakeholders;

f) establish effective market risk internal controls;

g) implement a comprehensive market risk reporting system that provides key aggregate information on the institution's market risk in sufficient detail that would allow for sound evaluation and decision making by the Board and Senior management;

h) review the institution's market risk policies, procedures and strategies, at least annually. The reviews should, inter alia, ensure consistency with the Board's market risk goals, objectives, risk appetite and tolerances, ensure continued relevance and help to identify where updates may be needed. Senior management should, where appropriate, make recommendations for changes that should be presented to the Board for approval;

i) ensure that market risk analysis (including analyses of the respective markets in which the

institution has or intends to have market risk exposures) and risk management activities are conducted by competent staff with technical knowledge and experience, consistent with the nature and scope of the institution's activities.

j) in conjunction with the Board, evaluate the effectiveness of the market risk management framework; and

k) establish a system of independent review.

5.3 Evaluation of the market risk

To manage the market risk, the institution must be cognizant of the value of its risk exposure and the impact of market fluctuations on the risk position. Availability of accurate data will enable, the institution to take appropriate measures on a timely basis,

Each institution should put in place techniques for evaluation of risks that accurately measure the impact of future market fluctuations. The choice of scenarios should take into account the volatility of rates, prices and take into account reasonable time bands to facilitate flexibility to unfavorable market fluctuations.

Model to be used to measure and mitigate institutions' exposure to market risk, must have been evaluated independently. These models must be revised as a function of the scale of exposure to market risk, the nature of market variations and the complexity of innovations associated with interest rate and price measurement.

5.4 Policies, Procedures and Limits

5.4.1 Policies

Institutions should have clearly defined policies and procedures for limiting and controlling market risk on both on- and off- balance sheet positions. These policies should be applied on a consolidated basis and as appropriate, at specific affiliates or other units of the institution.

Policies and procedures should be proportionate to the nature, size and complexity of the institution. Policies and procedures should also provide definitive market risk management guidance across the institution and should:

a) Detail the process by which the Board determines the institution's market risk appetite and tolerance;

b) Be aligned to the risk appetite and tolerance of the institution, providing robust parameters for risk taking by staff;

c) Be effectively communicated to all relevant staff and embedded within the culture of the financial institution;

d) Delineate lines of responsibility and accountability over market risk management decisions and should clearly define authorized instruments, hedging strategies and position-taking opportunities.

e). Identify the types of instruments and activities that the institution may employ or conduct, thus acting as a means through which the board can communicate their tolerance of risk on a consolidated basis and at different legal entities.

f). Identify quantitative parameters that define the levels of interest rate risk, price risk and foreign exchange risk acceptable for the institution and where appropriate, such limits should be further specified for certain types of instruments, portfolios and activities.

g) Apply on a consolidated basis, where appropriate;

h) Be reviewed, at least annually, to ensure they continue to be relevant;

i) Delineate the lines of authority and the responsibilities of the Board, senior management and other personnel responsible for managing market risk. They should include approval thresholds for different levels of staff and clearly outline how exceptions from these approved limits should be addressed;

j) Set out general methods for market risk identification that, among other things, clearly identifies and assesses the scope of activities that expose the institution to market risk and evaluates the degree of market risk inherent in those activities;

k) Establish how market risk is to be measured and communicated throughout the institution, including communication to the Board. These should cover, inter alia:-

i. methodologies and benchmarks for the measurement and management of market risk;

ii. the valuation process including policies and processes for making appropriate valuation adjustments for uncertainties in determining the fair value of assets and liabilities. such as positions that otherwise cannot be prudently valued, including concentrated and less liquid positions and clearly defined responsibilities of the various areas involved in the process;

iii. assumptions and parameters underlying the measurement system (and stress tests) which should be proportionate to the nature scale and complexity of the institution.

l) Outline appropriate strategies and internal controls including risk limits and segregation of duties that are consistent with the institution's risk appetite, risk profile and capital strength.
Policies should address strategies and limits for areas including trading desks (currencies, sources of funds), investment portfolios (high risk investments, portfolio mix, geographic regions, sectors, types of instruments), products (types of loans, types of accounts), instruments (issuance of shares, bonds, etc.);

m) describe the manner and frequency of market risk monitoring and reporting to be undertaken
including exception tracking and exception reporting;

n) set out the process and frequency of independent reviews (such as the internal audit function) of the institution's market risk management framework;

o) ensure that significant new strategies, products, and business units are integrated into the market risk management process. For new products, at a minimum, the procedures should outline the:-

i. steps to be taken to assess the levels of market risk and sources of market risk associated with the product;

ii. measures that could be undertaken to mitigate the risk; and

iii. market risk limits for the new product.

q) comprehensively consider the market risk that emanates from the various business units of the institution;

r) provide controls over permissible market risk mitigation activities such as hedging strategies;

s) address business continuity in the event of market risk issues that may impact the institution on a stand-alone basis or arising from systemic market risk events;

t) where applicable, outline the process for determining capital adequacy for market risk ensuring that the method of calculating market risk for capital adequacy purposes complies with standards prescribed by the Central Bank;

Prior to introducing a new product, hedging, or position-taking strategy, management should ensure that adequate operational procedures and risk control systems are in place. The board or its appropriate delegated committee should also approve major hedging or risk management initiatives in advance of their implementation.

5.4.2 Procedures

Institutions should establish appropriate procedures for implementation of market risk policy, and processes.

(a) These should be documented in a manual and the staff responsible for carrying out the procedures should be familiar with the content of the manual.

(b) The manual should set out the operational steps and processes for executing the relevant market risk controls.

(c) The manual should also be periodically reviewed and updated to take into account new activities, changes in systems and structural changes in the market.

(d) The procedures should cover all activities that are exposed to market risk.

Institutions should have clearly defined policies and procedures for limiting and controlling market risk on both on- and off- balance sheet positions. These policies should be applied on a consolidated basis and as appropriate, at specific affiliates or other units of the institution. Such policies and procedures should:

- Be designed to reflect the importance and complexity of the market risk to which the institution is exposed.

- Delineate lines of responsibility and accountability over market risk management decisions and should clearly define authorized instruments, hedging strategies and position-taking opportunities.
- Identify the types of instruments and activities that the institution may employ or conduct, thus acting as a means through which the board can communicate their tolerance of risk on a consolidated basis and at different legal entities.
- Identify quantitative parameters that define the levels of interest rate risk, price risk and foreign exchange risk acceptable for the institution and where appropriate, such limits should be further specified for certain types of instruments, portfolios and activities.
- Review and revise periodically the procedures so as to define the specific procedures and approvals necessary for exceptions to policies, limits and authorizations.
- Delineate a clear set of institutional procedures for acquiring specific instruments, managing portfolios and controlling the institution's aggregate market risk exposure.

5.4.2 Risk Limits

Each institution must establish prudent and precise limits for market risk. The level of exposure to market risk should not exceed set limits and should comply with the institution's guidelines on the risk.

To determine these limits, the institution must consider risk exposures.These limits must be reassessed regularly to reflect changes in the institution's risk profile.

An appropriate limit system should: -

- Enable management to control market risk exposures, initiate discussion about opportunities and risks and monitor actual risk taking against predetermined risk tolerances;
- Ensure that positions that exceed certain predetermined levels receive prompt management attention;
- Be consistent with overall approach to measuring market risk;
- Establish risk limits for business units, where appropriate, be approved and periodically be reviewed by the Board and senior management respectively. Changes in market conditions or the resources of the Institution should prompt a re-assessment of limits;
- Preferably be integrated, where applicable, with group-wide limits for each major type of risk assumed.
- Be appropriate to the size, complexity and capital adequacy of the institution as well as its ability to measure and manage its risk; and

- Be identifiable with individual business unit, portfolios, instrument types or specific instruments.

Institutions must have adequate information systems for measuring, monitoring, controlling and reporting market risk exposures. Reports must be provided on a timely basis to the board of directors, senior management and, where appropriate, individual business line managers.

The following are some of the board reports that should be provided:

- Violation of approved responsibilities by managers when taking interest rate risk exposures. or investing in un- approved instruments.
- Excesses over approved interest rate limits;
- Any exceptions highlighted by the internal auditor.

Compliance with limits should be monitored by a unit independent of the risk-taking activities. A Institution should have procedures prescribing the course of action for limit excesses. These actions should include investigating the reasons for the excesses, reporting the incidents to management and seeking approval from the Board or senior management. These procedures should also prescribe the actions required for the approval of temporary excesses and limit increases.

5.4 Measurement, Monitoring and Control

5.4.1 Risk Measurement

Institutions should implement suitable measures for all market risks assumed. The monitoring of these measures should be integrated into daily risk management process. The broad risk types to be measured are outlined below.

5.4.1.1 Interest Rate Risk

An institution should incorporate re-pricing risk (arising from differences between the timing of rate changes and the timing of cash flows), yield curve risk (arising from changing rate relationships across the spectrum of maturities), basis risk (arising from changing rate relationships among yield curves that affect the Institution's activities) and optionality risks (arising from interest rate related options embedded in the Institution's products). The Institution should also consider fee income that is sensitive to changes in interest rates.

Interest rate risk in each currency should be calculated separately. Yield curves should be divided into various maturity segments to capture variation in the volatility of rates along the yield curves. For each currency, the number of yield curves should reflect the risk factors that the institution is exposed to. There should be additional risk measures to capture credit spread and swap spread risks. For bonds and similar instruments, specific risk must also be measured.

5.4.1.2 Foreign Exchange Risk

An institution should calculate foreign exchange (FX) risk in each currency. Foreign exchange risk should include asset-liability mismatch of foreign currencies to the domestic currency. An Institution trading in non-deliverable foreign currencies should set limits reflecting the unique risk characteristics of these currencies. These characteristics include market liquidity, event and settlement date mismatch risks.

5.4.1.3 Commodity Risk

Commodities pose risks such as basis risk (the risk that the relationship between prices of similar commodities alters through time), interest rate risk (the risk of a change in the cost of carry for forward positions and options), forward gap risk (the risk that the forward price may change for reasons other than a change in interest rates) and directional risk arising from changes in their spot prices. An institution that is active in commodities trading should account for variations in the "convenience yield" between derivatives positions, such as forwards and swaps, and cash positions in the commodity. All significant levels of commodity exposures should be properly managed.

5.4.1.4 Credit Trading Risk

An institution that takes positions in credit instruments, such as bonds and credit derivatives, is exposed to the risks of changes in the credit spreads of the underlying issuers. Credit spread is premium above government or risk-free risk, required by the market for taking on credit exposures. Credit instruments are susceptible to default risk as well as credit migration risk. Default risk is the risk of direct losses from an obligor’s default and of indirect losses that could arise from a default event. Credit migration risk is the risk of direct losses from rating downgrades or upgrades and of indirect losses that could arise from a credit migration event. Institutions should identify, measure, monitor, control and report such risks.

5.4.1.5 Market Liquidity Risk

Market liquidity risk is the risk that an institution is unable to liquidate or offset a position at or near the last traded market price due to inadequate market depth or market disruptions. Available liquidity at any point is also a function of the size of trades that an Institution transacts at relative to the market. The institution should continually evaluate trading liquidity risk and its ability to hedge its positions.

All significant market risks, as determined by the Institution's definition of material risk, should be measured and aggregated on an institution-wide basis to the fullest extent possible. Where it is not possible to quantify the risk, the institution should seek to understand and report the risk qualitatively.

5.4.2 Risk monitoring and control

Institution's should establish a sound and comprehensive risk management process to monitor and control its market risk. This process should include, among other things,

- an appropriately detailed structure of risk limits, guidelines and other parameters used to govern market risk taking;
- an appropriate management information system (MIS) for controlling, monitoring and reporting market risk,
- accounting policies on the treatment of market risk.

Institutions should have a system that should be able to measure current exposures, through marked-to-market or marked-to-model pricing, as well as potential market risks. The institution's risk management system should, at least, provide the following information on a daily basis:

- the outstanding positions,
- unrealized profit or loss,
- the accrued profit or loss.

Institutions should ensure the integrity of data used by their risk management systems. Data used should be:

- appropriate (e.g. marked-to-market data for trading activities),
- accurate,
- complete (e.g. both on- and off-balance sheet positions),
- timely,
- frequently updated, and

- sourced independently of the position-taking units.

An Institution whose risk levels fluctuate significantly within a trading day should monitor its risk profile on an intra-day basis. The risk management system should, wherever feasible, be able to assess the probability of future losses. It should also enable an institution to identify risks promptly and take quick remedial action in response to adverse changes in market factors.

Institution's treasury and financial derivative valuation processes should be independent of its trading function. Institutions should regularly evaluate market risk measurement models and assumptions to ensure that they provide reasonable estimates of market risk. These should be validated before deployment. Staff involved in the validation process should be adequately qualified and independent of the trading and model development functions. A back-testing program should also be conducted regularly to verify that the models are reliable in measuring potential losses over time.

Foreign exchange risk management must not necessarily seek to eliminate the risks attributable to rate fluctuations. It must instead enable the institution to contain the effects of fluctuations of exchange rates within the limits within the institutions established after careful review of various possible rate circumstances.

5.4.3 Approaches to measuring and limiting Market Risk

Measuring risk is very critical to understanding the potential loss an institution may be exposed to in event of any loss. The principal goal should be to provide strong assurance that losses resulting from market risk will not substantially diminish the capital and earnings of an institution. Common approaches to measuring and limiting market risk are:

- Limit the size of the open positions in each currency as of the close of business each day. Limits are established for either the nominal size of the position or the size of the percentage;
- Limit the size and concentration of investment that is price sensitive, based on percentage of either total investment or total assets of the institution;
- Adherence to the regulatory requirements that pertain to the net open positions
- Determine, on a continuous basis, the size of the loss that would be incurred should the exchange rate move against the institution's open position.
- Determine the size of the loss that would be incurred should the prices of shares and other investments move against the position the institution has taken; and

- Ensure adequate training of personnel and segregation of duties between the front and the back office.

5.4.4 Allocation of Positions to the Trading Book

Institutions on-boarding market risk should allocate their trading positions to the trading book. A trading book consists of positions in financial instruments and commodities held either with trading intent or in order to hedge other elements of the trading book. Positions held with trading intent are those held intentionally for short-term resale and/or with the intent of benefiting from actual or expected short-term price movements or to lock in arbitrage profits.

Institutions should actively manage positions in their trading book and all trading book instruments must be fair valued daily and their valuation change recognised in the profit and loss account.

Institutions are required to have clearly defined policies and procedures for determining which exposures to include in, and to exclude from the trading book for purposes of: calculating their regulatory capital, to ensure compliance with the criteria for trading book and taking into account the Institution's risk management capabilities and practices.

Policies and procedures for determining inclusion and exclusion from the trading book should, at a minimum, address the following considerations: -

- The activities the Institution considers to be trading and as constituting part of the trading book for regulatory capital purposes;
- The extent to which an exposure can be marked-to-market daily by reference to an active liquid two-way market;
- The extent to which valuations for the exposure can be validated externally in a consistent manner;
- The extent to which legal restrictions or other operational requirements would impede the Institution's ability to effect an immediate liquidation of the exposure;
- The extent to which the Institution can actively risk manage the exposure within its trading operations; and
- The extent to which the Institution may transfer risk or exposures between the banking and trading books and criteria for such transfers.

The following are the basic requirements for positions eligible to receive trading book capital treatment.

a. Clearly documented trading strategy for the position/instrument or portfolios, approved by senior management (which would include expected holding horizon).
b. Clearly defined policies and procedures for the active management of the position, which must include:

- Positions are managed on a trading desk;
- Position limits are set and monitored for appropriateness;
- Dealers have the autonomy to enter into/manage the position within agreed limits and according to the agreed strategy;
- Positions are marked to market at least daily and when marking to model the parameters must be assessed on a daily basis;
- Positions are reported to senior management as an integral part of the institution's risk management process; and
- Positions are actively monitored with reference to market information sources (assessment should be made of the market liquidity or the ability to hedge positions or the portfolio risk profiles). This would include assessing the quality and availability of market inputs to the valuation process, level of market turnover, sizes of positions traded in the market, etc.

c. Clearly defined policy and procedures to monitor the positions against the Institution's trading strategy including the monitoring of turnover and stale positions in the Institution's trading book.

5.4.5 Prudent Valuation

Institutions should have prudent valuations for positions in their trading book. A framework for prudent valuation practices should at a minimum, include the following:

5.4.5.1 Governance Structures and Control Processes for Fair Valuing Exposures

Institutions should establish adequate governance structures and control processes for fair valuing exposures for risk management and financial reporting purposes to give management and the Central Bank confidence that their valuation estimates are prudent and reliable. The valuation governance structures and related processes should be embedded in the overall governance structure of the Institution, and consistent for both risk management and reporting purposes. This must include:

a. Documented policies and procedures for the process of valuation. This includes clearly defined responsibilities of the various areas involved in the determination of the valuation, sources of the market information and review of their appropriateness, frequency of independent valuation, timing of closing prices, procedures for adjusting valuations, end of month and ad-hoc verification procedures;

b. In addition, policies and procedures should set forth the range of acceptable practices for the initial pricing, marking-to-market/model, valuation adjustments and periodic independent revaluation; and

c. Clear and independent (i.e. independent of front office) reporting lines for the function, section or unit accountable for the valuation process.

In assessing whether sources of valuation are reliable and relevant, Institutions should consider, among other things:

- The frequency and availability of the prices/quotes;
- Whether those prices represent actual regularly occurring transactions on an arm's length basis;
- The breadth of the distribution of the data and whether it is generally available to the relevant participants in the market;
- The timeliness of the information relative to the frequency of valuations;
- The number of independent sources that produce the quotes/prices;
- Whether the quotes/prices are supported by actual transactions;
- The maturity of the market; and
- The similarity between the financial instrument sold in a transaction and the instrument held by the Institution.

5.4.5.2 Valuation Methodologies

5.4.5.2.1 Marking to Market

Institutions must mark-to-market as much as possible, using the more prudent side of bid/offer. Where values are determined to be in an active market, an institution should maximize the use of relevant observable inputs and minimize the use of unobservable inputs when estimating fair value using a valuation technique.

5.4.5.2.2 Marking to Model

When marking to market is not possible, as is the case of the absence of a transparent price from a liquid market, the valuation must rely on models or proxy-pricing methodologies, as well as on expert judgment. The outputs of such models and processes are highly sensitive to the inputs and parameter assumptions adopted, which may themselves be subject to estimation error and uncertainty. Moreover, calibration of the valuation methodologies is often complicated by the lack of readily available benchmarks.

Institutions relying on modelling for the purposes of valuation should ensure that the model is validated by a function independent of the relevant risk-taking businesses units. Institutions should also establish and maintain policies and processes for considering valuation adjustments for positions that otherwise cannot be prudently valued, including concentrated, less liquid, and stale positions.

5.4.5.2.3 Independent Price Verification

Independent price verification is the process by which market prices are regularly verified for accuracy. While daily marking-to-market may be performed by dealers, verification of market prices should be performed by a unit independent of the dealing room, at least monthly. Independent price verification need not be performed as frequently as daily mark-to-market.

5.4.6 Scenario Analysis and Stress Testing

Stress tests to measure vulnerability to loss arising from market risk operations should be undertaken regularly. Stress tests shall cover major interest rate, foreign exchange, commodities and equities exposures. Stress situations include but are not limited to market movements or institution specific situations in terms of profitability, liquidity and capital adequacy.

The risk measurement system should support a meaningful evaluation of the effect of stressful market conditions on the financial institution. **Stress testing** should be designed to provide information on the kinds of conditions under which the institution's strategies or positions would be most vulnerable and thus may be tailored to the risk characteristics of the institution.

An Institution may choose scenarios based on analyzing historical data of changes in market risk factors or creating forward-looking scenarios. The objective should allow the Institution to assess the effects of changes in market risk factors on its holdings and financial condition. Hence, scenarios chosen could include low probability adverse scenarios that could result in extraordinary losses. Scenario analysis and stress tests should be both quantitative and qualitative.

Scenario analysis and stress testing should, as far as possible, be conducted on an institution-wide basis, taking into account the effects of unusual changes in market and non-market risk factors**.** Such factors include prices, interest rates, volatilities, market liquidity, historical correlations and assumptions in stressed market conditions, the institution's vulnerability to worst case scenarios or the default of a large counterparty and maximum cash inflow and outflow assumptions.

Scenario analysis and stress testing would enable the Board and senior management to better assess the potential impact of various market related changes on the Institution's earnings and capital position and business strategies.

The Board and senior management should regularly review the results of scenario analyses and stress testing, including the major assumptions that underpin them. The results should be considered during the establishment and review of policies and limits. Depending on the potential losses projected by the scenario analysis and stress tests and the likelihood of such losses occurring, the Board and senior management may consider additional measures to manage the risks or introduce contingency plans.

5.4.7 Assets and Liability Committee

ALCO committee is crucial in sound management of market risk. The committee is responsible for supervision and management of Market Risk and liquidity risk. The committee generally comprises of senior managers from treasury, Chief Financial Officer, business heads generating and using the funds of the institution, credit, and individuals from the departments having direct link with interest rate and liquidity risks.

The size as well as composition of ALCO depends on the size of each institution, business mix and organizational complexity. To be effective ALCO should have members from each area of the institution that significantly influences market and liquidity risk.

The Asset and Liability Management Committee (ALCO) should review the management of foreign currency denominated assets and liabilities within the risk parameters approved by the Board of Directors.

5.4.8 Management Information System

An accurate, informative, and timely management information system is essential for managing market risk exposure, both to inform management and to support compliance with board policy. Reporting of risk measures should be regular and should clearly compare current exposure to policy limits. In addition, past forecasts or risk estimates should be compared with actual results to identify any modeling shortcomings.

The board on a regular basis should review reports detailing the market risk exposure of the institution. While the types of reports prepared for the board and for various levels of management will vary based on the institution's market rate risk profile, they should, at a minimum include the following:

- Summaries of the institution's aggregate exposures;
- Reports demonstrating the institution's compliance with policies and limits;
- Results of stress tests including those assessing breakdown in key assumptions and parameters;
- Summaries of the findings of reviews of interest rate risk, price risk, and foreign exchange risk;
- Policies, procedures, and the adequacy of the market risk measurement systems, including any findings of internal and external auditors/consultants;
- Maturity distribution by currency of the assets and liabilities for both on and off-balance sheet items;
- Outstanding contracts by settlement date and currency;
- Total value of outstanding contracts, spot and forward;
- Gains and losses, totals and comparison to previous day's;
- Market value of off-balance sheet products and aggregate dealing limits;
- Exceptional reports e.g. Limit or line excesses;
- Total value of outstanding investments, and current market values;
- Profit and loss, totals and comparison to previous mark to market and aggregate investment limits
- Limit or sectoral excesses and valuation of option contracts, if any.

5.5 Internal Controls and Audit

Institutions should have adequate internal controls to ensure the integrity of their market risk management process. These internal controls should be an integral part of the institution's overall system of internal control. They should promote effective and efficient operations, reliable financial and regulatory reporting, and compliance with Central Bank of Kenya's prudential and regulatory requirements.

The duties of the individuals involved in the risk measurement, monitoring and control functions must be sufficiently separate and independent from the business decision makers and position takers to ensure the avoidance of conflicts of interest.

An effective system of internal control for market risk includes:

- A strong control environment. These should include appropriate approval processes, exposure limits, reconciliation, reviews and other mechanisms designed to provide a reasonable assurance that the institution's market risk management objectives are achieved;
- An adequate process for identifying and evaluating risk;
- The establishment of control activities such as policies, procedures and methodologies;
- Adequate information systems; and
- Continuous review of adherence to established policies and procedures. This is an important element of an institution's internal control system over its market risk management process. Such reviews and evaluations should be conducted regularly by internal auditors or other individuals who are independent of the market risk function they are assigned to review.

The internal audit function of the financial institution should review and assess the market risk management process and ensure that management observe the laid down policies and procedures governing market risk management and that accounting procedures meet the necessary standards of accuracy, promptness and completeness.

6.0 OPERATIONAL RISK MANAGEMENT

6.1 Introduction

Operational risk has been defined as 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. It seeks to identify why a loss happened and at the broadest level includes the breakdown by four causes: people, processes, systems and external factors.

6.2 Guiding Principles

Institutions should develop, implement and maintain an enterprise-wide Operational Risk Management Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual institution will depend on a range of factors, including its nature, size, complexity and risk profile. The aim of the Operational Risk Management Framework is to ensure that an institution effectively manages its operational risks and business disruptions. The principles underpinning the Operational Risk Management Framework include the following:

6.2.1 Governance: An effective operational risk management framework should be properly governed, documented, and implemented.

6.2.2 Risk appetite: A risk appetite for operational risks should be defined and adhered to.

6.2.3 Identification and assessment: Operational risks should be comprehensively identified and assessed using appropriate tools and methods.

6.2.4 Institution: This has the meaning given in section 2 of the Banking Act.

6.2.5 Monitoring and reporting: Operational risks should be continuously monitored and reported to identify control weaknesses and potential breaches of risk appetite and limits.

6.2.6 Operational resilience: Critical operations are identified and assessed, and internal and external dependencies are mapped.

6.2.7 Tolerances for disruption established: Tolerances for disruption should set out the limits of disruption an institution can withstand across a range of severe but plausible scenarios.

6.2.8 Scenario analysis and testing: An institution's resilience in withstanding disruption of critical operations under various plausible scenarios should be continually evaluated. Scenario analysis should be conducted using appropriate techniques at both the business unit and enterprise-wide levels and incorporate a range of severe but plausible scenarios.

The policies defining the Framework should clearly;

- Identify the governance structures used to manage operational risk, including reporting lines and accountabilities;
- Describe the risk assessment tools and how they are used. Such tools may include, but not limited to:
    - Risk and control assessments.
    - Key risk indicators – qualitative and quantitative.
    - Operational risk event data analysis.
    - Scenario analysis.
- Describe the bank's accepted operational risk profile, permissible thresholds or tolerances for inherent and residual risk, and approved risk mitigation strategies and instruments;
- Describe the bank's approach to establishing and monitoring thresholds or tolerances for inherent and residual risk exposure;
- Establish risk reporting and Management Information System (MIS);
- Provide for appropriate independent review and assessment of operational risk; and
- Outline the bank's change management process, which should be comprehensive, appropriately resourced and adequately articulated across the institution. Require the operational risk policies to be revised whenever a material change in the operational risk profile of the bank occurs.

6.3 Board and Senior Management Oversight

The board of directors should take the lead in establishing the "tone at the top" which promotes a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. Operational risk management is about identifying and managing risks that could impact the operations of institutions. The objective of operational risk management is to minimize the frequency and intensity of disruptions and losses from those risks.

6.3.1 Role of Board of Directors Oversight

It is the responsibility of the board of directors to:-

- Establish a strong operational risk management culture throughout the institution.

- Ensure that the institution has developed, implemented and maintained an Operational Risk Management Framework that is fully integrated into the institution's overall risk management processes.
- Oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.
- Review the framework regularly to ensure that the institution is managing the operational risks arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities or systems.
- Approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

6.3.2 Role of Senior Management

Senior management is responsible for consistently implementing and maintaining throughout the institution policies, processes and systems for managing operational risk in all of the institution's material products, services and activities, consistent with the institution's risk appetite and tolerance.

Senior Management responsibilities include:-

- Implementing the operational risk management framework approved by the Board of Directors by consistently implementing and maintaining throughout the institution policies, processes and systems for managing operational risk in all of the institution's material products, services and activities, consistent with the risk appetite and tolerance.
- Ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to ensure the inherent risks and incentives are well understood.
- Ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.
- Ensuring that the institution's operational risk management policy has been clearly communicated to staff at all levels in the units that face material operational risk.
- Implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.
- Ensuring operational deficiencies are assessed and addressed in a timely and sustainable manner.
- Promoting and reinforcing a supportive risk management culture and behaviour.

6.4 Policies and Procedures

Institutions should have policies, processes and procedures to control or mitigate material operational risks. Operational risk policies and procedures that clearly define the way in which all aspects of operational risk are managed should be documented and communicated. These operational risk management policies and procedures should be aligned to the overall business strategy and should support the continuous improvement of risk management.

An institution's operational risk exposure is increased when it engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. An institution should therefore develop and implement policies and procedures that address the process for review and approval of new products, activities, processes and systems.

The review and approval process should consider:-

- inherent risks in the new product, service, or activity;
- resulting changes to the institution's operational risk profile, risk appetite and tolerance, including the risk of existing products or activities;
- the necessary controls, risk management processes, and risk mitigation strategies;
- the residual risk associated with all products or activities;
- changes to relevant risk limits; and
- the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

The approval process should also include ensuring that appropriate investment has been made for human resources and technology infrastructure before new products are introduced.

6.4.1 Policies on Outsourcing

Outsourcing is the use of a third party – either an affiliate within a corporate group or an unaffiliated external entity – to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes. While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities.

Outsourcing policies and risk management activities should encompass:

(a) Procedures for determining whether and how activities can be outsourced;
(b) Processes for conducting due diligence in the selection of potential service providers;
(c) Sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;
(d) Programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;
(e) Establishment of an effective control environment at the bank and the service provider;
(f) Development of viable contingency plans; and
(g) Execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

6.5 Measuring, Monitoring and Control

6.5.1 Measuring operational risk

Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal and external factors. Sound risk assessment allows the bank to better understand its risk profile and target risk management resources and strategies most effectively.

Examples of tools that may be used for identifying and assessing operational risk include:

- **Internal Loss Data Collection and Analysis:** Internal operational loss data such as loss arising from fraud, forgeries, robbery and system downtime provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic.

- **External Data Collection and Analysis:** External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organizations other than the bank.

- **Risk Assessments**: In a risk assessment, often referred to as a Risk Self Assessment (RSA), a bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact.

- **Business Process Mapping**: Business process mappings identify the key steps in business processes, activities and organizational functions. They also identify the key risk points in the overall business process. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness.

- **Scenario Analysis:** Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome. Examples of potentially disruptive events include:
  - Power outages.
  - Large-scale technology failures.
  - Critical third-party service disruptions.
  - Cyber incidents and data breaches.
  - Natural disasters.
  - Health pandemics.

- **Assessing and Modelling Operational Risk Considerations:** In conducting Operational Risk assessment, any assessment and model of operational risk should link in with the institution's wider operational risk framework. In particular, the Operational Risk quantification should clearly reflect the institution's internal control environment.

The capital requirement for operational risk shall be calculated according to the **Standardized Approach under Basel III**. The standardised approach methodology is based on the following components:

i) the **Business Indicator (BI)** which is a financial-statement-based proxy for operational risk;

ii) the **Business Indicator Component (BIC)**, which is calculated by multiplying the BI by a set of regulatory determined marginal coefficients (αi); and

iii) the **Internal Loss Multiplier (ILM)**, which is a scaling factor that is based on a bank's average historical losses and the BIC.

Detailed guidance on computation of each of the above components is provided under Part VI of CBK's Prudential Guideline on Capital Adequacy CBK/PG/03.

6.5.2 Monitoring

An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk.

Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss.

An institution should maintain a log of major operational risks events such as:-

- frauds and attempted frauds – both internal and external ;
- robberies and civil unrest;
- breaches of the bank's risk appetite and tolerance level;
- details of recent significant internal and external operational risk events and losses;
- Any operational risk events witnessed in the financial industry and how well the institution is prepared to mitigate such events;
- IT System outages.
- Frauds (both internal and external) and breaches of sensitive data
- Damage to Physical Assets arising from external events (e.g.9/11)
- Critical third-party service disruptions
- Employee relations including labour disputes and strikes,

Data capture and risk reporting processes should be analyzed periodically with a view to continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.

There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk. Management should implement a robust Management Information System (MIS), aligned with the institutional operational risk management framework, which ensures information is received by the appropriate people, on a timely basis, in a form and format that will aid in the monitoring and control of the business. The reporting process should include information such as:-

- The critical operational risks facing the institution;
- Risk events and issues together with intended remedial actions;
- The effectiveness of actions taken;
- Details of plans formulated to address any exposures where appropriate;
- Areas of stress where crystallization of operational risks is imminent.

6.5.3 Control and Mitigation

Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations; safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations. A sound internal control programme consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities.

An effective control environment requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals or a team without dual controls or other counter-measures may enable concealment of losses, errors or other inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimized, and be subject to careful independent monitoring and review.

In addition to segregation of duties and dual control, banks should ensure that other traditional internal controls are in place as appropriate to address operational risk. Examples of these controls include:

(a) Clearly established authorities and/or processes for approval;
(b) Close monitoring of adherence to assigned risk limits or thresholds;
(c) Safeguards for access to, and use of, bank assets and records;
(d) Appropriate staffing level and training to maintain expertise;
(e) Ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;
(f) Regular verification and reconciliation of transactions and accounts; and
(g) Vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.

Effective use and sound implementation of technology can contribute to the control environment. For example, 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.

The use of technology-related products, services, delivery channels and processes exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks.

An institution should have a detailed Business Continuity Plan. Recovery plans and business resumption priorities must be defined and contingency procedures tested and practised so that business and operating disruption arising from a serious operational risk incident is minimized. The recovery plan and incident response procedures should be evaluated periodically and updated as and when changes to business operations, systems and networks occur.

6.5.4 Stress Testing

An institution should conduct stress tests on a regular basis for a variety of short-term and protracted institution-specific and operational risks stress scenarios to identify sources of

potential operational risks and ensure that institution is prepared to continue in business after minor and major operational risk events. An institution should use the outcomes of stress tests to adjust its operational risk management strategies, policies, and positions and to develop effective contingency plans.

6.5.5 Incident Management

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

6.6 Internal controls and audit

Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. To be effective, strong internal control systems should be an integral part of the structures of an institution.

The business units should establish risk management and internal control procedures to address operational risks. While the extent and nature of the controls adopted by each institution will be different, very often such measures encompass areas such as code of conduct, delegation of authority, segregation of duties, audit coverage, compliance, succession planning, mandatory leave, staff compensation, recruitment and training, dealing with customers, complaint handling, record keeping, MIS and physical controls.

6.7 Risk Reporting and Disclosure

Institutions should disclose relevant operational risk exposure information to the Central Bank of Kenya (including the occurrence of significant operational loss events). Such reporting should be done in the manner (frequency and format) prescribed by CBK, that allows for the identification, assessment, monitoring and controls. Institutions should also have a formal disclosure policy that is subject to regular and independent review and approval by the senior management and the board.

7.0 INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) RISK MANAGEMENT

7.1 Introduction

The purpose of Information and Communication Technology risk management is to assist institutions to establish an effective mechanism that can identify, measure, monitor, and control the risks inherent in institutions' ICT systems, ensure data integrity, availability, confidentiality and consistency and provide the relevant early warning mechanism.

7.2 Board and Senior Management Oversight

7.2.1 Specific Responsibilities for the Board of Directors

The board of directors of institutions has the following responsibilities with respect to the management of information and communication technology risk:

- Ensure that the institution has in place an appropriate ICT governance structure and risk management framework which suits its own circumstances, business needs and risk tolerance.
- Periodically review the alignment of ICT strategy with the overall business strategies and significant policies of the institution.
- Approve ICT risk management strategies and policies.
- Set high ethical and integrity standards, and establish a culture within the institution that emphasizes and demonstrates to all levels of personnel the importance of ICT risk management.
- Establish an ICT Executive Governance Committee which consists of representatives from senior management, the ICT function, and major business units, to oversee these responsibilities and report the effectiveness of strategic ICT planning, the ICT budget and actual expenditure, and the overall ICT performance to the board of directors and senior management periodically.
- Ensure that an effective internal audit of the ICT risk management is carried out by operationally independent, well-trained and qualified staff, which report should be submitted directly to the ICT audit committee; and
- Ensure the appropriation of funding necessary for ICT risk management function.
- Understand the major ICT risks inherent in the institution's business, setting acceptable levels for these risks, and ensuring the implementation of the measures necessary to identify, measure, monitor and control these risks.

7.2.2 Specific Responsibilities for the Senior Management

The following are key responsibilities of senior management with regards to ICT risk:-

- Ensuring that all employees of the institution fully understand and adhere to the ICT risk management policies and procedures approved by the board of directors and the senior management, and are provided with pertinent training.
- Establish a mandatory Cybersecurity Awareness Program for all staff, including specialized training for those with high-privileged access.
- Ensuring customer information, financial information, product information and core banking system of the legal entity are held in a secure environment.
- Reporting in a timely manner to the CBK any significant adverse incidents of information and communication systems or unexpected events, and how they have been handled;
- Cooperating with the CBK in the surveillance of the risk management of information systems, and ensure that supervisory opinions are followed up; and
- Performing other related ICT risk management tasks.

7.2.3 Head of Information and Communication Technology

The following are the responsibilities of the Head of ICT:

- Play a direct role in key decisions for the business development involving the use of ICT in the institution;
- Ensure that information systems meet the needs of the institution, and the ICT strategies, in particular information system development strategies, comply with the overall business strategies and ICT risk management policies of the institution;
- Be responsible for the establishment of an effective and efficient ICT organization to carry out the ICT functions of the institution. These include the IT budget and expenditure, IT risk management, ICT policies, standards and procedures, ICT internal controls, professional development, ICT project initiatives, ICT project management, information system maintenance and upgrade, ICT operations, ICT infrastructure, Information security, disaster recovery plan (DRP), ICT outsourcing, and information system retirement;
- Ensure the effectiveness of ICT risk management throughout the organization including all branches.
- Organize professional trainings to improve technical proficiency of staff.

7.2.4 Staffing of the Information and Communication Technology Unit:

Institutions should designate qualified officer(s) in the Management function for ICT management. Staff in each position should meet acceptable minimum requirements on professional skills and knowledge. The following risk mitigation measures should be incorporated in the selection and management of ICT staff:

- Verification of personal information including confirmation of personal identification issued by government, academic credentials, prior work experience, professional qualifications, certificates of good conduct by the Police;
- Ensuring that ICT staff meet professional ethics and integrity by obtaining character reference from independent referees, former employers, relevant sector regulators;
- Signing of agreements with employees about understanding of ICT policies and guidelines, non-disclosure of confidential information, authorized use of information systems, and adherence to ICT policies and procedures; and
- Evaluation of the risk of losing key ICT personnel, especially during major ICT development stage or in a period of unstable ICT operations, and the relevant risk mitigation measures such as staff backup arrangement and staff succession plan.

7.2.5 Intellectual Proprietary Rights

Institutions should put in place policies and procedures to:

- ensure the utilization of only genuine and licensed software in order to avoid the violation of the law regarding intellectual properties,
- ensure purchase of legitimate software and hardware,
- prevention of the use of pirated software, and
- the protection of the proprietary rights of ICT products developed by the institution, and ensure that these are fully understood and complied with by all employees.

7.3 ICT Risk Management Framework

7.3.1 Information and Communication Technology Strategy

Institutions should formulate an ICT strategy that aligns with the overall business plan of the institution, ICT risk assessment plan and an ICT operational plan. The ICT strategy should ensure that adequate financial resources and human resources are allocated to maintain a stable and secure ICT environment.

7.3.2 ICT Risk Management Policy

Institutions should put in place a comprehensive set of ICT risk management policies that include the following areas:

- Information security classification policy,
- System development, testing and maintenance policy,
- ICT operation and maintenance policy,
- Access control policy,
- Physical security policy,
- Change controls policy,
- Personnel security policy,
- Business Continuity Planning and Crisis and Emergency Management procedure,
- ICT Third-Party Risk Management,
- Incident Management and Reporting,
- Data Protection and Privacy,
- Vulnerability and Patch Management,
- Asset Management and Inventory, and
- Acceptable Use Policy.

7.3.3 ICT Risk Identification

Risk identification entails the determination of all kinds of threats, vulnerabilities and exposures present in the ICT system configuration which is made up of components such as internal and external networks, hardware, software, applications, systems interfaces, operations and human elements.

Security threats such as those manifested in denial of service attacks, internal sabotage and malware infestation could cause severe disruption to the operations of an institution with consequential losses for all parties affected. Vigilant monitoring of these mutating, growing risks is a crucial step in the risk containment exercise.

Both threat-sources and threats must be identified. Threats should include the threat-source to ensure accurate assessment. Some common threat-sources include:

- Natural Threats—floods, earthquakes, hurricanes.
- Human Threats—threats caused by human beings, including both deliberate actions (network based attacks, virus infection, unauthorized access), and unintentional (Inadvertent data entry errors).

- Environmental Threats—power failure, pollution, chemicals, water damage

The risk management function in the institution should compile a list of threats that are present across the institution and use this list as the basis for all risk management activities.

7.3.4 Identifying Vulnerabilities

Different risk management schemes offer different methodologies for identifying vulnerabilities. In general, institutions should start with commonly available vulnerability lists or control areas.

The following tools and techniques are typically used to evaluate the effectiveness of controls, and can also be used to identify vulnerabilities:

- Vulnerability Scanners – software that can examine an operating system, network application or code for known flaws by comparing the system (or system responses to known stimuli) to a database of flaw signatures.
- Penetration Testing – an attempt by human security analysts to exercise threats against the system. This includes operational vulnerabilities, such as social engineering.
- Operational and Management Controls – A review of operational and management controls by comparing the current documentation to best practices (such as ISO 27001, NIST Frameworks, CIS Critical Controls, COBIT, PCI-DSS, OWASP Frameworks) and by comparing actual practices against current documented processes.

7.4 Risk Assessment, Measurement and Monitoring

7.4.1 Risk Assessment

To determine the likelihood of a future adverse event, threats to an ICT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the ICT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the ICT assets and resources affected (e.g., the criticality and sensitivity of the ICT system components and data).

A typical risk assessment methodology encompasses the following nine primary steps;

- System Characterization.
- Threat Identification.

- Vulnerability Identification.
- Control Analysis.
- Likelihood Determination.
- Impact Analysis.
- Risk Determination.
- Control Recommendations.
- Results Documentation.

7.4.2 Risk Measurement

Institutions should put in place a set of ongoing risk measurement and monitoring mechanisms, which should include:

- Pre and post-implementation review of ICT projects;
- Benchmarks for periodic review of system performance;
- Reports of incidents and complaints about ICT services;
- Reports of internal audit, external audit, and issues identified by CBK;
- Arrangement with vendors and business units for periodic review of service level agreements (SLAs);
- The possible impact of new development of technology and new threats to software deployed;
- Timely review of operational risk and management controls in operation area;
- Assessment of the risk profile on IT outsourcing projects periodically.

7.4.3 ICT Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

Because the elimination of all risk is usually impractical, it is the responsibility of senior management and functional and business managers to use the ***least-cost approach*** and implement the ***most appropriate controls*** to decrease mission risk to an acceptable level, with ***minimal adverse impact*** on the institution's resources and mission.

Generally, risk mitigation can be achieved through any of the following risk mitigation options:-

- **Risk assumption -** accept the potential risk and continue operating the ICT system or to implement controls to lower the risk to an acceptable level.

- **Risk avoidance -** avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).
- **Risk limitation –** limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls).
- **Risk planning -** manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.
- **Research and acknowledgment -** lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
- **Risk transference -** transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Institutions should therefore implement a comprehensive set of risk mitigation measures complying with the ICT risk management policies and commensurate with the risk assessment of the institution. At a minimum, the mitigation measures should include:

- A set of clearly documented ICT risk policies, technical standards, and operational procedures, which should be communicated to the staff frequently and kept up to date in a timely manner;
- Areas of potential conflicts of interest should be identified, minimized, and subject to careful, independent monitoring. Also it requires that an appropriate control structure is set up to facilitate checks and balances, with control activities defined at every business level, which should include:

  i) Top level reviews;
  ii) Controls over physical and logical access to data and system;
  iii) Access granted on "need to know" and "minimum authorization" basis;
  iv) A system of approvals and authorizations; and
  v) A system of verification and reconciliation.

7.5 Information Security

Institutions should put in place an information and communication security management function to develop and maintain an ongoing information security management program including;

- Promoting information security awareness,
- advising other ICT functions on security issues,
- serve as the leader of ICT incident response team, and
- report the evaluation of the information security of the institution to the board periodically.

The Information and communication security management program should be documented in an information and communication security policy which should also document the information security standards, strategy, implementation plan, and an ongoing maintenance plan.

The Information security policy should include the following areas:

- ICT security policy management,
- Organization information security,
- Asset management,
- Personnel security,
- Physical and environment security,
- Communication and operation security,
- Access control and authentication,
- Acquirement, development and maintenance of information system,
- Information security event management,
- Business continuity management, and
- Compliance.

7.5.1 Information Confidentiality

The Information and Communication Technology function of institutions should oversee the establishment of an information classification and protection scheme that categorizes data based on its sensitivity (e.g., Public, Internal, Confidential, Highly Confidential). All employees of the institution should be made aware of the importance of ensuring information confidentiality and provided with the necessary training to fully understand the information protection procedures within their responsibilities.

7.5.2 Authentication and Access Control

Institutions should have an effective process to manage user authentication and access control. Access to data and system should be strictly limited to authorized individuals whose identity is clearly established. Their activities in the information systems should be limited to the minimum required for their legitimate business use. An appropriate user authentication mechanism commensurate with the classification of information to be accessed should be adopted. Multi-Factor Authentication (MFA) should be enforced for all privileged access, remote access, customer-facing digital channels and access to systems processing sensitive information.

Timely review and removal of user identity from the system should be implemented when a user transfers to a new job or leaves the institution. The following controls should be put in place:-

7.5.2.1 Physical Security Zones

Institutions should ensure all physical security zones, such as computer centres or data centres, network closets, areas containing confidential information or critical ICT equipment, and respective accountabilities are clearly defined. Appropriate preventive, detective, and curative control measures should be put in place. A Visitor Management Policy must be enforced, requiring all non-employees to be escorted at all times within restricted zones.

7.5.2.2 Logical Security Domains

Institutions should divide their networks into logical security domains (hereinafter referred to as the "domain") with different levels of security. The following security factors have to be assessed in order to define and implement effective security controls, such as physical or logical segregation of network, network filtering, logical access control, traffic encryption, network monitoring, activity log, for each domain and the whole network:

- Criticality of the applications and user groups within the domain;
- Access points to the domain through various communication channels;
- Network protocols and ports used by the applications and network equipment deployed within the domain;
- Performance requirement or benchmark;
- Nature of the domain, i.e. production or testing, internal or external;
- Connectivity between various domains; and
- Trustworthiness of the domain.

7.6 Operating System and System Software

Institutions should secure the operating system and system software of all computer systems by:

- Developing baseline security requirement for each operating system and ensuring all systems meet the baseline security requirement;
- Clearly defining a set of access privileges for different groups of users, namely, end-users, system development staff, computer operators, and system administrators and user

administrators;

- Setting up a system of approval, verification, and monitoring procedures for using the highest privileged system accounts;
- Requiring technical staff to review available security patches, and report exceptions in the patch status to Head of ICT periodically; and
- Requiring technical staff to include important items such as unsuccessful logins, access to critical system files, and changes made to user accounts in system logs monitor the systems for any abnormal event manually or automatically, and report the monitoring periodically.

7.7 Application Software

Institutions should ensure the security of all the application software by:

- Clearly defining the roles and responsibilities of end-users and IT staff regarding the application security;
- Implementing a robust authentication method commensurate with the criticality and sensitivity of the application system;
- Enforcing segregation of duties and dual control over critical or sensitive functions;
- Requiring verification of input or reconciliation of output at critical junctures;
- Requiring that the input and output of confidential information are handled in a secure manner to prevent theft, tampering, intentional leakage, or inadvertent leakage;
- Ensuring the system can handle exceptions in a predefined way and provide meaningful messages to users when the system is forced to terminate; and
- Maintaining audit trail in either paper or electronic format.
- Requiring the user administrator to monitor and review unsuccessful logins and changes to users accounts.

7.8 Audit Trail

Institutions should have a set of policies and procedures controlling the logging of activities in all production systems to support effective auditing, security forensic analysis, and fraud prevention. Logging can be implemented in different layers of software and on different computer and networking equipment, which falls into two broad categories:

- **Transaction journals** are generated by application software and database management system, and contain authentication attempts, modification to data and error messages. Transaction journals should be kept according to the information retention policy legally stipulated in the country.

- **System logs** are generated by operating systems, database management system, firewalls, intrusion detection systems, and routers, etc. and contain authentication attempts, system events, network events and error messages. System logs should be kept for a period proportionate to the risk classification, but not less than one year.

- Institutions should ensure that sufficient items are captured in the logs to facilitate effective internal controls, system trouble shooting, and auditing while taking appropriate measures to ensure time synchronization on all logs. Sufficient disk space should be allocated to prevent logs from being overwritten. System logs should be reviewed for any exception. The review frequency and retention period for transaction logs or database logs should be determined jointly by ICT function and pertinent business lines, and approved by the IT Executive Governance Committee.

7.9 Encryption Technologies

Institutions should have the capacity to employ encryption technologies to mitigate the risk of losing confidential information in the information and communication systems or during its transmission. Appropriate management processes of the encryption facilities should be put in place to ensure that:

- Encryption facilities in use should meet international security standards or requirements;
- Staff in-charge of encryption facilities are well trained and vetted. This is verified through professional and academic testimonials, character reference from independent referees, certificates of good conduct;
- Encryption strength is adequate to protect the confidentiality of the information;
- Effective and efficient key management procedures, especially key lifecycle management and certificate lifecycle management, are in place.

7.10 Computing Equipment

Institutions should put in place an effective and efficient system of securing all end-user computing equipment which include desktop personal computers (PCs), portable PCs, teller terminals, automatic teller machines (ATMs), passbook printers, debit or credit card readers, point of sale (POS) terminals, personal digital assistant (PDAs), tablet devices and smartphones, and conduct periodic security checks on all ICT equipment.

7.11 Handling Consumer Information

Institutions should put in place a set of policies and procedures to govern the collection, processing, storage, transmission, dissemination, and disposal of customer information.

7.12 Training

All employees, including contract staff, should be provided with the necessary training to fully understand the institutions ICT policies, procedures and the consequences of their violation. Institutions should adopt a zero tolerance policy against ICT security violation.

7.13 System Acquisition, Development, Testing and Maintenance

7.13.1 System Development

- Institutions should have the capability to identify, plan, acquire, develop, test, deploy, maintain, upgrade, and retire information systems.
- Policies and procedures should be in place to govern the initiation, prioritization, approval, and control of ICT projects.
- Progress reports of major ICT projects should be submitted to and reviewed by the ICT Executive Governance Committee periodically.
- Decisions involving significant change of schedule, change of key personnel, change of vendors, and major expenditures should be included in the progress report.

7.13.2 Project Risks

Institutions should recognize the risks associated with ICT projects, which include the possibilities of incurring various kinds of operational risk, financial losses, and opportunity costs stemming from ineffective project planning or inadequate project management controls of the bank. Therefore, appropriate project management methodologies should be adopted and implemented to control the risks associated with ICT projects.

7.13.3 System Development Methodology

Institutions should adopt and implement a system implementation methodology to control the life cycle of Information systems. The typical phases of system life cycle include system analysis, design, development or acquisition, testing, trial run, deployment, maintenance, and retirement. The system implementation methodology to be used should be commensurate with the size, nature, and complexity of the ICT project.

7.13.4 Reliability, Integrity, and Relevance

Institutions should ensure system reliability, integrity, and relevance by controlling system changes with a set of policies and procedures, which should include the following elements:

- Ensure that production systems are separated from development or testing systems;
- Separating the duties of managing production systems and managing development or testing systems;
- Prohibiting application development and maintenance staff from accessing production systems under normal circumstances unless management approval is granted to perform emergency repair, and all emergency repair activities should be recorded and reviewed promptly;
- Progressing changes of ICT system configuration from development and testing systems to production systems should be jointly approved by the ICT function and business lines, properly documented, and reviewed periodically.

7.13.5 Data Integrity, Confidentiality, and Availability

Institutions should have in place a set of policies, standards, and procedures to ensure data integrity, confidentiality, and availability. These policies should be in accordance with the latest international data integrity and information security standards e.g. ISO 27001, NIST Frameworks, CIS Critical Controls, COBIT, PCI-DSS, OWASP Frameworks etc

7.13.6 System upgrade

Institutions should have a set of policies and procedures controlling the process of system upgrade. The underpinning software, namely, operating system, database management system, middleware, has to be upgraded, or the application software has to be upgraded. The system upgrade should be treated as a project and managed by all pertinent project management controls including user acceptance testing.

7.14 ICT Operations

7.14.1 Physical and Environmental Controls

Institutions should consider fully the environmental threats (e.g. proximity to natural disaster zones, dangerous or hazardous facilities or busy/major roads) when selecting the locations of their data centres. Physical and environmental controls should be implemented to monitor environmental conditions that could affect adversely the operation of information processing facilities. Equipment facilities should be protected from power failures and electrical supply interference.

7.14.2 Access by Third-party Personnel

In controlling access by third-party personnel (e.g. service providers) to secured areas, proper approval of access should be enforced and their activities should be closely monitored. It is important that proper screening procedures including verification and background checks, especially for sensitive technology-related jobs, are developed for permanent and temporary technical staff and contractors.

7.14.3 Segregation of Duties

Institutions should separate ICT operations or computer centre operations from system development and maintenance to ensure segregation of duties within the ICT function. The Institutions should document the roles and responsibilities of data centre functions.

7.14.4 Documentation of operational instructions

Institutions should detail operational instructions such as computer operator tasks, job scheduling and execution in the ICT operations manual. The ICT operations manual should also cover the procedures and requirements for on-site and off-site backup of data and software in both the production and development environments (i.e. frequency, scope and retention periods of back-up).

7.14.5 Problem management

Institutions should have in place a problem management and processing system to respond promptly to ICT operations incidents. This should include a requirement to record, analyze and escalate reported incidents to relevant ICT management staff., Institutions should keep track of all these incidents until rectification of the incidents and the causes analysed. A helpdesk function should be set up to provide front-line support to users on all technology-related problems and to direct the problems to relevant ICT functions for investigation and resolution.

7.14.6 System monitoring

Institutions should implement a process to ensure that the performance of application systems is continuously monitored and exceptions are reported in a timely and comprehensive manner. The performance monitoring process should include forecasting capability to enable exceptions to be identified and corrected before they affect system performance.

7.14.7 Capacity plan

Institutions should develop a capacity plan to cater for business growth and transaction increases due to changes of economic conditions. The capacity plan should be extended to cover back-up systems and related facilities in addition to the production environment.

7.14.8 Record keeping

Institutions should ensure the continued availability of technology related services with timely maintenance and appropriate system upgrades. Proper record keeping (including suspected and actual faults and preventive and corrective maintenance records) is necessary for effective facility and equipment maintenance.

7.14.9 Change management

Institutions should have an effective change management process in place to ensure integrity and reliability of the production environment. Institutions should develop a formal change management process.

7.15 Business Continuity Management

7.15.1 BCP plans

Institutions should have in place appropriate arrangements to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption in ICT The arrangements should align to the nature, scale and complexity of its business,. These arrangements should be regularly updated and tested to ensure their effectiveness.

7.15.2 Documentation

Institutions should document their strategy for maintaining continuity of its operations, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy.

7.16 Outsourcing

7.16.1 Supervisory Duties

Institutions should not contract out their obligations to regulatory authorities and should take reasonable care to supervise the discharge of outsourced ICT functions. (See details in the

Third-Party Guideline)

7.16.2 Critical ICT Functions

Institutions should take particular care to manage material outsourcing arrangement (such as outsourcing of data centre, ICT infrastructure, etc.), and should notify CBK when they intend to enter into such material outsourcing arrangement.

7.16.3 Risk Analysis

Before entering into, or significantly changing, an outsourcing arrangement, the Institution should:

- Analyze how the arrangement will fit with its ICT organization and reporting structure; business strategy; overall risk profile; and ability to meet its regulatory obligations;
- Consider whether the arrangements will allow it to monitor and control its operational risk exposure relating to the outsourcing;
- Conduct appropriate due diligence of the service provider's financial stability, expertise and risk assessment of the service provider, facilities and ability to cover the potential liabilities;
- Consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement (including what will happen on the termination of the contract); and
- Consider any concentration risk implications such as the business continuity implications that may arise if a single service provider is used by several firms.

7.16.4 Data Security

The Institution should enhance the management of ICT-related outsourcing by putting in place measures to ensure data security of sensitive information such as customer information. Such measures include;

- Ensure that there is clear separation between outsourced information and other information handled by the service provider;
- The staff of the service provider should be authorized on "need to know" and "minimum authorization" basis;
- Ensure that service provider guarantees that its staff meet the confidential threshold required;
- Ensure all related sensitive information are deleted from the service provider's storage when terminating the outsourcing arrangement.

7.16.5 Contingency Plan

The institution should ensure that it has appropriate contingency plans in the event of a significant loss of services from the service provider. Particular issues to consider include a significant loss of resources, turnover of key staff, or financial failure of, the service provider, and unexpected termination of the outsourcing agreement.

7.17 Internal Control and Audit

7.17.1 Systems Audit

Depending on the nature, scale and complexity of their business, it may be appropriate for institutions to combine their internal systems audit with the internal audit function. However, institutions that have capacity and the relevant competences are advised to separate systems audit from internal audit function.

The internal audit function should be adequately resourced and staffed by competent individuals, be independent of the day-to-day activities of the institution and have appropriate access to the institution's records.

7.17.2 Role of Internal Audit

Whether performed by a separate specialised ICT audit function or as a function within the internal audit, the responsibilities of the ICT audit function are:

- To establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the institution's systems and internal control mechanisms and arrangements;
- To issue recommendations based on the result of work carried out ;
- To verify compliance with those recommendations;
- To carry out special audit on the information system. This can arise from an information security incident or from a risk assessment report by the internal audit or risk management function. It involves investigating, analysing and reporting on the information system.

7.17.3 Frequency of IT Internal Audit

Institutions should determine the scope and frequency of ICT internal audit. This should be based on the nature, scale and complexity of its business, deployment of information and

communication technology and ICT risk assessment,. However, a comprehensive ICT internal audit shall be performed at a minimum once every year.

7.17.4 Implementing System Development

Institutions should engage its Internal Audit Department and ICT Risk Management Department when implementing system development of significant size and scale. This will ensure it meets the ICT Risk standards of the institution.

7.18 ICT External Audit

The requirement for external ICT audits complements the responsibilities of the internal audit functions, and risk management functions. It serves as an additional line of independent assurance to identify weaknesses, assess emerging risks, validate the effectiveness of control environments, and support timely remediation of deficiencies.

The ICT external audit should at minimum cover the following aspects:

- Risk assessment of the ICT systems.
- Review of the ICT Policies, strategy and direction.
- Business continuity management program.
- Systems change control process.
- Reporting, logging and auditability of the systems.
- Input-process-output controls.
- Adequacy of identification and authentication system.
- Protection against malicious malware.
- Operations and network management.

Institutions should ensure that the ICT external auditor reviews and examines institutions hardware, software, documentation and data to identify all potential ICT risks.

Institutions should ensure that the ICT external auditors strictly comply with the law and regulations by maintaining the confidentiality of private information accessed while conducting the ICT audit. ICT audits may be carried out by external auditors or specialised firms and should be conducted at least once every year.

8.0 REPUTATIONAL RISK MANAGEMENT

8.1 Introduction

Reputational risk refers to the risk arising from negative perception held by an institution's stakeholders (customers, shareholders, investors, debt-holders, market analysts, suppliers, employees, regulators, politicians, non-governmental organizations, media, or the community) which may adversely affect the institution's earnings, capital, liquidity, operations, or ability to maintain existing or establish new business relationships.

Key determinants of an institution's reputation include its performance in the following areas:

- Quality of products and service delivery
- Management of customer interactions and complaints
- Prevention and response to fraud incidents
- Cybersecurity and information security resilience
- Compliance with AML/CFT/CPF requirements
- Management of litigation and legal disputes
- Oversight of outsourcing and third-party arrangements
- Protection of customer and institutional data privacy
- Employee conduct and ethical behaviour
- Management of social media presence and online communications
- Identification and management of climate-related financial risks
- Governance of strategic partnerships and business relationships
- Responsible development and use of AI systems
- Compliance with regulatory and supervisory requirements

A strong positive reputation among stakeholders across multiple categories will result in a strong positive reputation for the financial institution. A well-managed reputation is a strategic asset that enables institutions to strengthen their market position, increase market value, build resiliency against shocks and attract and retain talent. Weak management of reputational risk may result in:

- Loss of customer confidence
- Liquidity stress or deposit withdrawals
- Increased regulatory scrutiny
- Litigation and financial penalties
- Decline in shareholder value
- Loss of business opportunities
- Operational disruptions
- Systemic contagion within the financial sector

8.2 Board and Management Oversight

Ultimate responsibility for reputational risk management rests with the Board. The Board of Directors should address explicitly reputational risk as a distinct and controllable risk to the institution's safety and soundness.

The Board should:

1) Approve the institution's Reputational Risk Management Strategy and associated risk tolerance levels
2) Establish a clear management structure with defined roles, authorities, and reporting lines for implementing the Reputational Risk Management Strategy
3) Ensure that the Reputational Risk Management Strategy is aligned with the institution's overall strategic objectives and risk appetite
4) Oversee senior management's implementation of the framework
5) Regularly review the Reputational Risk Management Strategy (at least annually) to ensure its continued effectiveness, incorporating emerging industry developments and technology innovations

Senior management should:

1. Implement the Board-approved strategy into policies, processes, and procedures
2. Ensure that staff across all functions understand and are trained on their role in managing reputational risk
3. Promote ethical culture and accountability

4. Conduct surveillance of external sources of reputational risk, including media, market intelligence, and stakeholder feedback, and report the findings accordingly to the Board

Reputation risk cuts across multiple business units in an institution. It requires a small, cross-functional team to create and implement a protection strategy. This team would comprise of a representative from corporate communications/public relations, the legal and compliance department, the health and safety department, operations, investor relations, customer relations, risk management, human resources, information security / ICT with input from the Chief Executive or Chairperson of the Board.

8.3 Policies, Procedures and Limits

Management must translate the reputational risk management strategy established by the Board of Directors into policies, processes and procedures that can be implemented and verified. While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures and controls within its purview, senior management must clearly assign authority, responsibility and reporting relationships to encourage this accountability. This responsibility includes ensuring that the necessary resources are available to manage reputational risk effectively.

Institutions should have policies, processes and procedures to control or mitigate material reputational risks. Authority and accountability for compliance should be clearly defined and enforced. Institutions' privacy policies should fully consider legal and litigation concerns. Policies, Procedures and Limits should cover the following with regards to Corporate Governance practices:

- Management Integrity – The personal ethics and behaviour of directors and senior management are important determinants of stakeholder confidence. The probity and conduct of such persons will always be under close scrutiny.
- Staff Competence and Support – Human capital is an important asset. Deficiencies in staff management (high turnover, misconduct, poor service quality) can lead to adverse publicity. Institutions should provide adequate training to raise employee awareness.

- Corporate Culture – The institution should promote a culture where:
  i) Ethical and responsible behaviour is encouraged.
  ii) Compliance issues or lax control standards are not tolerated.
  iii) A formal mechanism (e.g. Whistleblowing channel) exists for employees to voice concerns regarding potential threats to reputation (e.g. fraud, business malpractices).

8.4 Risk Measurement, Monitoring and Management Information System

8.4.1 Reputational Risk Identification and Measurement

Risk identification is critical for the subsequent development of viable reputational risk measurement, monitoring and control. Institutions must have a clear understanding of the main threats to their reputation, which may manifest through sustained negative media coverage, rapid fall in share price, loss of customer confidence, or social media backlash. They can be caused by factors such as the effects of activism, discrimination in the workplace, unethical trading, marketing failures, or more traditional risks such as product/service failure.

Once the risks have been identified, they need to be prioritised in order to help managers determine where to devote effort and resources. This prioritisation process should be linked to the institution's existing risk management strategies.

Sources of Reputational Risk

Some of the potential sources that can negatively affect the bank's reputation include:

1. **Financial Soundness / Business Viability**
   An institution's reputation may suffer if its financial stability or long-term viability is questioned. Significant losses, weak performance, or failed investments can reduce stakeholder confidence and raise concerns about management competence and sustainability.

2. **Business Practices**

   Institutions are expected to conduct business in a responsible, honest, and prudent manner. Unethical or unlawful practices, including unauthorized activities or improper selling practices, can erode public trust, attract regulatory sanctions, and damage reputation.

3. **Fraudulent Activities**

   Fraudulent activities, whether internal or external, can significantly harm an institution's reputation and customer confidence. Institutions should implement strong internal controls and monitoring mechanisms to prevent and detect fraud.

4. **Litigations**

   Institutions should implement measures to identify, assess, and manage litigation risks arising from contractual disputes, customer complaints, employment matters, regulatory actions, or other legal proceedings. Institutions should maintain strong legal review processes, proper documentation practices, dispute resolution mechanisms, and ongoing monitoring of legal exposures to minimize financial losses and reputational damage.

5. **Customer Satisfaction**

   Institutions should implement measures to safeguard customer interests and promote fair treatment in the provision of financial products and services. Such controls should include transparent disclosures, effective complaint handling mechanisms, fraud prevention measures, secure customer authentication processes, while appropriately considering the needs of persons with disabilities and other vulnerable customers in service design and delivery.

6. **AML/CPT/CPF Concerns**

   Institutions must ensure that they are not used as conduits for money laundering, terrorist financing, or proliferation financing as such activities may expose the institution to reputational risk. Key mitigants include strict compliance with KYC requirements, limits on transactions for non-account holders, supporting documentation for large transactions, enhanced due diligence for high-risk accounts, and ongoing monitoring of suspicious transactions.

7. **Contagion Risk / Rumours**

   Institutions may suffer reputational damage due to negative events affecting parent companies, subsidiaries, affiliates, or close business associates. Regulatory sanctions, financial instability, or unethical conduct by related parties can create adverse spillover effects and weaken stakeholder confidence.

8. **Transparency and Accountability**

   Transparent, timely, and accurate disclosure of material information is essential for maintaining stakeholder trust. Clear communication on an institution's strategy, performance, and risks enables stakeholders to better understand its values, objectives, financial condition, and future prospects.

9. **Product Governance Framework**

   Before introducing new products, the Board and senior management should identify and assess the associated firm-wide risks. They should ensure that appropriate infrastructure and internal controls are in place to effectively manage those risks. In this review, an institution should also consider the difficulty in valuing the new products and how they might perform in a stressed economic environment.

10. **Strategic partnerships**

    Institutions should conduct thorough assessments and ongoing oversight of strategic partnerships, joint ventures, fintech collaborations, and other business alliances to ensure alignment with the institution's strategic objectives, risk appetite, regulatory obligations, and ethical standards. Appropriate due diligence should be performed to assess the partner's financial soundness, operational capability, governance practices, cybersecurity posture, and reputational standing.

11. **Artificial Intelligence systems**

    Institutions should identify and manage AI-related risks that may result in reputational harm and establish governance and control frameworks for AI systems. Institutions should ensure that AI systems operate in a transparent, secure, fair, and accountable manner, with appropriate human oversight, model validation, bias testing, explainability measures, and continuous monitoring to prevent inaccurate, discriminatory, or unethical outcomes.

12. **Social media and online presence**

    Institutions should establish controls and monitoring mechanisms to manage risks

arising from social media platforms including misinformation, fraud, impersonation, social engineering, and reputational attacks. Measures should address official communications, employee conduct online, misinformation management, customer engagement protocols, cybersecurity risks and continuous monitoring of digital channels to promptly identify and respond to misleading or malicious content

13. **Data protection controls**

    Institutions should implement robust data governance and protection measures to ensure the confidentiality, integrity, and availability of customer and institutional data. Controls should include data classification, access restrictions, encryption, secure storage, data retention policies, and compliance with applicable data protection laws and regulations.

14. **Vendor due diligence procedures**

    Institutions should conduct comprehensive due diligence and ongoing oversight of third-party service providers, vendors, and outsourcing partners to ensure that they meet the institution's operational, security, financial, legal, and ethical standards. Contracts should clearly define service expectations, confidentiality obligations, risk responsibilities, and audit rights.

15. **Climate-related financial risks**

    Institutions should identify and manage climate-related financial risks. These risks include physical and transition risks, greenwashing, inadequate climate risk management, and insufficient climate-related disclosures. Institutions should also manage risks that may result in reputational harm, nature and biodiversity loss. Institutions should integrate climate risk considerations into governance structures, risk management processes, lending decisions, investment strategies, and stress testing frameworks to manage such risks effectively.

8.4.2 Risk Assessment Tools

Institutions should assess reputational risk not only in terms of its likelihood and impact, but also their ability to prevent, mitigate, and respond to reputational risk events. The assessment tools employed shall be proportionate to the institution's size, complexity, and risk profile, and enable the identification of material threats, potential consequences, and the effectiveness of existing controls and response measures.

Risk assessment tools may include:

1. Internal Expert Judgement: Executive workshops, Risk self-assessments, strategic vulnerability reviews, and in-depth interviews with the institution's area experts to obtain an internal perspective on business strategies, emerging risks, vulnerabilities, and potential threats to the institution's reputation.
2. Stakeholder Analysis: Identifying key stakeholders and assess their expectations, perceptions, and concerns. This provides an external perspective that enables institutions to understand how stakeholder views may influence their reputation and to proactively address emerging reputational risks.
3. Reputational Risk and Control Assessment: Evaluating root causes, existing controls, control effectiveness, and residual risk.
    - Risk Register: A document detailing each risk (category, description, root cause, existing controls, risk owner, response plan, likelihood/impact score). Institutions should maintain reputational risk registers capturing material exposures and mitigation actions.
    - Risk Heat Map: A visual tool to categorise and prioritise risks based on likelihood and impact. Institutions should develop risk heat maps to support prioritization of reputational threats based on likelihood and impact.
4. Stress Testing: Reputational risk scenarios should be included in stress testing to understand second-round effects (e.g. deposit runs, loss of correspondent banking lines). Results should feed into ICAAP and liquidity contingency plans.
5. Risk Sensing / Listening Posts: Using technology (including social media monitoring) to scan blogs, news, and forums for emerging threats, sentiment changes, and early warning indicators.

8.4.3 Risk Monitoring and Reporting

Institutions should establish procedures and monitoring mechanisms to identify and assess early warning signs of emerging risks. Such mechanisms should facilitate the timely detection of adverse developments and enable management intervention before risks materialize into significant reputational consequences.

Institutions should leverage information from multiple sources, including customer service functions, employee feedback channels, media monitoring tools, and stakeholder engagements. Customer service functions, in particular, may establish early warning signals of a trend occurring before the issue spills over to the public domain. Early warning indicators may include, but are not limited to:

- Volume, nature, and trends of customer complaints
- Breaches of internal controls, policies, or procedures
- Negative media coverage, adverse social media sentiment, or misinformation campaigns
- Staff awareness and conduct assessment results
- Regulatory breaches, enforcement actions, or supervisory findings
- Significant deposit outflows, liquidity pressures, or adverse market reactions
- Stakeholder perception and public opinion survey results
- Operational errors, processing failures, or service disruptions
- System outages, cybersecurity incidents, or technology failures
- Fraud incidents, including those involving digital channels, AI-generated deepfakes, or identity impersonation
- Material deterioration in key risk, financial, operational, or customer service performance indicators

The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Institutions should periodically review and re-evaluate the early warning indicators to ensure that they remain effective, and forward-looking in managing reputation risk. The results of these monitoring activities should be included in management and Board reports.

Institutions should establish a reputational event reporting mechanism that defines reporting requirements, reporting lines, escalation procedures, and timelines to ensure that reputational risk events and identified deficiencies are reported and addressed through appropriate corrective actions. Institutions should allocate adequate resources and implement effective training programmes to strengthen awareness, promote compliance, and enhance the management of reputational risks.

Institutions should leverage appropriate communication and information-sharing channels to provide timely, accurate, and consistent information to internal and external stakeholders during normal operations and periods of heightened reputational risk. Such channels should facilitate coordinated communication, support crisis management efforts, promote consistency of messaging, and enable the capture and dissemination of lessons learned from previous incidents. In monitoring reputational risk, institutions should consider, at a minimum, the following:

- **Staff awareness and risk culture**
  Institutions shall foster a risk-aware culture that encourages employees to identify, report, and respond to potential reputational risks. Relevant business units should participate in the development and periodic review of early warning indicators, leveraging emerging risk intelligence to enhance the effectiveness of the monitoring framework.
- **Pre-implementation assessment of initiatives**
  Institutions should assess the potential reputational impact of significant new products, services, policies, technologies, strategic initiatives, outsourcing arrangements, and partnerships before implementation. Such assessments should form part of the institution's approval and risk review processes.
- **Customer complaints and stakeholder feedback**
  Institutions should maintain mechanisms for capturing, analysing, and monitoring customer complaints, service issues, stakeholder concerns, and other indicators of dissatisfaction. Trend analysis of such information should be used to identify emerging reputational risks, inform corrective actions, and enhance service delivery and customer trust.
- **Codes of conduct and ethical standards**
  Institutions should establish and maintain codes of conduct that reflect their values, ethical standards, and stakeholder expectations. Such codes should be supported by regular training, communication, monitoring, and periodic review to ensure continued relevance and effective implementation.

8.4.4 Management Information System

An Institution's Management Information Systems (MIS) should provide the Board and senior management with timely and accurate information on the institution's overall risk profile. Such information should capture all material risk exposures and enable informed decision-making. The Board and senior management should understand the assumptions, methodologies, and limitations underlying the risk measures and reports generated by the MIS. The MIS should be supported by appropriate infrastructure and capabilities that:

- Facilitate the aggregation of risk exposures and risk measures across business lines, products, entities, and activities
- Support the identification, monitoring, and analysis of risk concentrations, interconnected exposures, and emerging risks

An institution's MIS should be capable of capturing limit breaches and there should be procedures in place to promptly report such breaches to senior management, as well as to ensure that appropriate follow-up actions are taken. For instance, similar exposures should be aggregated across business platforms to determine whether there is a concentration or a breach of an internal position limit.

MIS developed to achieve this objective should support the ability to evaluate the impact of various types of economic and financial shocks that affect the whole of the financial institution. Further, an institution's systems should be flexible enough to incorporate hedging and other risk mitigation actions to be carried out on a firmwide basis while taking into account the various related basis risks.

To enable proactive management of risk, the Board and senior management need to ensure that MIS is capable of providing regular, accurate and timely information on the institution's aggregate risk profile, as well as the main assumptions used for risk aggregation. MIS should be adaptable and responsive to changes in the institution's underlying risk assumptions and should incorporate multiple perspectives of risk exposure to account for uncertainties in risk measurement. In addition, it should be sufficiently flexible so that the institution can generate forward-looking scenario analyses

that capture management's interpretation of evolving market conditions and stressed conditions.

8.5 Internal Controls and Audit

The institution's Board of Directors should adopt and support strong internal controls and written policies and procedures and ensures that management effectively communicates these throughout the institution. The Board should regularly verify whether its system of internal controls is adequate to ensure well-ordered and prudent conduct of business.

Institutions should regularly monitor, test, and independently review their reputational risk management processes. Reviews should assess the effectiveness of controls (including changes in market conditions, personnel, technology and structures of compliance with exposure limits) and ensure that there are appropriate escalation procedures for any exceeded limits.

The risk management function should be independent of business lines to ensure effective oversight and avoid conflicts of interest. Corporate communications, public relations, and stakeholder engagement functions should ensure compliance with approved communication policies, provide timely and consistent stakeholder communications, and monitor public perception to identify and mitigate reputational risks.

An independent review of the risk measurement system should be carried out regularly in the institution's own internal auditing process. This review should include both the activities of the business trading units and of the independent risk control unit. A review of the overall risk management process should take place at regular intervals (ideally no less than once a year) and should specifically address, at a minimum:

- The adequacy of the documentation of the risk management system and process
- The integrity of the management information system
- The validation of any significant change in the risk measurement process

9.0 COMPLIANCE RISK MANAGEMENT

9.1 Introduction

Compliance risk is the current or prospective risk to earnings and capital arising from violations or non-compliance with laws, rules, regulations, agreements, prescribed practices, or ethical standards, as well as from the possibility of incorrect interpretation of effective laws or regulations. Institutions are exposed to compliance risk due to relations with a great number of stakeholders, e.g. regulators, customers, counterparties, as well as tax authorities, local authorities and other authorised agencies.

In addition to the legal and regulatory framework put in place by the home regulatory agencies, institutions operating across borders must also ensure compliance with the applicable legal and regulatory requirements in the other jurisdictions in which they conduct business.

9.1.1 Compliance Risk Governance Framework: The Three Lines of Defence

Institutions should use the three Lines of Defence model as a risk governance framework to strengthen accountability, control effectiveness, and regulatory compliance across all levels of the institution.

The first line (business units) owns and manages risks in daily operations by embedding controls within processes and ensuring adherence to approved risk limits.

The second line (risk management, compliance, and control functions) develops risk policies, formulates the risk appetite framework and limits, monitors risk exposure, recommends mitigations and provides independent challenge and oversight to the business.

The third line (internal audit) provides independent assurance to the Board and senior management on the effectiveness of governance, risk management, and internal control systems.

9.1.2 Impact of Compliance Risk

Non-compliance with the legal and regulatory framework exposes an institution to payment of fines, penalties, damages, and the violation of contracts. It can also lead to diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential and an inability to enforce contracts. Furthermore, public knowledge of legal and

regulatory violations can cause substantial harm to a bank's reputation, contributing to a loss of public confidence.

9.1.3 Organisation of Compliance Function

All institutions should establish an independent compliance function which facilitates efforts to comply with legal and regulatory requirements by tracking and documenting compliance. The function should also be sufficiently resourced, and its responsibilities should be clearly specified.

Institutions should organise their compliance function and set priorities for the management of their compliance risk in a way that is consistent with their own risk management strategy and structures.

Some institutions may wish to organise their compliance function within their operational risk management function, as there is a close relationship between compliance risk and certain aspects of operational risk. Others may prefer to have separate compliance and operational risk functions but establish mechanisms requiring close cooperation between the two functions on compliance matters.

The independence of the head of compliance and any other staff having compliance responsibilities may be undermined if they are placed in a position where there is a real or potential conflict between their compliance responsibilities and their other responsibilities. It is therefore expected that when compliance staff perform non-compliance tasks, institutions ensure that conflict of interest is avoided.

9.2 Board and Senior Management Oversight

The ultimate accountability for compliance risk management rests with the Board, which should be aware of the major aspects of the institution's compliance risk as a separate risk category that should be managed.

The Board of Directors of an institution is responsible for the following:

- defining the compliance risk management system and ensuring that the system is aligned with overall business activities;
- approving compliance risk management policy that provides the senior management with clear guidelines and procedures for managing compliance risk;

- establishing a management structure capable of implementing the institution's compliance risk management process; and
- periodically reviewing the institution's compliance risk management policy to ensure proper guidance is provided for effectively managing the institution’s compliance risk.

Management should fully understand all aspects of compliance risk and exhibit a clear commitment to compliance. The Board and senior management should ensure that there is an effective, integrated compliance risk management framework. This includes the establishment of an independent compliance function.

9.3 Policies and Procedures

Institutions should have policies, processes and procedures to control or mitigate compliance risks. Authority and accountability for compliance should be clearly defined and enforced.

An institution’s compliance policy should explain the main processes by which compliance risk is to be identified and managed through all levels of the institution’s organizational structure. The policy should also define the compliance function as an independent function, with specific roles and responsibilities of the compliance staff, and detailing the compliance officer’s communication methods with the management and staff in the various business units.

Compliance risk management policy should be part of the overall risk management policy of the institution and should precisely determine all important processes and procedures in minimising the institution’s compliance risk exposure. The policy should be clearly formulated and in writing. The policy must contain, at least, the following:

a) Definition of compliance risk;
b) Objectives of compliance risk management;
c) Procedures for identifying, assessing, monitoring, controlling and managing compliance risk;
d) Well-defined authorities, responsibilities and information flows for compliance risk
e) Management at all management levels; and
f) Clear statement of the institution's accepted tolerance for compliance risk exposure.

9.4 Measuring, Monitoring and Control of Compliance Risk

The compliance function should monitor the institution’s compliance status periodically and report to the Board or a committee of the Board. The compliance function should also report

to the Central Bank the compliance status as required from time to time through the compliance return **(Appendix I)**.

The compliance function should consider ways to measure compliance risk (e.g. by using performance indicators) and use such measurements to enhance the institution's risk assessment. This may include keeping a log of legal and regulatory breaches and near-miss logs.

Institutions should have in place a system that ensures that deficiencies identified by the compliance function are promptly managed and meaningful corrective action implemented. Training programs should include developments in the legal and regulatory frameworks to ensure that control of compliance risk is effective. All the necessary resources should be provided to support the compliance function.

Institution's management should show preparedness towards the anticipation of compliance risk and ability to respond well to changes in the market, technology or regulatory framework.

9.4.1 Management Information System

Technology can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems (e.g. an increasing number of customer complaints, irregular trading or payments activity, etc.). The institution's management information systems should therefore be sound to be able to capture aspects of non-compliance. This is possible when the institutions have a strong control culture. Compliance considerations should be incorporated into product and system development and modification processes, including changes made by outside service providers or vendors.

9.5 Internal Audit

The scope of activities of the compliance function should be subject to a periodic independent review by the internal audit function. The review of compliance activities by the internal audit function should test the controls in place within the bank to ensure compliance with the applicable laws, rules and standards.

APPENDIX I

CBK/RMG/ 7-1				
	MONTHLY COMPLIANCE RETURN			
	Institution:			
	Financial Year:		Version 1.1.7.2	
	Start Date:			
	End Date:			
No.	**Legal and Regulatory Requirements**	**Actual Position**	**Compliance Yes/No**	**Comments**
1.	Common Equity Tier 1 (CET1) (Minimum for Banks and Mortgage Finance companies – Ksh.5 billion by December 31, 2026, Ksh.7 billion by December 31, 2027, Ksh.8 billion by December 31, 2028, Ksh.10 billion by December 31, 2029 (**B.A. Section 7(1).**			
2.	Additional Tier 1 Capital/Total Risk Weighted Assets Ratio (**B.A. Section 18)**			
3.	Tier 1 to Total Risk Weighted Assets Ratio (**B.A. Section 18)**			
3.	Total capital to Total Risk Weighted Assets Ratio **(B.A. Section 18)**			
4.	CET1 to Total Deposits ratio is 8%. B.A. Section 17			
5.	Leverage ratio ≥ 4% **(CBK/PG/03 on Capital Adequacy)**			
6.	Liquidity Ratio: Statutory minimum requirement of 20%. **B.A. Section 19(1)**			
7.	Liquidity Coverage Ratio (LCR) ≥ 100% **(CBK/PG/05 on Liquidity Management)**			
8.	Net Stable Funding Ratio (NSFR) ≥ 100% **(CBK/PG/05 on Liquidity Management)**			
9.	Single Borrower limit - 25% of Core Capital. **B.A. Section 10(1)**			
10.	The institution must not grant any advance or credit facility against the security of its own shares. **B.A. Section 11(1)(a)**			
11.	The institution must not grant any facility to a company in which it has an equity interest directly or indirectly of 25% or more of the share capital of that company. **B.A. Section 11(1)(b)**			

CBK/RMG/ 7-1				
	MONTHLY COMPLIANCE RETURN			
	Institution:			
	Financial Year:		Version 1.1.7.2	
	Start Date:			
	End Date:			
No.	**Legal and Regulatory Requirements**	**Actual Position**	**Compliance Yes/No**	**Comments**
12.	All insider borrowing must be secured. **B.A. Section 11(1)(c) & (d)**			
13.	All loans to directors and management should be at arm's length and approved by the full board and should be reported to CBK within seven days. **B.A. Section 11(1)(e)**			
14.	Single insider borrower limit - 20% of Core capital. **B.A. Section 11(1)(f)**			
15.	Total insider borrowing limit - 100% of Core Capital. **B.A. Section 11(1)(g)**			
16.	The institution must not grant any credit facility, give a guarantee, or incur any liability in a Fraudulent or reckless manner. **B.A. Section 11(1)(h)**			
17.	Investment in Land & Buildings **purchased after 10.06.1999 is** limited to not more than 20% of Core Capital. **B.A. Section 12(c) and (CBK/PG/07 - Prohibited Business)**			
18.	Restriction on ownership of share capital to 25%. **B.A. Section 13(1)**			
19.	Transfer of 5% Shareholding of an Institution must be approved by CBK. **B.A. Section 13(4)**			
20.	Total advances for real estate are limited to 25 % of total deposits, except for MFCS. **B.A. Section 14(1)**			
21	Loans and Advances to be classified in accordance with the risk classification of assets and provisioning. **(CBK/PG/04)**			
22.	All capitalized expenditure, including preliminary expenses, must be written off before paying dividends. **B.A. Section 20(1)**			

CBK/RMG/ 7-1				
	MONTHLY COMPLIANCE RETURN			
	Institution:			
	Financial Year:		Version 1.1.7.2	
	Start Date:			
	End Date:			
No.	**Legal and Regulatory Requirements**	**Actual Position**	**Compliance Yes/No**	**Comments**
23.	The Institution must make Adequate Provisions for bad and Doubtful Debts. **B.A. Section 20(2)(b) and (CBK/PG/04)**			
24.	Institutions must display in a conspicuous position in every office and branch a copy of the latest audited Balance Sheet and Profit and Loss Account. **B.A. Section 22**			
25.	Institutions must furnish information at such time and in such manner as required by the Central Bank. **B.A. Section 28**			
26.	Officers of an institution must take reasonable steps to secure the accuracy of information submitted to CBK. **B.A. Section 50(1)(b)**			
27.	Every institution must submit to CBK within three months of the end of its financial year the following: **B.A. Section 23(1) (Reported once after 1st Quarter)**			
	(a) Audited Balance Sheet			
	(b) Audited Profit & Loss			
	(c) A copy of the auditor's report in the prescribed form relating to its activities			
27.	An institution incorporated outside Kenya or a Kenyan incorporated institution with branches outside Kenya must submit to CBK;			
	(a) An Audited Balance Sheet for the global operations			
	(b) An audited Profit and Loss Account for global operations (report once after audit)			
28.	Foreign Exchange exposure limit- 10 % of Core Capital. (**CBK/PG/06 - Foreign Exchange Exposure Limits)**			

CBK/RMG/ 7-1				
	MONTHLY COMPLIANCE RETURN			
	Institution:			
	Financial Year:		Version 1.1.7.2	
	Start Date:			
	End Date:			
No.	**Legal and Regulatory Requirements**	**Actual Position**	**Compliance Yes/No**	**Comments**
29.	Aggregate large exposures are restricted to not more than 5 times of Core Capital. **(CBK/PG/07 - Prohibited Business)**			
30.	All Suspicious transactions should be reported (**CBK/PG/08 - Proceeds of Crime and Money Laundering Prevention)**			
31.	No Institution shall increase its rate of Banking or Other Charges except with prior approval of the CBK (**B.A. Section 44)**			
32.	An institution shall be limited in what it may recover from a debtor with respect to a non-performing loan to the maximum amount under Section 44A (2). **B.A. Section 44A (1)**			
33.	No Institution shall Impose Any Form of Charges on a savings, seven-day call, or fixed deposit account. **B.A. Section 16A (1)**			
34.	The institution must appoint an external auditor qualified under section 161 of the Companies Act and seek CBK Approval (Reported once a year). **(CBK/PG/09 - Appointment, Duties & Responsibilities of External Auditors)**			
35.	If the institution has changed or removed its auditors, was written approval obtained from CBK? **B.A. Section 25(1) and (CBK/PG/09 - Appointment, Duties & Responsibilities of External Auditors)**			
36.	The Institution must make its Annual Contribution to the Kenya Deposit Insurance Corporation (KDIC) (to be reported once a year). **B.A. Section 38**			
37.	All Officers of an institution must be qualified to hold office and shall cease to hold office and shall not			

CBK/RMG/ 7-1				
	MONTHLY COMPLIANCE RETURN			
	Institution:			
	Financial Year:		Version 1.1.7.2	
	Start Date:			
	End Date:			
No.	**Legal and Regulatory Requirements**	**Actual Position**	**Compliance Yes/No**	**Comments**
	thereafter be eligible to hold office in any institution if any of them is as stated below: B.A. **Section 48**			
	(a) Bankrupt			
	(b) Convicted of an offence involving dishonesty or fraud			
	(c) Disqualified from holding office under B.A. Section 32A			
	(d) Removed from office under the provisions Of B.A. Section 34			
38.	Does the institution comply with the following **(CBK/PG/02 - Corporate Governance) requirements:**			
	(a) Chief Finance Officer (Head of Finance) and Head of Internal Audit should be members of ICPAK.			
	(b) The Company Secretary should be a member of ICPSK.			
	(c) Every Board member must attend at Least 75 percent of the Board Meetings Annually.			
	(d) No Chief Executive Officer, Executive Director or senior management should own more than 5% of the institution's shareholding.			
39	Has the institution established a Compliance Function which includes an ML/TF/PF Section (CBK Prudential Guidelines on Corporate Governance (CBK/PG/02) and Proceeds of Crime and Money Laundering (Prevention) Prudential Guidelines (CBK/PG/08) and Compliance Risk Management).			
40	Compliance with Consumer Protection provisions as stipulated in the Consumer Protection Guideline (CBK/PG/22).			

CBK/RMG/ 7-1				
	MONTHLY COMPLIANCE RETURN			
	Institution:			
	Financial Year:		Version 1.1.7.2	
	Start Date:			
	End Date:			
No.	**Legal and Regulatory Requirements**	**Actual Position**	**Compliance Yes/No**	**Comments**
	NB: 1. This Compliance return should be submitted by 5th of every month to the Central Bank of Kenya, Bank Supervision Department. 2. Misreporting and late submission will be subject to penalties. 3. Officers compiling, checking and authorizing this return shall be held accountable for the accuracy/inaccuracy of this return.			
	AUTHORIZATION:			
	We declare that this return, to the best of our knowledge and belief is correct.			
	Name of Compiling Officer: **.....**	**Sign:** **……**		**Date: ……...**
	Name of Authorising officer (1): **.....**	**Sign:** **…….**		**Date: ……...**
	Name of Authorizing officer (2): **.....**	**Sign:** **……..**		**Date: ……...**

10. COUNTRY AND TRANSFER RISK MANAGEMENT

10.1 Introduction

10.1.1 Definitions

Country risk is the risk that economic, social, and political conditions and events in a foreign country will adversely affect an institution's financial condition. For example, financial factors such as currency controls, devaluation or regulatory changes, or stability factors such as mass riots, civil war and other potential events that contribute to institutions' operational risks.

In addition to the negative effect that deteriorating economic conditions and political and social unrest may have on the rate of default by obligors in a country, country risk also includes the possibility of nationalization or expropriation of assets, government repudiation of external indebtedness, sudden changes in exchange control, tariffs and trade policies, and currency depreciation or devaluation.

Transfer risk is the risk that a borrower may not be able to secure foreign exchange to service its external obligations. Where a country suffers economic, political or social problems, leading to drainage in its foreign currency reserves, the borrowers in that country may not be able to convert their funds from local currency into foreign currency to repay their external obligations.

Other types of country and transfer risk

i. **Sovereign risk** denotes a foreign government's capacity and willingness to repay its direct and indirect (i.e. guaranteed) foreign currency obligations.

ii. **Contagion risk** arises where adverse developments in one country lead to a downgrade of rating or a credit squeeze not only for that country but also other countries in the region, notwithstanding that those countries may be more creditworthy and that the adverse developments do not apply to them.

iii. **Currency risk** - the risk that a borrower's domestic currency holdings and cash flow become inadequate to service its foreign currency obligations because of devaluation;

iv. **Indirect country risk** – the risk that the repayment ability of a domestic borrower is endangered owing to the deterioration of the economic, political or social conditions in a foreign country where the borrower has substantial business relationship or interests.

v. **Macroeconomic risk** – the risk that the borrower in a country may, for example, suffer from the impact of high interest rates due to measures taken by the government of that country to defend its currency.

vi. **Geopolitical and sanctions risk**: the risk of adverse impacts arising from geopolitical events such as international conflicts, trade restrictions, or sanctions regimes that may disrupt international relations and economic stability.

vii. **Climate and environmental risk:** country-level physical and transition risks related to climate change.

10.1.2 Background

- When an institution engages in international lending, establishes a subsidiary or a branch in a foreign country or incurs a cross-border exposure, it is exposed to not only customary credit risk but also country risk. Country risk is the primary factor that differentiates international lending from domestic lending. It encompasses all the uncertainties arising from the economic, social and political conditions of a country that may cause borrowers in that country to be unable or unwilling to fulfil their external obligations.

- Country risk may arise from deteriorating economic conditions, political and social upheavals, nationalisation or expropriation of assets, government repudiation of external indebtedness, exchange controls and currency devaluation.

- Country risk is a special form of risk over which institutions can exercise little direct influence. Institutions should therefore ensure that they have adequate systems and expertise to manage their cross-border exposures and avoid taking undue concentration risks on such exposures.

- The level of sophistication of an institution's country risk management system should be commensurate with the size, nature and complexity of its cross-border exposures.

10.1.3 Board and Senior Management Oversight

The Board of Directors is responsible for defining the institution's country and transfer risk appetite. Further the Board is required to develop and approve policies, limits, and a governance framework for country and transfer risk. The Board shall ensure that country risk is integrated into the institution's enterprise risk management framework, capital planning,

liquidity management, and stress testing processes. The Board shall also ensure adequate resources and expertise to manage country and transfer risk.

Senior Management is responsible for implementing the approved policy, establishing effective procedures and monitoring compliance. A designated senior officer, typically the Chief Risk Officer, shall have overall accountability for country and transfer risk management.

10.2 Policies and Procedures

Institutions with significant cross-border exposure should have adequate policies and procedures for identifying, monitoring and controlling country risk and transfer risk in their international lending and investment activities. The institution policies and procedures should also provide for maintenance of appropriate reserves against such risks. The details to be included in the policy, and any procedures drawn up in respect of them, depend on the nature and scope of an institution's cross-border activities.

Generally, an institution should define its business strategy for operations in overseas countries. It should establish the parameters for conducting such business, including its risk appetite and risk tolerance, taking into account its financial resources, staff expertise and systems. The institution should also have systems for identifying, measuring, monitoring, reporting and provisioning for country risk. Such policies/ procedures should encompass the following aspects:

(1) Clear lines of authority (including approval of cross-border lending and exceptions), responsibility and accountability for country risk management;
(2) Types of country risk which may be incurred by the institution and the policies and procedures for managing them (in particular whether the institution's country risk management process is centralized or decentralized and integrated with the overall credit risk management);
(3) The overall limits and sub-limits for cross-border exposures;
(4) The standards and criteria which the institution will use to analyze the risk of particular countries;
(5) The internal country rating system, if any, or how the country risk elements are factored into the institution's existing loan classification system;
(6) The method to be used in measuring country risk exposures;
(7) The country risk provisioning policy and methodology;
(8) Types of and criteria for acceptable collateral and guarantees, financial instruments and hedging strategies (e.g. credit derivatives or netting arrangements) which are allowed

to be used for the mitigation of country risk and the requirements for perfection of collateral;

(9) The minimum standard terms and conditions to be incorporated in loan documentation in accordance with the legal requirements of each country;

(10) The requirement for registration, if applicable, of credit granted and guarantees accepted, noncompliance with which may render the exposure or guarantee not legally enforceable by the institution; Lists of designated lawyers for evaluating the legitimacy of documentation and perfection of collateral; Due diligence requirements for the lawyers.

(11) Any other risk mitigation techniques to be employed by the institution.

(12) Procedures for dealing with deteriorating situations in a country, with clear contingency plans and exit strategies; and

(13) Types of management reports on country and transfer risk.

(14) Prohibited and restricted country lists;

The policy should be reviewed at least annually to determine if it is still appropriate for the institution's business and compatible with changing market conditions.

10.3 Measurement and Monitoring of Country Risk

Each institution must be in a position to identify country risk exposure and monitor the performance of these positions. Systems for measuring country exposure need to be tailored according to the size and complexity of the institution's international lending and investing operations. The objective is to maintain a system comprehensive enough to capture all significant exposures and detailed enough to permit adequate analysis of different types of risk.

10.3.1 Measurement System

Each institution needs to develop country risk measurement system framework which:

a) Makes Allowance for Risk Allocation

Each institution exposed to country and transfer risk should be able to determine where the final risk lies. In addition to allocating each claim according to the residence of the borrower, it will also be necessary to consider how to take into account additional factors which in practice may give the institution a claim on a resident of a different country. The institution's system should therefore be capable of assessing the exposure by country of the borrower and make an allowance for risk transfers.

b) Ensures Consolidation

Each institution should measure country and transfer risk on a consolidated basis in order to obtain a picture of overall exposure to foreign borrowers outside its own operations. Consolidation embraces the operations of the institution's branches, subsidiaries, other related institutions and any other institution that assists in the management of overall exposure to country risk. In addition to measuring its country exposure on a consolidated basis, the institution should also take account of the gross country exposure arising from the funding of its individual overseas branches and subsidiaries.

c) Capture the Breakdown and Analysis of Claims by Borrowing Country

Country exposure should include on balance sheet, off balance sheet and contingent exposures which represent claims on residents of another country. A breakdown of residual maturity of claims will assist in providing a comprehensive maturity profile of indebtedness. Additional breakdowns, for example, distinguishing between claims on sovereign borrowers, banks and others, will also assist the institution's management to assess the country exposure.

Deposits from a country should not ordinarily be offset against credits to that country unless the institution has established a legal right of set-off vis-à-vis the same customer. Some potential claims that may involve risk include letters of credit and legally binding commitments to lend to foreign clients. Fiduciary operations should also be considered where the institution acts as an agent, which may give rise to country exposure.

The country risk measurement should also be able to capture exposure by country, counterparty type, currency, tenor, and product.

Forward-looking indicators, stress testing, and scenario analysis shall be used to assess potential deterioration in country conditions where the institution has exposure. The findings must be brought to the attention of the senior management officers responsible.

10.3.2 Risk tolerance limits

Banks with foreign exposure must have risk tolerance limits for country risk. The limits must be in line with the risk appetite of the bank and should be reviewed regularly and adjusted in response to material changes in country risk profiles.

For effective oversight, institutions are required to:

- Specify authorised activities and instruments.
- Set up a mechanism to monitor and report the institutions' country exposure for senior management and BOD's review.

10.3.3 Internal Control System

The institutions should have adequate information systems and internal controls to monitor compliance with country risk limits. The systems should enable the institution to detect a limit violation in good time and enable timely reporting to the senior management and the board. The employees who are entrusted with controlling country risk limits must have the required knowledge and must be sufficiently independent from the staff whose work they are assigned to monitor.

10.3.4 Lending principles

The following principles should be taken into consideration:-

i. Institutions should ensure that facilities granted to overseas borrowers are subject to the basic prudent credit granting criteria applicable to domestic exposures. The principle of "**Know Your Customer**" should be upheld.

ii. Institutions should ascertain the identity and the ultimate ownership of the borrowers, regardless of their place of incorporation and the complexity of their group structure. Where appropriate, institutions should obtain written evidence or confirmation from relevant parties of the identity of borrowers and their shareholder structure in name and percentage terms.

iii. Credit should only be granted to creditworthy borrowers and due diligence should be carried out. Institutions should not simply lend on the basis of the name or official status of a borrower or rely on any implicit governmental guarantee. Institutions should satisfy themselves that the borrowers have sufficient foreign currency assets or income streams to service their foreign currency obligations.

iv. Institutions should not grant credit based on inadequate information. In some countries, borrowers may be unable to provide comprehensive financial information or audited accounts prepared in accordance with international accounting standards. However, institutions should obtain sufficient information to properly assess the credit proposal.

v. As with all lending, institutions lending to overseas entities should verify what the funds are being used for. Institutions should assure themselves that the proceeds are used for the intended purpose and are not diverted to speculative investments in commodities, property or stock markets. Where funds are being used for a project, institutions should satisfy themselves that funds are not used for purposes other than financing the project. Frequent site visits and drawing by installments can help to prevent the misapplication of funds.

vi. Institutions should not grant facilities to a particular economic sector purely based on government direction or benefits provided by the government such as tax concessions. They should place greater weight on borrowers' repayment ability and the risks of and return from each transaction.

vii. Some countries are undergoing a process of economic development and restructuring. The infrastructure of commercial laws and regulations may not develop at the same pace. In larger countries, owing to the needs of different regions, a lack of uniformity in laws and regulations and the interpretation of central directives by regional and provincial governments may exist. Institutions should therefore beware of the assumption that what applies in one region or province applies in another. In case of need, institutions should seek advice from external counsel and get clearance from the relevant authorities.

viii. Before accepting collateral covering overseas exposures, institutions should ensure that there has been full compliance with statutory procedures to strengthen validity and enforceability. Where tangible collateral such as land and buildings in the country concerned is taken, institutions should ensure that the pledgor has good title to the collateral and that any valuation reports are reliable. To this end, institutions should retain local lawyers who are familiar with local laws, regulations and practices to check the legitimacy and enforceability of loan agreements, guarantees and other documentation.

10.3.5 Country Risk Ratings

A number of institutions may not have the capacity to develop internal country risk assessment mechanisms. For other institutions, it may not be feasible to establish these mechanisms, given the level of their cross-border exposure. The institutions that have significant cross-border exposure, greater analytical resources and access to better information should consider external rating as an input for their internal ratings. Ratings should be reviewed semi-annually or more frequently if the situation warrants.

Economics or research units in each major institution having significant cross-border and foreign exposure should be entrusted with preparing assessments of the country risk of the countries in which the institution is involved. The analysis, process and the level of resources devoted to it will depend upon the size of foreign exposure and the following may be taken into account:-

- A formal country risk analysis should be conducted at least semi-annually for every country which the bank has a significant level of exposure (the significant level may be determined by the board or management).
- The analysis should be properly documented and conclusions reported in a way that provides the decision makers with a reasonable basis for determining the nature and level of the institution's exposure in a country.
- The analysis should cover all exposures and take into account all aspects of broadly defined concepts of country risk.

10.3.6 Country Risk Limits

Institutions can minimise the country risk inherent in their cross-border exposures by diversification and setting country exposure limits. In setting the country exposure limits the following should be considered:

- Prudential limitations - Section 8(A) of the Banking Act requires branches and subsidiaries outside Kenya to be approved by the Central Bank. Further, Section 12 (b) of the Banking Act places restrictions for institutions in Kenya from acquiring or holding a beneficial interest in an undertaking (subsidiaries in this particular case) to a maximum of 25% of its core capital.

- Since different product lines or activities in the same country carry different levels of risk, it is appropriate to support aggregate country exposure limit with more discrete controls. Such controls might take the form of sub-limits on the basis of business lines, types of obligors or tenor etc.

- There may be separate limits for total country exposure, as well as country foreign currency exposure. However, Foreign Exposure limits as set out in the Central Bank of Kenya Prudential Guidelines on Foreign Exchange Exposure Limits (CBK/PG/06) must strictly be adhered to.

Limits should be periodically reviewed to incorporate changing scenarios. Finally, once the limits are set, they should not be breached without going through a procedure for approval

from a designated approving authority as identified by the board or policy-making group, which actually approved the policy and the said limits. The institutions should establish a mechanism of monitoring compliance with these limits. Any breach of limits should be reported to the senior management who should take appropriate corrective action.

10.3.7 Management Information System

Institutions should have an effective system in place to generate management reports which are detailed enough to permit analysis of different types of risk and cover all aspects of institution's operations. The reports should also identify the exceptions in a timely manner. Institutions should consider not only outstanding exposures but also undrawn commitments as well.

10.4 Internal Control and Audit

Country risk management process should have an adequate internal control mechanism. To achieve objectivity, the responsibility of marketing and lending personnel should be segregated from responsibilities of personnel who analyse country risk, assign country risk ratings and set limits structure. The internal audit function, in addition to review of compliance with policies /procedures, should ensure the integrity of the reports / information prepared for senior management, governance effectiveness and adequacy of controls.

10.5 Reporting and Disclosure

Country risk exposure as well as comments on large differences between the bank’s own ratings and externally available country assessments must be part of the institution's risk reporting. This reporting must also include regular country and transfer risk reports which should be reported quarterly to the Central Bank as per Appendix II (CBK/PR/30). Extraordinary changes/events must be reported immediately to the Central Bank.

11.0 MODEL RISK MANAGEMENT

11.1 Introduction

Model risk refers to the potential for adverse financial consequences associated with models, which may result from decisions made based on model output.

Model risk increases with greater model complexity and usage and can arise from a wide variety of situations, including:

- The use of a modelling approach that is not appropriate for the model's intended use.
- Incorrect assumptions used during model development.
- Inappropriate and/or inaccurate data used for model estimation.
- Incorrect standards for model accuracy relative to the model's intended use.
- Mistakes in model implementation that cause the implemented model to differ from the initial model.
- Misinterpretation of model results.

Models are simplified representations of real-world relationships among observed characteristics, values, and events; they are based on assumptions that make them useful in estimating values and predicting events, but which also can have limitations and create model risks. A model has three distinct components namely:

i. **Input**: The input component of a model encompasses the data and assumptions used to develop the model;
ii. **The processor:** This is usually a methodology constructed from mathematics, statistics, finance or economics and transforms inputs into estimates;
iii. **Results / Reporting component:** This is the output of the model which can either be quantitative or qualitative.

Material models are used to support key functional activities and decision-making processes of an institution. Errors and/or improper functioning of such model will likely result in significant impact on strategic positioning and substantial financial losses in relation to capital.

11.2 Governance

11.2.1 Clear Roles and Responsibilities

Every party involved in the model life cycle should have clearly defined and communicated responsibilities. This clarity ensures accountability and supports effective oversight and decision-making. Key roles include:

- **Model Owner:** The unit(s) or individual(s) responsible for coordinating model development, implementation and deployment, ongoing monitoring and maintaining the model's administration, such as its documentation and reporting. The model owner may also be the model developer or user.
- **Model Developer:** The unit(s) or individual(s) responsible for designing, developing, evaluating, and documenting a model's methodology.
- **Model Reviewer:** The unit(s) or individual(s) responsible for reviewing the model's conceptual soundness, inputs, methodology, assumptions, and performance. Other responsibilities might include providing the model developer and user with guidance on the appropriateness of models for defined purposes and assessing model monitoring results as a part of periodic or ongoing validation.
- **Model Approver:** The unit(s) or individual(s) or committee(s) with the authority to approve the use of a model within the institution, typically after considering the findings reported by the model reviewer and other governance requirements. This role is often part of a higher-level governance body (for example, a Model Risk Committee or senior management function) that ensures each model aligns with the institution's risk appetite and strategic objectives.
- **Model User:** The unit(s) or individual(s) that rely on the model's outputs to inform business decisions.
- **Model Stakeholder:** The unit(s) or individual(s) that are involved in the model lifecycle, use and governance of the model (for example, all parties defined above, legal team, compliance function).
- **Model Risk Committee:** Institutions should establish a Model Risk Committee or designate an existing committee with responsibility for oversight of model risk. The committee should serve as the primary governance and reporting forum for matters relating to models throughout their lifecycle and should be responsible for overseeing all models and ensuring the effective management of model risk across the institution.

  The committee may comprise both permanent and ad hoc members. Permanent members may include the Chief Risk Officer, Head of Model Development, Head of Model

Validation, and Head of Internal Audit among others. Ad hoc members may include relevant business representatives, model users, and other subject matter experts involved in the model under discussion, such as model developers or validators.

11.2.2 Board and Senior Management Oversight

The prerequisites of an effective model risk management include an informed board, capable management, staff with relevant expertise and efficient systems and procedures. It is the responsibility of an institution's board and management to implement best practices in model governance at every stage of the model risk management cycle.

11.2.2.1 The Board of Directors

The ultimate responsibility for model risk management rests with the Board of Directors. The Board of Directors should:

- Have sufficient knowledge of the models used in the institution.
- Establish a comprehensive model risk management framework that is part of its broader risk management framework and proportionate to its size, business activities, the complexity of its models, and the nature and extent of use of models.
- Approve the model risk management policy and its annual review to ensure it remains aligned with the institution's current circumstances, priorities, and strategic direction.
- Approve the scope and application of models used by the institution.
- The institution shall establish and maintain a Model Risk Appetite Framework approved by the Board. The framework shall define the level of model risk the institution is willing to accept as it achieves its strategic objectives.
- Provide challenges to the outputs of the material models and understand: the capabilities and limitations of the models, the model operating boundaries under which model performance is expected be acceptable, the potential impact of poor model performance and the mitigants in place should model performance deteriorate.

With respect to material models, the Board or a dedicated committee should be responsible for approval of:

- The results of model validation.
- Withdrawal and introduction of changes to models.
- Monitoring the introduction of suitable remedial and corrective measures.

In order to execute its function effectively, the Board is required to receive and review, on an ongoing basis, and at least annually, the following information:

- An inventory/register of all models used across the institution.
- Key findings of performed monitoring, model validation and internal audits.
- The status of recommendations (from monitoring, validation and audit) issued in the previous periods and the effectiveness of the remedial and corrective measures undertaken.
- Assessment of the level of the institution's aggregate exposure to model risk in the context of the adopted risk tolerance level.
- A list of planned measures in the management of models and the anticipated risk.

11.2.2.2 Senior Management

The senior management is responsible for implementing sound policies and procedures, keeping in mind the strategic direction and risk appetite specified by the board. To effectively oversee the daily and long-term management of model risk management framework, senior managers should:

- Establish policies and procedures to operationalize the model risk management framework and ensure compliance;
- Assign the roles and responsibilities of the framework;
- Ensure independent validation;
- Evaluate and review model results and validation and internal audit reports;
- Ensure effective challenge;
- Actively manage model risks making use of all available information;
- Ensure availability of adequate and appropriately skilled personnel responsible for model risk management;
- Ensure availability of adequate management information system infrastructure and access to data for the effective performance of tasks;
- Ensure accuracy of the model register and model materiality assessments;
- Ensure an integrated approach to aggregate model risk measurement, assessment and ongoing monitoring in the context of the adopted risk tolerance level; and
- Take prompt remedial action when necessary to ensure the firm's aggregate model risk remains within the board approved risk appetite.

11.3 Policies and Procedures

Institutions should develop and implement policies and procedure manuals approved by the Board, outlining the processes of identification, estimation, monitoring, control and reporting of model risk. The policies and procedures should be reviewed regularly to ensure they remain relevant to the institution's model risk appetite and risk profile, as well as changes in the economic and business environment and emerging technologies to which the institution is exposed.

11.3.1 Policies

Institutions should have comprehensive policies that formalize the model risk management framework and ensure its effective implementation.

The bank’s model risk management policy should provide for the following:

- The definitions of model and model risk, and any external taxonomies used to support the model identification process.
- Appropriate organizational structures for model risk management, including governance structure, reporting lines, and accountability.
- Clearly defined roles, responsibilities, and scope of work for individuals, committees, and functions involved in the model risk management process.
- Standards for model development, including; model testing, model selection criteria, documentation standards, model performance assessment criteria and thresholds, and supporting system controls.
- Minimum standards for model risk management within the institution, including formal processes for managing models and their associated risks throughout all stages of the model lifecycle.
- Appropriate safeguards to prevent the use of models that do not meet specific quality standards or are characterised by excessive risk level.
- Model risk tolerance levels which are cognizant of an institution’s risk appetite.
- Model materiality assessment approach, including: the criteria and data sources used to assess model materiality; how model materiality is used to determine the scope, intensity and frequency of model validation; the roles and responsibilities for assessing model materiality and complexity; and the process for the approval of model materiality assessments.
- Model change management, including the materiality criteria used to assess the potential impact of proposed changes.

- Standards for measuring and monitoring model performance, including: the criteria to be used to measure model performance; the thresholds for acceptable model performance; criteria to be used to determine whether model recalibration or redevelopment is required when model performance thresholds are breached; processes for conducting root cause analyses to identify model limitations and systemic causes of performance deterioration processes for performing and use of back-testing.
- The key model risk mitigants, including: the use of model adjustments and overrides to reflect use of expert-judgement; processes for restricting, prohibiting, or limiting a model's use and how model validation exceptions are escalated.
- The updating of the policy at regular intervals and when material changes have occurred that will impact the model risk management process.

11.3.2 Procedures

Institutions should establish appropriate procedures and processes to implement their model risk management policies and include the following features:

- Model origination, documentation, and review of the model's conformity with internal and external requirements.
- Selection of external service providers of models and the scope of the services rendered.
- Defining the scope of model application, the usage and the limitations of the model, including determination of circumstances when the model and its results are not valid.
- Model testing procedures; approval of the results of the model implementation tests in the production environment, confirming that the model meets all the intended functionalities and operates in line with the test version of the model.
- The governance, validation, independent review, approval and monitoring procedures that need to be followed when a material change is made to a model.
- Data quality management procedures, including: the rules and standards for data quality, accuracy and relevance; identification of type and sources of data used by models; ensuring access to the right data at the stages of development, use and performance quality verification of the model.
- The creation of timelines for the various stages from model development through to reviews and decommissioning, informed by the performance of the model and environmental developments.
- Creation of back-up copy of the model, the documentation and the source code.
- Upgrading and maintaining model code.
- Performance of model validation and approval of the validation results.
- Development of a model register/inventory.

- Perform quality assurance on the services provided by external suppliers.
- Updating the model, the code and related documentation to reflect any changes done.
- Preparation of management information and reports.
- Model monitoring, documentation of monitoring findings, and approval of the results obtained through the monitoring process.
- Initiation of specific remedial or corrective measures in the case of deterioration of model performance quality.
- Standards for model validation, including: clear roles and responsibilities; the validation procedures performed; how to determine prioritisation, scope, and frequency of re-validation; processes for effective challenge and monitoring of the effectiveness of the validation process; and reporting of validation results and any remedial actions.

11.4 Model Lifecycle

Model Lifecycle comprises various stages that define the existence of a model from conceptualization to decommissioning. Key lifecycle stages include model design (including model rationale, data, methodology, and development), validation, approval, implementation, monitoring, review and re-validation, change management, and decommissioning. The sequence and application of these stages may vary depending on the nature, complexity, and use of the model, as well as the institution's governance arrangements.

11.4.1 Model Development

All models should have a clear statement of purpose and design objective(s) to guide the model development process. The design of the model should be suitable for the intended use, the choice of variables and parameters should be conceptually sound and support the design objectives. Mathematical specifications and numerical techniques and approximations should be explained in detail with particular attention to their merits and limitations. The underlying assumptions of the model should be reasonable and valid.

The choice of modelling technique should be conceptually sound and supported by published research, where available, or generally accepted industry practice where appropriate. The output of the model should be compared with the outcomes of alternative theories or approaches and benchmarks, where possible.

11.4.1.1 Use of data

Data can vary in terms of sources, formats, and types. It may be structured, semi-structured or unstructured. It can also be synthetically generated or derived from proxy sources. The

consequences of flawed data (for example, due to inaccuracies, bias, or missing records) is significant.

Institutions should adopt robust data governance with standards for collecting, storing, and accessing data used in models. This should be integrated with enterprise-level data governance, strategy, and management. Data leveraged for model development should be:

- Accurate and fit-for-use (that is, free from material errors with biases understood and managed).
- Relevant and representative (that is, reflecting the intended target population of the model).
- Compliant (that is, adhering to statutory, regulatory, and internal requirements for data ethics and customer privacy).
- Traceable (that is, having documented lineage and provenance).
- Timely (that is, updated at an appropriate frequency).

One important purpose of the above data properties is to enhance the explainability of the model and associated outputs. Consideration needs to be given to the potential for unwanted bias within the data which can translate into unfair model outputs with associated reputational risks.

Institutions should also:

- Regularly perform thorough data quality checks (for example, outlier detection, missing value analysis, and consistency evaluations).
- Implement controls to ensure quality and document provenance and use of synthetic data and proxy data.
- Have controls to ensure appropriate data cleansing operations (for example, handling of inaccurate and missing values).

11.4.2 Model Testing

Model testing is a core component of model development that evaluates whether a model performs as intended. Testing may include a range of activities, from out-of-sample and out-of-time testing, to a comparison of alternative assumptions and methodologies, to a critical assessment of data quality, relevance, and inputs. Testing may be performed by model developers in collaboration with model users.

The specific approach depends on the model’s characteristics. The extent and rigor of testing should be commensurate with the model's complexity and materiality. For models that have

relatively less material impact or for banking organizations with relatively less complex operations, model testing may be more limited in scope.

11.4.3 Model Validation

Institutions should put in place appropriate model validation processes and activities intended to verify that models are performing as expected, with respect to their design objectives and uses. The model validation performed by model developers is the first line of defense against model risk. Model developers should conduct their own validation of the model to ensure that appropriate steps were taken in model development.

All material models, whether they were internally or externally developed, should be subject to validation. The validation techniques employed should be in line with the usage of the model, the complexity and materiality of the model, as well as the institution's size and complexity.

The timing, nature, and frequency of validation activities will vary based on model purpose, model methodology, frequency and scope of model change
s, data limitations, and other practical constraints.

11.4.3.1 Independent Validation Function

- The size and complexity of an institution may warrant the establishment of an independent model validation unit. In situations where the scale and complexity of an institution's operations do not support the establishment of a fully-fledged model validation unit, model validation can be performed through a peer review process. Further, institutions may outsource the validation of their models to external validators who have the technical expertise to perform the function.
- The validation function provides an objective and unbiased opinion on: the suitability and soundness of models for their intended use, the design and integration of the system supporting the model, the accuracy, relevance and completeness of the development data, and the output and reports used to inform decisions.
- The validation function should operate independently from the model development process and from model owners and users.
- The validation function should be responsible for the independent review and the periodic re-validation of models and should provide their recommendations on model approvals to the appropriate model approval authority.

- While model owners are responsible for model performance, model users, owners, and validators share the responsibility for ongoing model performance monitoring and process verification.
- The validation function should have sufficient organisational standing to provide effective challenge and have appropriate access to the board and/or board committees to escalate concerns around model usage and model risk management in a prompt and timely manner.

11.4.3.2 Independent Review

All models should be subject to an independent review to ensure that models are suitable for their intended use. The independent review should:

- Cover all model components, including model inputs, calculations, and reporting outputs.
- Assess the conceptual soundness of the underlying theory of the model, and the suitability of the model for its intended use.
- Critically analyse the quality and extent of the model development evidence, including whether the data used to develop the model are relevant, complete, and representative of the portfolios, products, assets, or customer base for which the model is intended.
- Evaluate qualitative information and judgements used in model development, and ensure those judgements have been conducted in an appropriate and systematic manner, and are supported by appropriate documentation; and
- Conduct additional testing and analysis, as necessary, to identify potential model limitations and ensure they are addressed on a timely basis.
- Review the developmental evidence of the sensitivity analysis performed by the model developers to confirm the impact of key assumptions and the selection of variables during model development on the model outputs.

11.4.4 Periodic Revalidation

Institutions should undertake regular independent revalidation of models (typically less detailed than the validation applied during initial model development) to determine whether the model has operated as intended, and whether the previous validation findings remain valid, should be updated, or whether validation should be repeated or augmented with additional analysis.

11.4.5 Model approval

Model approval processes should occur throughout the model lifecycle. The model approval decision typically involves two components:

- Assessing whether the model is suitable to be implemented into production (or continue to be used) based on its intended use.
- Affirming the assigned model risk rating and residual risk assessment.

The model may be approved despite identified weaknesses or limitations provided that compensating mitigants are in place, or the model stakeholder group provides justification for using a model with known limitations or weaknesses.

11.4.6 Model Implementation

Model Implementation is the process of deploying a model into production, where design and testing meet real-world applications. It is critical to ensure that models perform as intended, are used appropriately and integrate smoothly into business processes. Without strong governance at this stage, models can underperform, be misused, or introduce operational and compliance risks. Treating implementation with the same rigour as development, validation, and monitoring helps ensure reliable performance, operational readiness, and user confidence.

11.4.7 Change Management

All material model changes should be governed through a formal change control process that includes comprehensive review, testing, validation, and approval prior to implementation. The changes may include, but not limited to, methodology changes, the introduction of new variables, changes in data sources, model assumptions, or recalibration of parameters.

The institution should conduct impact assessments to evaluate the effect of proposed changes on model performance, risk exposure, outcomes, and related business processes. Every material change must be assigned a unique version identifier and tracked throughout its lifecycle to maintain a clear audit trail and facilitate accountability. In addition, all relevant model documentation, validation reports, monitoring plans, governance records, and model inventory entries should be promptly updated following the implementation of any approved change to ensure ongoing accuracy, transparency, and effective model governance.

11.4.8 Use of externally developed models

Boards and senior management are ultimately responsible for the management of model risk, even when they enter into an outsourcing or third-party arrangement.

For third-party vendor models, institutions should:

- Satisfy themselves that the vendor models have been validated to the same standards as their own internal model risk management expectations.
- Verify the relevance of vendor supplied data and their assumptions.
- Validate their use of vendor models and conduct ongoing monitoring by comparing model outputs with actual outcomes.
- Ensure that they have contractual rights to obtain sufficient information to independently assess vendor models.

Institutions within banking groups using models developed by their parent-group may leverage the outcome of the parent-group's validation of the model if they can:

- Demonstrate that the parent-group has implemented a model risk management framework and model development and validation standards in line with the expectations set out in this guideline.
- Verify the relevance of the data and assumptions for the intended application of the model by the subsidiary.
- Ensure the model validation conducted is adequate.

11.5 Identification, Monitoring and Reporting

11.5.1 Model Risk Identification

An institution should identify the risk categories that can potentially impact a given model and provide adequate documentation and information concerning the magnitude of the exposures and the controls in place. The assessment should include the following:

- The risks associated with model development, highlighting the model limitations identified in the development phase and their potential impact on model outputs.
- A detailed assessment of the risk arising from low quality data used in model development, the lack of access to relevant data, deficiencies that arise due to the processes of data extraction, processing, aggregation and storage.
- Areas where the sample data size was insufficient, and where the frequency of the data was inadequate.
- The risks associated with:

i. Assumptions used in model development.
ii. Model governance and the management of model risk.
iii. Inadequate documentation.
iv. Model implementation.
v. Misuse or inappropriate application of models.

vi. Estimated parameters and the reliability of model outputs.

11.5.2 Model Risk Rating

A risk rating approach should be implemented based on inherent model risk, thereby reflecting model vulnerabilities and materiality of model impacts. This enables institutions to ensure that their most critical or complex models receive enhanced scrutiny, while less risky models are subject to fewer requirements.

The risk rating approach should be supported by clear, measurable criteria for each risk dimension and incorporate both quantitative and qualitative factors:

- Quantitative factors include the importance, size and growth of the portfolio that the model covers (as applicable), or potential operational, security or financial impacts.
- Qualitative factors include business use or purpose, model complexity or level of autonomy, reliability of data inputs, customer impacts, or regulatory risk.

Each model should be assigned a model risk rating. Institutions should have defined processes to do this. The processes may include having a temporary risk rating that is confirmed in the model review or model approval stage of the model lifecycle. Model risk ratings should be regularly reviewed and updated as appropriate, including when a trigger event occurs (for example, a decrease in performance or a material change in the model's use, data, or infrastructure).

11.5.3 Stress Testing

Institutions should establish a programme for stress testing material models to assess their robustness under adverse but plausible conditions. The scope, frequency, and severity of stress tests should be commensurate with the model's complexity, materiality, and risk. Stress test results should be documented, reviewed by the appropriate governance bodies, and used to identify model limitations, inform model improvements, and strengthen model risk management practices.

11.5.4 Management Information System

Institutions should have a reliable Management Information System (MIS) designed to provide the board of directors, senior management and other appropriate personnel with timely and forward-looking information on the model risk of the bank.

The MIS should have the following capabilities at a minimum:

- Enable tracking of all models within the institution from inception to retirement, listing the necessary documentation through the life of a model inclusive of origination documentation, validation reports, approvals and data used in model development.
- Storage of all model codes and capturing of changes made to the codes, capturing the name, date and documentation used to effect the changes made to the code.
- Monitor model performance against established thresholds and key performance indicators and identify model deterioration or performance drift.
- Produce accurate, timely, and forward-looking reports for the board of directors, senior management, model owners, and relevant committees.
- Facilitate the aggregation and reporting of model risk information across business units, model categories, and materiality levels.
- Generate alerts for key model risk events, including validation due dates, periodic reviews, performance monitoring, model expiry, and policy breaches.
- Maintain comprehensive audit trails of model activities, approvals, modifications and user access.
- Support data quality monitoring by identifying incomplete, inaccurate, or inconsistent model input data and reporting data quality issues.
- Allow the reporting and escalation of model risk events across the affected stakeholders within the institution.

11.5.5 Model monitoring

Ongoing model monitoring involves an evaluation of the extent to which a model is performing as expected given potential changes in products, exposures, activities, clients, data relevance, or market conditions. A model that no longer performs as expected may warrant overlays, adjustment, or redevelopment of the model depending on an institution's model risk management policy as it pertains to model deterioration.

An effective ongoing monitoring plan may also include regularly assessing any model limitations at the development stage and overtime, along with procedures for responding to any issues that may occur, before and after a model is approved for use. The frequency and scope of monitoring reports will depend on the nature of the model, the availability of new data or modeling approaches, and model materiality.

Model monitoring should document, at a minimum:

- Monitoring standards covering frequency, scope, and evaluation criteria as applied to different risk rating levels and model types.

- Evaluating criteria that include both quantitative measures (for example, performance metrics) and qualitative assessments (for example, verifying the model is within its original scope).
- Tracking and evaluating operational factors such as changes in model performance, model usage, input data, external dependencies (for example, version updates), or the characteristics of what is being modelled (for example, added product features).
- Defining thresholds for breaches and criteria for material model modifications, including changes in operational factors.
- Determine contingency plans for model unavailability, deterioration in model performance, or outright failure along with the escalation procedures for addressing these.
- Identified issues, including their communication to relevant stakeholders and the actions taken in accordance with the institution's escalation procedures.

11.5.6 Model Performance Assessment

An institution is expected to have detailed procedures for the assessment of model performance quality. The procedure manuals should clearly articulate the steps that are to be adhered to in the process of model performance assessment taking into account the materiality and specificity of the model.

Suitable measures for assessment of model performance quality should be developed. The measures should be comparable across different model classes and should be interpretable through expert opinion. Further, the assumptions and conditions of applicable statistical tests should be recognized to avoid error in model assessment.

The model performance quality assessment is expected to take into account results from back testing and stress testing to assess the quality of the results that the model produces.

Institutions are expected to perform model performance assessment at least once annually or when necessary guided by the frequency of usage of the model and changes in the operating environment that are deemed to have material impact on the models.

11.5.7 Model Documentation

For effective implementation of the model, institutions should maintain the documentation of all the models in place, some of the details to be maintained include:

- The use of data: a description of the data sources, any data proxies, and the results of data quality, accuracy, and relevance tests;

- The choice of methodology: the modelling techniques adopted and assumptions or approximations made, details of the processing components that implement the theory, mathematical specification, numerical and statistical techniques;
- Performance testing: details of the tests or criteria that will be used to monitor the model's ongoing performance during use, and the rationale for the choice of tests or criteria selected;
- And model limitations and use of expert judgement: the nature and extent of model limitations, justification for using any model adjustments to address model limitations, and how those adjustments should be calculated over time.
- A detailed description of changes made to the model or any intentions to withdraw the model from usage.

11.5.8 Model Inventory

Institutions should maintain an up-to-date inventory of all the models in use capturing the following information in respect of each model:

- the name, number and version of model;
- the origin, scope of application and purpose of the model;
- model materiality assessment;
- location of source documents related to the model;
- assessment of the risk exposure level and the model risk level;
- schedule of future actions related to the model;
- material changes that have been made to the model and the individual who made the changes; and
- the names of individuals responsible for validation, the dates when validation was last performed, and the frequency of future validation.

11.5.9 Model Reporting

Model risk management reporting is the structured process of tracking and communicating model performance, inventory status, and material risk metrics to oversight committees. All the material model failures, significant model risk events, changes in the model policies and significant changes to the model shall be reported to the respective board committee of the institutions.

11.6 Artificial Intelligence

Institutions may use Artificial Intelligence **(**AI) and machine learning in model risk management, especially during model validation such as stress testing of the developed

models and real-time model monitoring. Model risk management softwares can help institutions to manage model risk more effectively. These software's provides advanced features, such as model inventory and tracking and mapping metrics, models and policies to multiple regulatory requirements.

When establishing a rationale for models using advanced techniques like AI. The institution should consider several additional factors that stem from the nature of these models. These includes:

- Level of transparency and explainability required.
- Need for alternative controls, potential for the model to lead to biased outcomes.
- Negative social and ethical implications, or privacy risks.

11.7 Model Decommissioning

Model decommissioning is the formal retirement of a model from active use. An institution may decommission a model due to:

- performance issues (for example, a severe performance failure, repeated monitoring breaches, excessive overrides),
- policy, business, regulatory, or strategic changes,
- obsolete data, methodology, or cost–benefit considerations.

Before decommissioning a model, an institution should:

- Alert all relevant stakeholders of the planned decommission.
- Retain the retired model and documentation for a set period as a benchmark or fallback.
- Determine the additional actions are needed for decommissions of any third-party models.
- Monitor downstream effects to ensure no residual impacts.

11.8 Internal controls and audits

Institutions should ensure that the model risk management processes are subjected to internal audit at least annually. The audit is expected to take into account all actions undertaken by the various participants who have influence on the model risk management process and the various phases of the model lifecycle.

Internal auditors must review the policies, processes, and tools used to control the risks and manage the environment related to models as well as the governance structures for model risk management.

The audit of the model risk management process should give particular attention to:

- The adequacy of the model risk management policy in relation to the risk of the models in the institution.
- Compliance with, and application of, policies and procedures governing the model risk management process.
- The division of tasks and the independence of processes of development, validation and use of models.
- The appropriateness and use of institutional information and data in the model risk management process.
- The completeness and currency of the model register with particular attention paid to assessment of model materiality and model risk level.
- The methods and management of access to the model codes and model change management.
- The quality of management information contained in reports, including the reporting of adverse results and the timeliness and effectiveness of the actions taken to address them.
- Validation process to provide assurance that the validators were not involved in the development process and that the testing results support the accuracy of the validation.
- Ensuring that appropriate revisions or enhancements to internal controls are made.

12.0 RISK MANAGEMENT GUIDELINE ON MONEY LAUNDERING, TERRORISM FINANCING AND PROLIFERATION FINANCING

Abbreviations

AI: Artificial Intelligence

AML: Anti-Money Laundering

BO: Beneficial Owner

CDD: Customer Due Diligence

CFT: Combating Financing of Terrorism

CPF: Countering Proliferation Financing

CBR: Correspondent Banking Relations

DNFBP: Designated Non-Financial Business and Professions

EDD: Enhanced Due Diligence

FATF: Financial Action Task Force

FI: Financial Institution

FRC: Financial Reporting Centre

KYC: Know Your Customer

MER: Mutual Evaluation Report

ML: Money Laundering

NPO: Non-Profit Organisation

PBO: Public Benefit Organisation

PEP: Politically Exposed Person

POTA: Prevention of Terrorism Act

POT-PFR: The Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Prevention, Suppression and Disruption of Proliferation Financing) Regulations.

POT-TFR: The Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on the Suppression of Terrorism) Regulations.

NRA: National Risk Assessment

PF: Proliferation Financing

REC: Recommendation

RBA: Risk-Based Approach

SAR: Suspicious Activity Report

STR: Suspicious Transaction Report

SDD: Simplified Due Diligence

TF: Terrorism Financing

TFS: Targeted Financial Sanctions

VA: Virtual Asset

VASP: Virtual Asset Service Provider

1. Introduction and Scope

These Guidelines provide a Basel-aligned framework for the sound management of money laundering, terrorist financing and proliferation financing risks (ML/TF/PF). They are informed by the Basel Committee on Banking Supervision (BCBS) Guidelines and the Financial Action Task Force (FATF) Recommendations and guidance.

The Guidelines are intended to support institutions in embedding AML/CFT/CPF risk management within their overall governance, risk management and internal control frameworks. Consistent with Basel Committee expectations, institutions should ensure that ML/TF/PF risks are identified, assessed, monitored, controlled and mitigated as part of prudent banking practice.

Key Objectives of these Guidelines include:

Effective ML/TF/PF risk management helps institutions and supervisory authorities safeguard the financial system by:

- protecting the reputation of individual institutions and national banking systems by preventing and deterring the misuse of institutions to launder illicit proceeds or to raise, move or use funds in support of terrorism;
- preserving the integrity of the financial system and supporting government efforts to address corruption and combat the financing of terrorism; and
- reducing institutions' exposure to serious risks, including reputational, operational, compliance and concentration risks, which may arise where ML/TF/PF risk management is inadequate or absent..

2. Active Board and Senior Management Oversight

The Board of Directors has ultimate responsibility for ensuring that the institution maintains an effective AML/CFT/CPF risk management framework. Senior management is responsible for implementing the Board-approved framework, embedding a strong risk culture, allocating adequate resources, and ensuring that deficiencies are promptly remediated.

Board and senior management oversight should be active, informed and continuous. The governance framework should ensure clear accountability, timely escalation of material risks and deficiencies, and effective challenge by independent control functions.

2.1 Board Responsibilities

- The Board should approve the institution’s AML/CFT/CPF strategy, risk appetite and risk-based approach.
- The Board should ensure that the institution identifies, assesses and understands its ML/TF/PF risks and applies controls that are commensurate with those risks.
- The Board should oversee the adequacy of resources, systems and independent assurance supporting the AML/CFT/CPF framework.

2.2 Governance Arrangements and Board Reporting

The Board has ultimate responsibility for governance of ML/TF/PF risk management and should ensure that an overarching framework is in place, proportionate to the institution's size, complexity and risk profile. Accordingly, the Board should:

i. Approve the institution's AML/CFT/CPF strategy.

ii. Establish a risk management culture and ensure that the bank has adequate processes for identifying, assessing, evaluating, mitigating, and understanding the nature and scope of the bank's ML/TF/PF Risk.

iii. Approve the institution's AML/CFT/CPF internal controls, policies, and procedures.

iv. Oversee an AML/CFT/CPF risk assessment, including the identification and mitigation of ML/TF/PF risks.

v. Monitor and assess the effectiveness of the institution's AML/CFT/CPF program, ensuring prompt remediation of deficiencies in response to evolving risks, regulatory developments, and inspection findings.

vi. Ensure that senior management effectively implements Board-approved AML/CFT/CPF policies and is held accountable for addressing deficiencies and compliance failures.

vii. Appoint a suitably qualified and independent Money Laundering Reporting Officer (MLRO) at the senior management level who should report directly to the Board or a designated Board committee.

viii. Ensure that appropriate AML/CFT/CPF training is provided to Board members, senior management, and staff, commensurate with their roles and exposure to ML/TF/PF risks.

ix. Where applicable, ensure the effective implementation of group-wide AML/CFT/CPF policies and oversight of branches and subsidiaries, including those operating in higher-risk jurisdictions.

x. Ensure that adequate financial, human, and technological resources are allocated to support the effective implementation of the AML/CFT/CPF programme.

xi. Ensure that the AML/CFT/CPF controls are subject to regular independent testing and that identified weaknesses are remediated in a timely manner.

xii. Ensure that the institution cooperates with the relevant competent authorities on AML/CFT/CPF matters.

xiii. Ensure that management remains responsive to evolving regulatory expectations, supervisory feedback and emerging sound practices.

2.3 Senior Management Responsibilities

Senior management is responsible for the effective implementation, day-to-day management and ongoing operation of the institution's AML/CFT/CPF framework. In this regard, senior management should:

i. Conduct and maintain institutional ML/TF/PF risk assessments.

ii. Implement effective AML/CFT/CPF policies and procedures covering CDD, EDD, ongoing monitoring, sanctions screening, suspicious transaction reporting and targeted financial sanctions, in line with applicable laws and regulations.

iii. Submit reports to the Board or a designated committee on the institution's ML/CFT/CPF risks, compliance status, suspicious transaction reporting, audit findings, and regulatory or supervisory matters.

iv. Support the MLRO, ensuring they can exercise sufficient authority, independence, access to information, and resources to discharge their responsibilities effectively.

v. Develop and implement regular training programmes for senior management and staff, commensurate with their roles, responsibilities and exposure to ML/TF/PF risks.

3. Adequate Policies, Procedures and Limits

Institutions should maintain Board-approved AML/CFT/CPF policies, procedures and limits that are proportionate to their size, complexity, business model, customer base, products, delivery channels and geographic footprint. Policies should translate the institution's risk appetite into operational requirements and define minimum standards for customer acceptance, due diligence, enhanced due diligence, sanctions screening, transaction monitoring, suspicious transaction reporting, record keeping, training and new product approval.

- Delineation: The institution should have a clear delineation of roles, responsibilities, and accountability for the implementation of consistent policies across the institution.
- Review Cycle: Procedures should be documented in procedure manuals and periodically reviewed at least annually to ensure they reflect current developments.
- Minimum Coverage: At a minimum, documented procedures must cover:

  i. Risk assessment.

  ii. Customer due diligence.

  iii. Enhanced due diligence and transaction monitoring for high-risk customers, including Politically Exposed Persons.

  iv. Ongoing monitoring of transactions.

  v. Detection and reporting of suspicious transactions.

  vi. Targeted financial sanctions.

  vii. Record keeping.

3.1 Customer Acceptance Policy

- Institutions should develop and implement clear customer acceptance policies and procedures to identify the types of customers that are likely to pose a higher ML/TF/PF risk.
- Policies should require baseline due diligence for all customers and enhanced measures where risk is elevated. Simplified measures may be applied only in demonstrably lower-risk situations.
- Financial Inclusion Note: It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged.
- Where the risks are higher, decisions to enter into or pursue business relationships should require enhanced due diligence measures, such as senior management approval. The policy should also define circumstances under which the bank would not accept a new business relationship or would terminate an existing one.

3.2 Customer Due Diligence

3.2.1 Identification and Verification Framework

- CDD measures should be applied not only to customers but also to persons acting on their behalf and beneficial owners. Institutions should establish a systematic procedure for identifying and verifying these parties.
- A bank should not establish a banking relationship, or conduct any transactions, until the identity of the customer has been satisfactorily established and verified.
- Institutions should also verify that any person acting on behalf of the customer is duly authorised.
- The identity of customers, beneficial owners, and representatives should be verified using reliable, independent source documents, data, or information. Banks should be aware that the best documents are those most difficult to obtain illicitly or to counterfeit.
- When relying on alternative source documents, institutions must ensure that the methods (e.g., checking references with other financial institutions, obtaining financial statements) are appropriate and in accordance with risk profiles.
- An institution may require customers to complete a written declaration of the identity and details of the beneficial owner, although the bank should not rely solely on such declarations.

3.2.2 Non-Face-to-Face Verification

Any mechanism which avoids face-to-face contact inevitably poses challenges for customer identification. Institutions offering telephone banking, mobile banking, and/or internet banking should implement procedures to identify and authenticate the customer.

As with face-to-face verification, the procedures to check identity must serve two purposes:

- They must ensure that a person bearing the name of the applicant exists and lives at the address provided.
- They must ensure that the applicant is that specific person.

In no case should a bank disregard its customer identification and verification procedures just because the customer is unable to be present for an interview.

The bank should take into account risk factors such as why the customer has chosen to open an account far away from its principal area of operations, in particular in a foreign jurisdiction. It is critical to apply enhanced due diligence to customers from jurisdictions known to have AML/CFT/CPF strategic deficiencies when called for by the FATF, international bodies, or national authorities.

3.2.3 Customer Risk Profiling

- Information Collection: Purpose of the relationship, level of assets, size of transactions, and the regularity or duration of the relationship should be collected to build a customer profile. The scope should be determined by the customer's business model and activities.
- Profile Functions**:** Customer risk profiles will:
    - Facilitate the identification of any account activity that deviates from "normal" expected behaviour.
    - Assist the bank in determining if a customer category is higher-risk and requires enhanced CDD.
    - Reflect the bank’s understanding of the intended purpose, nature of the business relationship, expected level of activity, and where necessary, sources of funds, income, or wealth.
- Any significant information collected on customer activity or behaviour should be used in updating the institution’s risk assessment of the customer.

3.2.4 CDD Documentation and Incomplete CDD

- An institution should obtain customer identification papers and necessary documentation when undertaking CDD based on the requirements of POCAMLA, POCAML Regulations, and its risk-based policies. The nature and extent of verification information depend on the risk assessment and type of applicant.
- Prohibition on Opening: When an institution is unable to complete CDD measures, it should not open the account, commence business relations, or perform the transaction.
- Delayed Verification: If essential not to interrupt the normal conduct of business, verification may be completed after establishing the relationship under strict risk

management procedures regarding the conditions and restrictions under which the customer may utilize the account prior to verification.

- Remediation and Blocking: Where problems of verification arise during the relationship that cannot be resolved, the institution should close or otherwise block access to the account. Institutions should consider filing an STR in cases where there are problems with the completion of CDD measures.
- Suspicion of Predicate Offences: Where CDD checks raise suspicion that funds are the proceeds of predicate offences related to ML/TF/PF, institutions should not open accounts. Institutions must file an STR with the relevant authorities accordingly and ensure that the customer is not informed, even indirectly, that an STR has been, is being, or should be filed (anti-tipping-off).

3.3 Enhanced Due Diligence Frameworks

3.3.1 High-Risk Customers

High-risk customers will require the application of enhanced due diligence to verify customer identity. If the relationship is complex, or if the size of the account is significant, additional identification measures may be advisable, determined based on the level of overall risk.

3.3.2 Politically Exposed Persons

Politically Exposed Persons (PEPs) present elevated ML/TF/PF risks by virtue of the positions of public trust they hold or have held. Institutions should apply enhanced scrutiny to business relationships and transactions involving PEPs, including their family members and close associates, consistent with applicable legal and regulatory requirements.

3.3.2.1 PEP Categories

- Foreign PEPs: Individuals entrusted with prominent public functions by a foreign country (e.g., heads of state or government; senior politicians; government ministers; senior government, judicial, or military officials; senior executives of state-owned enterprises; senior officials of political parties).
- Domestic PEPs: Individuals entrusted with prominent public functions domestically within Kenya (e.g., members of the National Assembly and Senate; members of County Assemblies; Cabinet Secretaries and Principal Secretaries; senior officials of Constitutional Commissions and Independent Offices; parastatal entities; senior judiciary; officers of the KDF and National Police Service).
- International Organisation PEPs: Persons entrusted with a prominent function by an international organisation (e.g., senior management such as directors, deputy directors, members of boards).
- Family Members: Spouses, civil partners, children and their spouses or partners, and parents of the PEP.

- Close Associates: Individuals known to have joint beneficial ownership of legal entities or arrangements with a PEP; close business relations with a PEP; or those who are sole beneficial owners of an arrangement set up for the benefit of a PEP.

3.3.2.2 Identification, Screening, and De-escalation

- Onboarding and Continuous Screening: Screen all new customers and beneficial owners against commercially available PEP databases, domestic and international lists, adverse media sources, and government registers at the point of onboarding and on an ongoing basis thereafter.
- Trigger Event Screening: Screen existing customers when periodic CDD reviews are conducted and whenever a trigger event occurs, such as a material change in circumstances, a significant transaction or a transaction monitoring alert.
- Verification Supplementation: Use open-source information, including publicly available disclosures from other relevant Kenyan authorities, to supplement commercial screening tools. Do not rely solely on customer self-declaration.
- Cessation of PEP Status: An individual who no longer holds a prominent public function does not automatically cease to be a PEP. Institutions should apply a risk-based approach, continuing to apply PEP-level scrutiny for a period of not less than twelve months following the cessation of the public function. Beyond this period, institutions should make a documented risk-based determination subject to senior management review.

3.3.2.3 Risk Assessment of PEP Relationships

When evaluating a PEP relationship, institutions must conduct a risk assessment considering:

- The nature and seniority of the public function and degree of discretionary authority.
- The jurisdiction, including whether it is subject to heightened corruption risk as reflected in indices like Transparency International's Corruption Perceptions Index.
- The source and nature of the PEP's wealth and origin of funds.
- The nature, purpose, and expected activity of the account.
- Whether the PEP is a current officeholder or former officeholder; and
- The existence of adverse information from credible open sources or law enforcement.

Note: Foreign PEPs should always be treated as higher-risk customers and subject to full EDD measures. Domestic and international organization PEPs should be subject to a risk-based determination, with enhanced measures applied upon elevated risk indicators.

3.3.3 Correspondent Banking

Correspondent banking relationships present elevated ML/TF/PF risks because the correspondent institution extends services to customers of the respondent institution whose identities it does not verify. FIs must apply specific and enhanced due diligence

measures to cross-border correspondent banking relationships and, on a risk-basis, to significant domestic inter-bank service arrangements.

3.3.3.1 Due Diligence on Respondent Institutions

Before establishing a new relationship, the correspondent institution must gather information to understand the respondent's framework. At a minimum, the institution should:

- Assess Controls: Cover the respondent institution's regulatory and supervisory framework, its jurisdiction of incorporation, its compliance with FATF Recommendations (via MERs and follow-up processes), the adequacy of its CDD/monitoring systems, STR filing practices, and its record with respect to enforcement actions.
- Assess Ownership: Identify the beneficial owners and senior management of the respondent institution and check for adverse information.
- Assess Customer Base: Obtain a clear understanding of the respondent's primary customer segments, geographic reach, products offered, and expected transaction flows.
- Document and Update: Document all due diligence in the correspondent relationship file, updating it periodically at a minimum every three years or whenever a trigger event occurs.

3.3.3.2 Approval, Prohibitions, and Payable-Through Accounts

- Senior Management Sign-Off: The decision to establish a new relationship requires senior management approval. For respondent institutions located in high-risk jurisdictions, approval should be obtained at the most senior level, accompanied by a documented justification.
- Shell Bank: FIs shall not establish or continue correspondent banking relationships with shell banks. FIs shall implement reasonable measures to ensure that respondent institutions do not permit their accounts to be used by shell banks. Any suspicion of shell bank exposure must be immediately escalated to the MLRO and senior management for review and potential relationship termination.
- CDD Responsibilities for Payable-Through Accounts: Responsibilities of each party must be clearly documented. Where third parties transact directly through the correspondent account (payable-through accounts), the correspondent must ensure the respondent has verified customer identities at equivalent standards and is able to provide relevant CDD information upon request. The correspondent remains ultimately responsible for risk management.
- Ongoing Monitoring and Exit: Transactions should be regularly reviewed to identify patterns inconsistent with the expected profile. If an institution cannot obtain sufficient information or mitigation fails, it should not establish or should terminate the relationship, document the decision and consider filing an STR with the FRC.

3.3.4 Sanctions Screening Policy Requirements

Institutions should maintain policies requiring customers, beneficial owners and relevant transactions to be screened against applicable domestic and international sanctions lists before onboarding, during the relationship and when lists are updated.

3.3.5 Transfers of Funds During Account Opening

- Transfers of funds from an account in the customer's name in another institution during account opening should be subjected to the same CDD standard as the initial deposit.
- Institutions should conduct their own due diligence and consider the possibility that the transfer is occurring because the customer's account was closed elsewhere due to illicit activity concerns.
- If an institution has reason to believe that an applicant has been refused banking facilities due to illicit activity concerns, it should classify the applicant as higher risk, apply EDD, and consider filing an STR or rejecting the customer.

3.3.6 Anonymous and Numbered Accounts Restrictions

- An institution should not open an account or conduct ongoing business with a customer who insists on anonymity or who gives an obviously fictitious name.
- Confidential numbered accounts should not be treated as anonymous accounts; they are subject to the exact same CDD procedures as all other customers' accounts, even if procedures are restricted to selected staff.
- The identity of a numbered account holder must be verified and known to a sufficient number of staff to facilitate effective due diligence.

3.3.7 Enhanced Due Diligence for Elevated PF Risk

The following high-exposure customer types present elevated PF risk and shall be subject to enhanced due diligence:

- Trading and import/export companies dealing in goods appearing on dual-use control lists.
- Freight forwarders and logistics companies operating across transit hubs and free trade zones.
- Manufacturers of dual-use goods (chemicals, electronics, aerospace components, machinery).
- State-owned enterprises and government procurement entities from sanctions-impacted jurisdictions.
- Entities in free-trade zones experiencing reduced customs and documentation controls; and
- Shell companies and complex ownership structures utilizing obscured beneficial ownership or nominee directors.

3.3.7.1 PF Enhanced Due Diligence (EDD) Measures

Where an institution identifies an elevated PF risk, the following specific measures shall be applied:

- Obtain detailed information on the specific goods traded, countries of origin/destination, and the concrete end-use of goods.
- Identify and verify all beneficial owners and ultimate controlling parties.
- Verify the existence and legitimacy of the underlying trade transaction by reference to shipping documents, commercial invoices, bills of lading, and cargo manifests.
- Obtain senior management approval before establishing or continuing the relationship.
- Apply enhanced ongoing monitoring to detect deviations from expected trade patterns or the sudden introduction of new goods categories.

3.4 Employee and Management Training Programmes

3.4.1 Execution of Training Programmes

- Institutions should implement ongoing employee training programmes so that staff are adequately trained to implement AML/CFT/CPF policies and procedures.
- The timing and content of training must be adapted according to staff needs and the institution's risk profile, varying by function, job responsibility, and length of service. Course materials should be tailored to specific responsibilities to ensure sufficient operational knowledge.
- New employees should be required to attend training as soon as possible after being hired.
- Refresher training must be provided regularly to ensure that staff are reminded of their obligations and that their knowledge and expertise are kept up to date. Scope and frequency should be tailored to the risk factors to which employees are exposed.
- The institution's policies and procedures must be communicated to all personnel through regular training.

3.4.2 Board and Senior Management Training

- Institutions should conduct AML/CFT/CPF training tailored specifically for board members and senior management.
- At a minimum, the training must address governance oversight, compliance with AML/CFT/CPF legislation, regulatory expectations, and the institution's distinct ML/TF/PF risk exposure.

3.5 New Products, Technologies and Innovation Risks

3.5.1 Pre-Launch Risk Assessment

- Institutions should complete the assessment of ML/TF/PF risks, and take the appropriate risk management measures, prior to launching new products and services, business practices, operational techniques, or technologies.
- Institutions should integrate these risk assessment and mitigation requirements directly into their new product, service, channel, or technology development processes.
- For the purpose of assessing these risks, institutions may utilize the same or similar risk assessment models or methodologies as those utilized for institutional risk assessments, updated as necessary for the particular circumstances.
- Institutions should document new product, service, practice, technique, or technology risk assessments, in keeping with the nature and size of their businesses.

3.6 Wire Transfers and Travel Rule Mandates

3.6.1 Payment Chain Definitions

- Originating Institution: The institution that initiates a wire transfer on behalf of the originator (the sending customer).
- Beneficiary Institution: The institution that receives a wire transfer for the account of the beneficiary (the receiving customer).
- Intermediary Institution: Any institution that processes a wire transfer in the payment chain between the originating and beneficiary institutions.
- Cross-Border Wire Transfer: A wire transfer where the originating institution and the beneficiary institution are located in different countries.
- Domestic Wire Transfer: A wire transfer where the originating institution and the beneficiary institution are both located in Kenya.
- Batch Transfer: A wire transfer comprising a series of individual wire transfers sent by a single originator and bundled for transmission.

3.6.2 Obligations of Originating Institutions

For all cross-border wire transfers, the originating institution should obtain and include in the transfer message the following information about the originator and beneficiary:

- Originator Information Required: Full legal name; account number (or unique transaction reference number); address (or in its absence, national identity number, customer ID, or date and place of birth); purpose and source of funds; and required beneficiary info.
- Beneficiary Information Required: Full legal name; account number (or unique transaction reference number); and purpose and source of funds.

3.6.2.1 Cross-Border, Domestic, and Batch Thresholds

- Cross-Border Threshold: Cross-border wire transfers of any amount should include the required originator and beneficiary information. There is no minimum threshold below which these requirements do not apply.
- Domestic Wire Transfers: Originating institutions should ensure the transfer message includes the originator's account number or unique transaction reference number. Full info must be made available to the beneficiary institution and authorities within three business days on request.
- Batch Transfers: Ensure the file contains full originator and beneficiary information for each individual transaction and that full info can be disaggregated by the beneficiary institution upon receipt.
- Verification: Originator information must be consistent with held CDD information, verified at account opening; transfers must not be initiated if identity is unverified.

3.6.3 Obligations of Intermediary Institutions

- Intermediary institutions should ensure that all originator and beneficiary information received with a wire transfer is retained and passed on in full for each subsequent transmission in the payment chain.
- Where technical limitations prevent full transmission, the intermediary should retain a record of all information received and make it available to the beneficiary institution or authorities on request.
- Intermediary institutions should apply risk-based monitoring to wire transfers passing through their systems to identify transfers lacking required info, involving high-risk jurisdictions, or displaying patterns indicative of ML/TF/PF.

3.6.4 Obligations of Beneficiary Institutions

Beneficiary institutions should have policies and procedures to identify wire transfers that arrive without required originator or beneficiary information. Where a transfer arrives lacking information, the beneficiary institution should:

- Take risk-based measures to obtain the missing information from the originating or ordering institution.
- Where information cannot be obtained within a reasonable period, consider restricting or refusing to credit the transfer to the beneficiary account.
- Consider whether the absence of required information warrants filing an STR.
- Screen all incoming wire transfers against relevant sanctions lists and PEP databases. Where a match is identified, apply TFS procedures and withhold credit pending completion of review; and
- Monitor incoming wire transfer activity for patterns indicative of ML/TF/PF, including high volumes of small transfers structured to avoid reporting thresholds or transfers from high-risk jurisdictions.

3.6.5 Record-Keeping and Virtual Asset Integration

- Record Retention: All originator and beneficiary information relating to wire transfers must be retained for a minimum period of seven years from the date of the transaction and made available to the CBK, FRC, and law enforcement on request.
- Virtual Asset Wire Transfers: Where wire transfers are conducted using virtual asset networks or involve VASPs, the obligations set out in this section apply in full to the institution component of the transfer, alongside virtual asset-specific rules.

3.7 Virtual Assets and Virtual Asset Service Providers

3.7.1 Interpretive Definitions

- Virtual Asset: A digital representation of value that can be digitally traded or transferred and used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, or other financial assets covered elsewhere.
- Virtual Asset Service Provider (VASP): Any natural or legal person that, as a business, conducts operations for or on behalf of another party including: exchange between virtual assets and fiat currencies; exchange between forms of virtual assets; transfer of virtual assets; safekeeping/administration of virtual assets; and provision of financial services related to an issuer's offer or sale of a virtual asset.
- Virtual Asset Transfer: A transaction conducted on behalf of an originator through a VASP or obliged entity, which moves a virtual asset from one virtual asset address or account to another.

3.7.2 Enhanced CDD Requirements for VASP Customers

Where an institution's customer is a VASP, enhanced due diligence measures must be applied. In addition, the institution should:

- Identify and verify the legal ownership and management structure of the VASP.
- Assess the AML/CFT/CPF framework applied by the VASP (CDD procedures, monitoring, and STR practices).
- Assess whether the VASP is licensed or registered with the Capital Markets Authority, CBK, or equivalent foreign authority, and the adequacy of the supervisory framework.
- Obtain information on the types of virtual assets supported and the nature of the customer base.
- Apply enhanced ongoing monitoring to the relationship, focusing on unusual volumes or changes in status.

  Prohibition: Institutions shall not establish or continue a business relationship with a VASP that is not registered or licensed with a competent AML/CFT/CPF supervisory authority and cannot demonstrate equivalent controls.

4. Adequate Risk Monitoring and Management Information Systems

4.1 Risk Assessment, Monitoring and Reporting Framework

- Sound risk management requires the identification and analysis of ML/TF/PF risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks.
- An institution should conduct a comprehensive risk assessment to evaluate ML/TF/PF risks. The institution should consider all the relevant inherent and residual risk factors at the country, sectoral, bank, and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied.
- An institution should develop a thorough understanding of the inherent ML/TF/PF risks present in its customer base, products, delivery channels, and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business.
- This understanding should be based on specific operational and transaction data and other internal information collected by the bank as well as external sources of information such as national risk assessments and country reports from international organisations.
- The policies and procedures for CDD, customer acceptance, customer identification and monitoring of the business relationship and operations will then have to take into account the risk assessment and the bank's resulting risk profile.
- An institution should have appropriate mechanisms to document and provide risk assessment information to CBK.

4.2 Risk Reporting and Management Information

- ML/TF/PF risk assessment information should be communicated to the Board and senior management in a timely, complete, understandable and accurate manner.
- MIS should support informed decision-making by presenting material risk exposures, control deficiencies, STR trends, sanctions alerts, remediation status and emerging typologies.
- Responsibility for preparing, validating and escalating AML/CFT/CPF risk information should be clearly allocated within the governance framework.

4.3 Transaction Monitoring Systems

4.3.1 Transaction Monitoring Systems

A bank should have an AML/CFT/CPF monitoring system in place that is adequate with respect to its size, its activities and complexity, as well as the risks present. The monitoring system used should at a minimum:

- Cover all accounts of the bank's customers and transactions for the benefit of, or by order of, those customers.
- Enable the bank to undergo trend analysis of transaction activity.
- Identify unusual business relationships and transactions in order to prevent ML/TF/PF.
- Provide accurate information for senior management relating to changes in the transactional profile of customers.

- Allow the bank, and where appropriate the group, to gain a centralised knowledge of information organized by customer, product, across group entities, or timeframes.
- Use adequate parameters based on national and international experience on the methods and the prevention of ML/TF/PF.
- Make use of the standard parameters provided by the developer of the IT monitoring system, calibrated to reflect the bank's own risk situation; and
- Enable a bank to determine its own criteria for additional monitoring, filing an STR, or taking other steps to minimise risk.

4.3.2 Configuration and Baselining

- A well-defined customer profile acts as a dynamic baseline for establishing expected behaviour when conducting monitoring. In compiling the profile, the bank should incorporate updated, comprehensive, and accurate CDD information.
- The MLRO must have access to relevant IT systems and records necessary to discharge the function effectively.
- Institutions are required to ensure that their transactional monitoring systems are configured in view of their specific risks, contexts, and needs.
- Institutions should be mindful that there is no one-size-fits-all approach to configuring transaction monitoring rules. It is critical to ensure these are calibrated against customer types, range of products, business activities, geographical exposures, and cross-border natures.
- Institutions should periodically test and refine their transaction monitoring rules. Internal audit should evaluate the AML/CFT/CPF IT systems to ensure that they are appropriate and used effectively by the first and second lines of defence.

4.3.3 Integrated Management Information Systems

- Institutions should ensure they have appropriate integrated management information systems, commensurate with size and complexity, to provide both business units and risk/compliance officers with timely information.
- Systems must support the monitoring of customer relationships across lines of business and consolidate transaction history, missing account opening documentation, and significant changes in behaviour or profile.
- Institutions should screen customer databases whenever sanctions lists change, and should also conduct periodic screening to detect foreign PEPs and other higher-risk accounts.

4.3.4 Ongoing Monitoring Frameworks

- Ongoing monitoring should be conducted in relation to all business relationships and transactions, with the extent based on risk as identified in the institution's risk assessment and CDD efforts. Enhanced monitoring should be adopted for higher-risk customers or transactions.
- An institution should conduct cross-sectional product/service monitoring to identify and mitigate emerging risk patterns.

- In establishing monitoring scenarios, institutions should utilize the customer's risk profile, CDD data, and information obtained from law enforcement or other authorities to identify transactions that do not make economic sense, involve large cash deposits, or deviate from expected behaviour.
- Institutions should establish specific policies regarding the extent and nature of required CDD, frequency of ongoing account monitoring, and updating of CDD information and records.

5. Adequate Internal Controls

Institutions should maintain an effective system of internal controls that is commensurate with their ML/TF/PF risk profile and aligned to the three lines of defence. Internal controls should provide reasonable assurance that policies are implemented consistently, suspicious activity is escalated and reported promptly, sanctions obligations are met without delay, and weaknesses are identified and remediated in a timely manner.

- Be adequately resourced in terms of budget, tools and staff.
- Have clearly defined roles and responsibilities.
- Maintain appropriate training and competency standards.
- Promote a sound risk management culture across the organisation.
- Communicate effectively across the three lines of defence.

5.1 First Line of Defence: Business Units

The first line of defence refers to the business units (e.g., front office, customer-facing activity) as the first line in charge of identifying, assessing, and controlling the risks of their business. As part of the first line:

- Policies and procedures should be clearly specified in writing and communicated to all personnel.
- Policies should clearly describe employee obligations, operating instructions and guidance for maintaining compliance with applicable AML/CFT/CPF requirements.
- Internal procedures for detecting and reporting suspicious transactions must be utilized.
- Business units must have adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards.
- Business units must implement ongoing employee training programmes so that bank staff are adequately trained to implement the bank's AML/CFT/CPF policies and procedures.

5.2 Second Line of Defence: Risk, Compliance and MLRO Function

The second line of defence comprises Risk, Compliance and the MLRO function. It should be independent of business units, provide objective advice to management, and act as the principal contact point for relevant authorities.

- Monitoring and Independence: The MLRO should monitor fulfilment of AML/CFT/CPF obligations through sample testing, exception report reviews and escalation of material issues. Potential conflicts of interest should be avoided; the MLRO should not hold business-line, data protection or internal audit responsibilities.
- Operational Mandates: Where conflicts between business lines and the responsibilities of the MLRO arise, procedures should ensure concerns are objectively considered at the highest level.
    - The MLRO will be the pivotal point of contact with the FRC and CBK for AML/CFT/CPF purposes.
    - The officer should have the necessary authority, along with access to systems and records to enable the fulfilment of responsibilities.
- Core Functions of the MLRO:
    - Receive and review suspicious transaction reports (STRs) from staff.
    - File STRs with the FRC without delay.
    - Develop and enforce the institution's AML/CFT/CPF compliance programme.
    - Coordinate training of staff in AML/CFT/CPF awareness and detection methods; and
    - Maintain close co-operation and liaison with the FRC and CBK.
- Reporting Lines: The MLRO should be approved by CBK and have a direct reporting line to senior management and the board. The chief risk officer or the chief compliance officer or equivalent may serve as the MLRO. In case of a separation of duties, the relationship between these officers and the MLRO must be clearly defined and understood.

5.3 Third Line of Defence: Independent Assurance

The third line of defence is the internal audit function, which provides independent assurance to the Board Audit Committee on the adequacy and effectiveness of AML/CFT/CPF governance, controls and risk management.

- Strategy and Scope: A bank should establish a methodology for conducting audits of:
    - The adequacy of the bank's AML/CFT/CPF policies and procedures in addressing identified risks.
    - The effectiveness of bank staff in implementing the bank's policies and procedures.
    - The effectiveness of compliance oversight and quality control, including parameters and criteria for automatic alerts; and
    - The effectiveness of the bank's training of relevant personnel.

- Expertise and Frequency: Senior management should ensure that audit functions are allocated staff that are knowledgeable and have the appropriate expertise. Audit scope, methodology, and frequency must be appropriate for the bank's risk profile.
- Proactive Review: Periodically, internal auditors should conduct AML/CFT/CPF audits on a bank-wide basis and be proactive in following up their findings and recommendations.

5.4 Internal Access to Information

An institution should ensure that its internal control, compliance, audit, and other oversight functions, particularly the MLRO, have full access to all information as needed.

5.5 Management of Information and Record-Keeping

5.5.1 Seven-Year Record Retention Rule

- Institutions should ensure that all information obtained in the context of CDD is recorded, including verifying documents and transcription into the institution's IT systems.
- Clear rules must be implemented regarding record maintenance, prescribed privacy measures, and data definitions.
- Retention Mandate: Records must be kept for at least seven years from the termination of the banking relationship or the execution of an occasional transaction.
- Litigation Hold: Where accounts are closed in the event of an ongoing investigation or litigation, all records must be retained until the official closure of the case.
- Adequate records documenting the evaluation process related to ongoing monitoring, review, and any conclusions drawn must be maintained to demonstrate compliance to regulators.

5.5.2 Maintenance and Supplying Information

- Updating Information: Institutions should ensure records remain accurate, up-to-date, and relevant by undertaking regular reviews of existing records and updating CDD info.
- Supervisory Access: Institutions must be able to demonstrate to supervisors, on request, the adequacy of their risk assessment, management, and mitigation frameworks; customer acceptance policies; CDD/EDD procedures; ongoing monitoring; and all reported STR details.

5.6 Assessment of ML/TF/PF Risks Associated with Virtual Assets

Institutions should assess their exposure to virtual assets and VASPs as part of their institutional risk assessment. This assessment should consider, at a minimum:

- Whether the institution's customers include VASPs or persons engaged in virtual asset activities, and the nature/volume of such activity.

- Whether the institution processes payments or transfers related to virtual asset exchanges, purchases, or redemptions.
- Whether virtual asset-related activity passes through correspondent banking relationships.
- The adequacy of AML/CFT/CPF controls applied by any VASP counterparty.
- The anonymity or pseudonymity features of the virtual assets concerned, including mixing or tumbling services; and
- The jurisdictional risk profile of the VASP, including whether it is subject to supervision equivalent to FATF standards.

5.7 Travel Rule[1] Compliance and Monitoring Typologies

- Travel Rule Enforcement: When institutions participate in virtual asset transfers, wire transfer obligations apply in full. Required originator and beneficiary information must be transmitted to the receiving VASP. Where technical limitations prevent full transmission, institutions should apply risk-based compensating controls, including enhanced monitoring.
- Configuration for Crypto Typologies: Transaction monitoring systems must be configured to identify payments to/from VASPs and transactions displaying crypto typologies. Scenarios include:
    - Multiple small-value transfers to or from exchange platforms that aggregate to a significant volume.
    - Transactions involving VASPs in jurisdictions with inadequate frameworks.
    - Customer activity correlating with virtual asset price movements or exchange activity inconsistent with profile; and
    - Transactions involving virtual asset mixing/tumbling services, privacy coins, or alternative anonymity mechanisms.
- Emerging Risks: Institutions should remain alert to the rapidly evolving landscape—including decentralized finance (DeFi) platforms, non-fungible tokens (NFTs) used as value transfers, and other innovations—updating systems as new typologies are identified by the FATF, CBK, or FRC.

---

[1] The changes to Recommendation 16 of the FATF standard, also referred to as the 'Travel Rule' in the context of virtual assets, were agreed by members at the FATF's June 2025 Plenary meeting. They will ensure consistency of information required in payment messages to build a clearer picture of who is sending and receiving money and help to eliminate fraud and error impacting customers. The changes to the Standards include:

- Clarifying responsibilities within the payment chain.
- Standardised information requirements.
- Requirements to introduce tools that protect against fraud and error.
- Clarification on card transactions.

(source: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html)

5.8 Proliferation Financing Risk Management

5.8.1 Institutional Risk Assessment Factors

Institutions shall include PF risk as a distinct, documented component of their institutional risk assessment, approved by senior management and reviewed at least annually. In conducting the assessment, institutions must consider:

- Customer Base: Importers, exporters, freight forwarders, shipping agents, trading companies, government procurement entities, or manufacturers dealing in goods with dual-use applications.
- Product Exposure: Trade finance products (Letters of Credit, documentary collections, bank guarantees, supply chain finance), correspondent banking services, or wire transfer services.
- Jurisdictional Exposure: Connections to the DPRK, Iran, or jurisdictions subject to PF UNSCRs, or those identified as having weak export controls or known procurement routes for WMD-related goods.
- Ownership Risk: Customers or beneficial owners connected to government entities or state-owned enterprises in jurisdictions subject to PF-related sanctions.
- Transactional Complexity: Processing involving multiple intermediaries, complex corporate structures, or payments inconsistent with the apparent scale of business.

5.9 Suspicious Transaction Reporting and Asset Freezing

5.9.1 Reporting Timelines and Internal Processes

- Ongoing monitoring must enable institutions to identify suspicious activity, eliminate false positives, and report promptly genuine suspicious transactions.
- Where there is suspicion that a transaction or activity relates to money laundering, terrorism financing, proliferation financing or the proceeds of crime, a reporting institution shall report the suspicious or unusual transaction or activity to the Centre in the specified manner within two days after the suspicion arose.
- Institution policies and procedures should:
    - Clearly specify the process for identifying, investigating, and reporting directly to the FRC, as well as mechanisms for managing targeted financial sanctions and escalating matters to the Counter Financing of Terrorism Inter-Ministerial Committee.
    - Contain a clear description for employees of their obligations and instructions for internal analysis, investigation, and guidance on how to complete reports.
    - Provide for methods to assess whether statutory obligations are always observed.
    - Reflect the strict principle of confidentiality; and
    - Ensure investigations are conducted swiftly and that reports contain relevant information produced in a timely manner.

- Once suspicion has been raised, institutions must take appropriate action to adequately mitigate the risk of the institution being used for criminal activities. This may include a review of the risk classification of the customer or the entire relationship itself.
- Appropriate action may necessitate escalation to the appropriate level of decision-maker to determine how to manage the relationship, considering factors such as cooperation with law enforcement agencies or the FRC.

5.10 Group-Wide and Cross-Border Compliance Contexts

5.10.1 Global Process for Managing Customer Risks

- Consolidated risk management means establishing and administering a process to coordinate and apply policies and procedures on a group-wide basis, implementing a consistent baseline across international operations. Policies should identify, monitor, and mitigate group-wide risks, not merely comply strictly with local laws.
- An institution should have robust information-sharing among the head office and all its branches and subsidiaries. Every effort should be made to ensure that the group's ability to obtain and review information is not impaired because of modifications to local policies necessitated by local legal requirements.
- Conflict of Laws: In cases where host jurisdiction requirements are stricter than the group's, group policy should allow the branch or subsidiary to adopt and implement the host jurisdiction's local requirements. Where the host country does not permit the proper implementation of those standards, the MLRO should inform the Central Bank. The Group should consider additional measures including, as appropriate, closing operations in that host country.
- Authorization: For effective group-wide monitoring, institutions should be authorized to share information about their customers, subject to adequate legal protection, with their head offices or parent bank, applying to both branches and subsidiaries.

5.10.2 Risk Assessment and Management at Group Level

- Institutions should have a thorough understanding of all risks associated with customers across the group, either individually or as a category, and should document and update these on a regular basis.
- In assessing customer risk, a bank should identify all relevant risk factors (e.g., geographical location, transaction activity patterns, product usage) and establish criteria for identifying higher-risk customers. These criteria should be applied across the bank, its branches, subsidiaries, and through outsourced activities.
- Customer risk assessments should be applied on a group-wide basis, while recognizing that customers in the same category may pose different risks in different jurisdictions.
- The information collected must be used to determine the level of overall group risk and support the design of group controls (e.g., tighter monitoring, more frequent data updating, or location visits).

- Compliance and internal audit staff, particularly the MLRO, or external auditors, should evaluate compliance with all aspects of group policies, centralized CDD effectiveness, and information-sharing requirements.
- Internationally active banking groups must ensure a strong internal audit and a global compliance function.
- The MLRO of the Banking group should include the responsibility for group-wide compliance with all relevant AML/CFT/CPF policies, procedures, and controls nationally and abroad.

5.10.3 Consolidated AML/CFT/CPF Policies and Procedures

- Introducer Reliance: A bank should understand the extent to which legislation allows it to rely on procedures undertaken by other institutions when business is being referred. A bank should not rely on introducers subject to standards less strict than its own, entailing monitoring of the referring bank's jurisdiction.
- Intra-Group Introducers: A bank may rely on an introducer part of the same financial group and consider placing a higher level of reliance on it, provided the introducer is subject to the same standards and supervised at the group level. The bank must ensure it obtains customer information from the referring bank to facilitate reporting to the FRC if needed.
- Consistency vs. Local Adjustments: Each subsidiary/branch should comply with minimum group policies, implementing consistent customer acceptance, CDD, and record-keeping with adjustments for business line or geographical variations. Local monitoring should be complemented by a robust process of information-sharing with the head office regarding heightened-risk accounts.
- Consolidated Scope: A bank should monitor significant customer relationships, balances, and activity on a consolidated basis, regardless of whether accounts are held on-balance sheet, off-balance sheet, as assets under management, or on a fiduciary basis.
- Centralized Database Processing: In implementing centralized processing systems, a bank should adequately document and integrate local and centralized transaction monitoring functions to ensure it can monitor for patterns of potential suspicious activity across the group and not just at isolated levels.

5.10.4 Specific Group Mandate of the MLRO

A bank performing business nationally and abroad should ensure that MLRO responsibilities extend to AML/CFT/CPF compliance for the whole group, including:

- Creating, coordinating, and performing a group-wide assessment of the implementation of a single AML/CFT/CPF strategy.
- Ensuring formulation and implementation of AML/CFT/CPF policies and procedures.
- Ongoing monitoring of the fulfilment of all AML/CFT/CPF requirements on a group-wide basis, nationally and abroad.

- Satisfying him/herself (including through on-site visits on a regular basis) that there is group-wide compliance; and
- Granting the Group MLRO the authority to issue directives or implement necessary measures for all national and international branches, subsidiaries, and subordinated entities.

5.10.5 Group-Wide Information-Sharing Arrangements

- Institutions should oversee the coordination of information-sharing. Subsidiaries and branches should proactively provide the head office with information concerning higher-risk customers and respond to requests in a timely manner.
- Group-wide standards should include descriptions of processes for identifying, monitoring, and investigating unusual circumstances, taking into account local data protection and privacy laws.
- The overall risk management function should evaluate risks posed by activity reported by branches and have policies to ascertain if other branches hold accounts for the same customer (including related or affiliated parties).
- Banks should have policies governing global account relationships deemed higher-risk, including escalation procedures and guidance on restricting or closing accounts.
- Head offices should be able to require all branches and subsidiaries to search files against specified lists of individuals or organisations suspected of aiding and abetting ML, TF, and PF, and report matches to supervisors, law enforcement, or FIUs.

5.10.6 Mixed Financial Groups

- Mixed financial groups (engaging in banking, securities, and insurance businesses) should have the ability to monitor and share information on customer identity and transactions across the entire group, remaining alert to customers utilizing services in different sectors.
- Differences in activities between sectors may justify variations in AML/CFT/CPF requirements. The group should be alert to these differences when cross-selling products and services, ensuring the appropriate sector-specific AML/CFT/CPF requirements are strictly applied.

5.11 Targeted Financial Sanctions

5.11.1 Applicable Sanctions Mandates

Compliance with TFS is non-discretionary and absolute. FIs should screen against and enforce the following regimes:

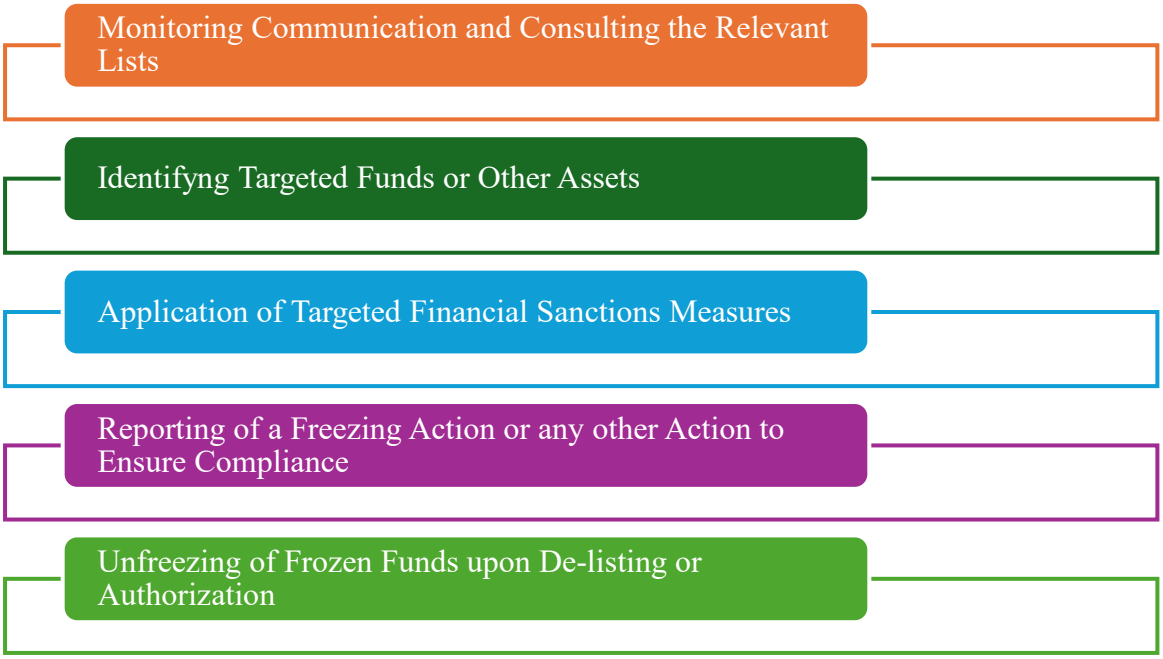
- UNSCR 1267 Series: Al-Qaeda / ISIL sanctions regime. Requires freezing of funds, travel bans, and arms embargoes against individuals listed by the UNSCR 1267/1989/2253 Committee. Screen against the UN Consolidated Sanctions List.
- UNSCR 1373: Counter-Terrorism sanctions. Requires freezing without delay the funds and assets of persons who commit, attempt, or facilitate terrorist acts.

Designations may be made domestically; institutions must screen against domestic designation lists published by Kenyan authorities.

- UNSCR 1718 and successor resolutions: requires institutions to monitor transactions and business relationships, on an on-going basis, against updated 1718 Sanctions list to mitigate proliferation financing risks.

5.11.2 Targeted Financial Sanctions Obligations of Reporting Institutions

Financial institutions are required to comply with targeted financial sanctions obligations to ensure compliance with relevant United Nations Security Council Resolutions on the prevention of terrorism, terrorism financing, proliferation of weapons of mass destruction and related financing. These obligations include:



5.11.3 Screening for TFS

- Institutions should implement automated screening systems capable of screening all customers, beneficial owners, and transactions against applicable sanctions lists in real time or as close to real time as practicable.
- Screening systems must be updated immediately following new designations.
- Screening should be done at least in the following circumstances:
    - Upon receipt of updates to the relevant UNSC sanctions list or Domestic List. In such cases screening must be conducted without delay to ensure compliance with implementing asset freezing measures;
    - During onboarding of new customers or before facilitating single or once-off transactions;
    - When customer information changes or is being updated; or
    - During processing of payments and value transfers, including wire transfers.

- The screening database must cover all customers and beneficial owners, not only new customers at onboarding.
- Systems must be calibrated to identify phonetic matches, aliases, transliterations, and alternative name variations.
- Algorithms must be tested and validated regularly to ensure matching capabilities function effectively.

5.11.4 Application of Targeted Financial Sanctions Measures

Targeted financial sanctions measures must be applied immediately upon identification of a sanctions target and must remain in force until the person or entity is removed from the relevant United Nations Security Council sanctions list or domestic list. No legal action shall be taken against any person or entity, including reporting institutions, for the good-faith execution or enforcement of an order designating a person or freezing the funds or other assets of a designated entity under the POT-TFR and POT-PFR.

5.11.5 Freezing of Funds or Other Assets Without Delay and Without Prior Notice

Financial institutions should freeze, without delay and without prior notice, the funds or other assets of designated persons and entities.

The funds, property, or other assets to be frozen include:

- all funds or other assets owned or controlled by a designated person or entity, including assets not linked to a specific terrorist act, plot, or threat;
- funds or other assets wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities;
- funds or other assets derived or generated from assets owned or controlled, directly or indirectly, by designated persons or entities; and
- funds or other assets of persons or entities acting on behalf of, or at the direction of, designated persons or entities.
- No frozen funds or other assets may be released to a designated person or entity without authorisation from the Committee.

5.11.6 Prohibition on Making Funds, Assets, Economic Resources, or Related Services Available

No person or entity may make funds, assets, economic resources, or financial or other related services available, directly or indirectly, wholly or jointly, for the benefit of designated persons or entities. This prohibition also applies to entities owned or controlled, directly or indirectly, by designated persons or entities, and to persons or entities acting on their behalf or at their direction, unless licensed, authorized, or otherwise notified in accordance with the relevant United Nations Security Council resolution.

5.11.7 Reporting Obligation

Within 24 hours of taking freezing action, the person who effected the freeze must submit a report to the Committee through the Secretary via:

Email: *tfs@frc.go.ke*

A reporting institution must use the prescribed reporting template and specify the assets frozen, or actions taken, including any attempted dealings with property or funds subject to the freezing action.

In the broader context of countering the financing of terrorism and proliferation financing, a reporting institution must also submit a suspicious transaction or activity report in accordance with section 44 of the Proceeds of Crime and Anti-Money Laundering Act (Cap. 59A), where applicable.

5.11.8 Unfreezing Obligation

Persons or entities holding targeted funds or other assets must immediately unfreeze them in the following circumstances:

- where funds or other assets were inadvertently or mistakenly frozen due to name similarity with a designated person or entity on a domestic list, after:
  - confirmation that the name is not a target match and approval is obtained from the Committee; or
  - the Committee approves an application confirming that the person or entity is not the designated person or entity and communicates its decision.
- upon receipt of a notification and directive from the Committee concerning a bona fide third-party claim to frozen funds or assets, following approval of the application by the Committee;
- upon de-listing of a designated person or entity by the relevant United Nations Security Council Sanctions Committee or the Counter Financing of Terrorism Inter-Ministerial Committee, once the Committee circulates the de-listing notification; or
- where the Committee authorizes access to frozen funds or other assets under the domestic listing framework and provides clear guidance to facilitate access for:
  - necessary basic expenses, including rent or mortgage payments, food, monthly family expenses, medicines and medical treatment, taxes, insurance premiums, and public utility charges;
  - reasonable professional fees or reimbursement of expenses incurred for legal services;
  - fees or service charges for the routine holding or maintenance of frozen funds, financial assets, or economic resources; and
  - extraordinary expenses, provided the request is assessed by the Committee and, if favourably considered, forwarded to the relevant Sanctions Committee for approval.

Annex I: Guidance on Conducting ML/TF/PF Risk Assessments

A. Introduction

Regulation 7 of the POCML Regulations requires financial institutions to conduct a risk assessment to identify, assess, understand, monitor, manage and mitigate the money laundering, terrorism financing and proliferation financing risks associated with their activities.

The assessment should consider the institution's inherent ML/TF/PF risks, the strength of its control environment and any additional measures required to manage residual risk.

B. Purpose and Scope

This Guidance Note is intended to assist financial institutions in conducting ML/TF/PF risk assessments. In particular, it supports institutions in ensuring that their risk assessments:

The risk assessment should follow a documented methodology that moves from risk identification to inherent risk assessment, control effectiveness assessment, residual risk determination, reporting, remediation and periodic review. This sequence supports a risk-based approach by linking identified ML/TF/PF risks to proportionate controls, governance oversight and measurable follow-up actions.

- comply with Kenya's AML/CFT/CPF legal and regulatory framework;
- align with international standards, including the FATF Recommendations and Basel Core Principles;
- are sufficiently robust to support a risk-based approach to managing ML/TF/PF risks;
- take account of risks relating to products, services, delivery channels, customers, business relationships, geography and other relevant factors; and
- support the implementation of effective mitigation measures and ongoing monitoring of ML/TF/PF risks that reporting entities may face in their activities and business relationships.

C. Accountability and Stakeholders

Board of Directors

The board should understand the money laundering, terrorism financing and proliferation financing threats and vulnerabilities facing the institution. It should also ensure that the institution adopts a risk-based approach to managing ML/TF/PF risks.

The board's responsibilities include:

- ensuring that a documented ML/TF/PF risk assessment framework is developed;
- reviewing the outcomes of the risk assessment process;
- understanding the institution's ML/TF/PF risk profile;
- allocating adequate resources for the assessment;
- approving strategic decisions proposed by management following the assessment; and
- ensuring that all relevant departments and functions participate in the process.

Senior Management

Senior management should ensure that the institution's activities remain consistent with the business strategy, risk appetite and policies approved by the board. Senior management should:

- implement the board-approved ML/TF/PF risk assessment framework;
- continuously improve the collection and analysis of data used in the assessment;
- provide periodic reports on the institution's ML/TF/PF risk assessment;
- ensure that actions arising from gaps or deficiencies are implemented;
- clearly assign roles and responsibilities for the assessment process;
- ensure that results are shared with all relevant parties; and
- ensure that a copy of the risk assessment is submitted to the Central Bank of Kenya, where required.

Money Laundering Reporting Officer

The Money Laundering Reporting Officer should coordinate and support the risk assessment process. Key responsibilities include:

- coordinating the ML/TF/PF risk assessment process;
- collating and verifying input, data and comments from relevant departments;
- analysing data to understand identified risks;
- engaging business units during the assessment;
- determining residual risk across relevant categories;
- determining the institution's overall AML/CFT/CPF risk profile; and
- preparing reports for senior management and the board.

Business Units

Ownership and management of the risk assessment process may depend on how the assessment is structured, including whether it is conducted by business line, country or region. The institution's structure, footprint and complexity should inform this decision.

Although the MLRO, Compliance Officer or dedicated Risk Officer may coordinate the assessment, business-line heads and other first-line employees should be actively engaged. They are often best placed to provide detailed insight into ML/TF/PF risks and to supply customer and transactional data.

Front-line engagement is essential because business units retain ownership of ML/TF/PF risks and are responsible for implementing actions arising from gaps or weaknesses identified during the assessment.

Control Functions

An ML/TF/PF risk assessment should involve both business functions and control functions, including Internal Audit, Risk Management and, where applicable, External Audit. Management should ensure that the risk assessment process and results are subject to independent review. Where a control function undertakes part of the assessment, its

role should be clearly set out in the risk assessment framework. Reports from any independent review should be shared with senior management and the board.

D. Conducting a Risk-Based Institutional Risk Assessment

A risk assessment enables a financial institution to identify, assess and understand the ML/TF/PF risks that may arise from its business activities and customer relationships. At a minimum, the assessment should consider:

- the institution's customers and their characteristics;
- products and services offered;
- delivery channels and transaction-related risks;
- geographic locations and markets; and
- other relevant qualitative factors.

The risk-based approach is the overall framework for managing ML/TF/PF risk. The ML/TF/PF risk assessment is a specific component of that framework and provides the evidence base for proportionate controls.

The institution should take account of relevant national, sectoral and supervisory risk assessments when identifying and assessing ML/TF/PF risks. Where the institution's assessment differs from those external sources, the rationale should be documented.

A risk assessment should identify the institution's inherent ML/TF/PF risks based on its characteristics, business model and activities; evaluate the design and operational effectiveness of the control framework; and determine the residual risk that remains after controls are applied.

The results should inform the development, implementation, monitoring and periodic updating of the institution's risk-based control framework. The assessment does not need to be complex, but it should be proportionate to the nature, size and complexity of the institution's operations.

Smaller or less complex institutions may use simpler assessments, particularly where they serve similar customer categories or operate within a limited jurisdiction or service range.

More complex institutions—such as those serving diverse customer segments, offering multiple services or operating across several jurisdictions—should adopt more sophisticated assessments that reflect their risk profile.

For example, smaller institutions may use standardized risk matrices or checklists, while larger institutions may require detailed risk models and analysis. All institutions may consider using data analytics and artificial intelligence to improve the accuracy and efficiency of their assessments, where appropriate.

Where an institution uses automated scoring, data analytics or artificial intelligence in the assessment, it should ensure that the methodology is explainable, periodically validated, subject to appropriate governance and supported by reliable data. Limitations, assumptions and overrides should be documented.

D.1 Purpose of the ML/TF/PF Risk Assessment

The primary purpose of an ML/TF/PF risk assessment is to strengthen institutional risk management by identifying the risks the institution faces, assessing how those risks are mitigated by AML/CFT/CPF controls and determining the residual risk that remains.

The results of the assessment may be used to:

- identify gaps and opportunities to improve AML/CFT/CPF policies, procedures, processes, systems and controls;
- develop a risk appetite statement that reflects the institution's ML/TF/PF risk tolerance and supports risk-based resource allocation;
- assess whether business-unit compliance programmes align with their risk profiles;
- reduce residual risk through effective mitigation strategies or by limiting exposure to risks that cannot be adequately managed;
- inform senior management of key risks, control gaps and remediation efforts;
- enhance regulatory compliance and reporting;
- support strategic decisions on customer exits, account restrictions or other risk-reduction measures; and
- inform supervisors about key risks, control gaps and remediation efforts across the institution.

D.2 Characteristics of an Effective Risk Assessment Methodology

To implement an effective ML/TF/PF risk assessment, a financial institution should establish a methodology that:

- documents each step of the assessment process and the rationale supporting the risk assessment;
- describes the risk factors assessed, the quantitative and qualitative data evaluated, the stakeholders involved, the scoring criteria, weightings and any scoring overrides applied;
- integrates relevant external information, including national and sectoral risk assessments, FATF public statements, typologies, industry reports, law enforcement information and supervisory feedback;
- allows risks to be assessed by business unit, business line, activity or legal entity, where appropriate;
- yields separate risk ratings for ML, TF and PF, where the institution's methodology supports separate assessment of those risks;
- is reviewed and updated regularly to reflect changes in risks, regulatory expectations and technology;
- defines the assessment units in scope and the approach for applying data, risk factors, scoring and weightings across those units;

- ensures that data-driven, weighted or analytics-based methodologies meet applicable standards for risk management models; and
- is subject to appropriate internal review and approval by senior management and the board.

D.3 Granularity and Level of Detail

Financial institutions may organize their ML/TF/PF risk assessments in different ways depending on their size, legal form and complexity. Assessments may be conducted across business lines, legal entities or other assessment units and then consolidated into an enterprise-level assessment.

Where practical, institutions should adopt standardized methodologies across assessment units while retaining sufficient flexibility to tailor the assessment to the risks of each unit.

For example, a larger institution may conduct a global ML/TF/PF risk assessment supported by regional or country-level assessments.

Larger institutions should ensure that assessments are tailored to the relevant business line and that the data used is relevant, validated and subject to assurance checks.

Regardless of the approach adopted, assessment results should be aggregated into an enterprise-level view of inherent risk, mitigating controls and residual risk.

D.4 Frequency of the ML/TF/PF Risk Assessment

An institution should update its ML/TF/PF risk assessment at least every two years and whenever material trigger events occur, including significant changes to its products, services, customers, delivery channels, geographic exposure, ownership structure, technology, regulatory obligations or external threat environment.

Trigger-event updates help ensure that the assessment continues to reflect the institution's current ML/TF/PF risks and control environment.

D.5 Principles and Best Practices for Institutional Risk Assessments

General Guidance on Institutional ML/TF/PF Risk Assessments

Methodology. Financial institutions should design and implement an ML/TF/PF risk assessment methodology that is proportionate to their size, nature, complexity, business model and risk profile. While methodologies may differ across institutions, each institution should ensure that its assessment is evidence-based, consistently applied, adequately documented and capable of supporting a risk-based AML/CFT/CPF compliance programme.

Data quality. Institutions should conduct appropriate data quality and assurance checks on data used in the risk assessment. Where data is incomplete, inaccurate or inconsistent, the institution should document the limitation, apply reasonable validation or remediation measures and consider the impact of the data issue on the assessment outcome. The risk

assessment process should not be used as a substitute for correcting underlying data quality deficiencies.

Quantitative and qualitative analysis. Institutions should use both quantitative metrics and qualitative judgement to support the assessment. Quantitative indicators may include customer volumes, transaction values, product usage, geographic exposure, alert trends, suspicious transaction reporting, control testing results and other relevant data. Qualitative judgement should be documented and supported by a clear rationale.

Working papers and evidence. Institutions should retain working papers, data extracts, scoring tools, assumptions, approvals and other records used to prepare the assessment. These records should be sufficient to allow senior management, the board, supervisors or independent reviewers to understand how the assessment was performed and how conclusions were reached.

Assessment report. Institutions should prepare a final enterprise-level ML/TF/PF risk assessment report that sets out inherent risks, control effectiveness, residual risks, key observations, supporting data and required remedial actions. Where assessments are conducted at branch, business-line, regional or legal-entity level, the results should be consolidated into an enterprise-wide view.

Policies and governance documentation. Institutions should document the governance arrangements for the risk assessment, including ownership, roles and responsibilities, approval requirements, frequency of review, escalation procedures and processes for tracking actions arising from control weaknesses or heightened residual risk.

Third-party support. Where an institution engages a consultant or other third party to support the assessment, the institution remains responsible for the methodology, quality, conclusions and outcomes of the assessment. The institution should maintain effective oversight of the engagement and avoid undue reliance on external parties.

D.6 How to Conduct the Risk Assessment

An institutional ML/TF/PF risk assessment typically involves three core steps:

- Assess inherent risk: identify and assess the ML/TF/PF risks inherent in the institution’s business model and activities, including customer, product, service, delivery channel, geographic and operating-structure risks.
- Assess the control environment: evaluate the design and operational effectiveness of policies, procedures, systems and other controls used to mitigate inherent risks.
- Determine residual risk: assess the risk that remains after controls are applied to inherent risk.

1. Inherent Risk	→	2. Control Environment	→	3. Residual Risk
Identify ML/TF/PF risks across customers, products, channels, geography and operations.		Evaluate policies, procedures, systems and controls that mitigate risk.		Assess remaining risk after controls are applied.

Stage 1: Identifying and assessing inherent risk

Identifying Inherent Risk

Customer Risk

Customer risk should be assessed based on the characteristics of the institution's customer base, including customer type, legal form, ownership and control structure, industry or occupation, expected activity, risk rating, beneficial ownership and related-party exposure. Institutions should consider whether any customer segment presents elevated ML/TF/PF risk.

- customers operating in unusual circumstances, including unexplained geographic distance from the institution or unexplained movement of accounts or funds across institutions or jurisdictions;
- customers with complex, opaque or unusual ownership or control structures;
- foreign financial institutions and money or value transfer service providers;
- non-bank financial institutions and other regulated or high-risk sectors;
- politically exposed persons, including their family members and close associates;
- foreign individuals, foreign legal persons, offshore entities and shell companies;
- cash-intensive businesses;
- non-governmental organisations, charities and non-profit organisations; and
- professional service providers and other intermediaries acting on behalf of customers.

Institutions should maintain a customer-risk assessment worksheet or equivalent tool that records, at a minimum, the customer type, inherent risk rating, rationale, relevant mitigating controls, score or weighting and residual risk rating.

Product and Service Risk

Institutions should assess the ML/TF/PF risks associated with each product and service offered. The assessment should consider how the product or service may be used, misused or abused, including whether it enables anonymity, rapid movement of funds, complex transactions or cross-border activity.

- use of cash, virtual assets, precious metals, precious stones or other higher-risk media of exchange;
- cross-border transfers or multi-currency activity;

- products or services involving intermediaries, agents, third parties or reliance on another institution's customer information;
- features that may permit anonymity, limited transparency, pooling or obfuscation of funds;
- complex structures or transactions that lack a clear economic or lawful purpose;
- products or services using emerging technologies or financial innovations; and
- near-instantaneous, irreversible or difficult-to-recall settlement or processing.

Delivery Channel Risk

Institutions should assess the ML/TF/PF risks arising from the channels through which customers are onboarded, serviced and able to transact. Delivery channels may include branches, agents, intermediaries, digital channels, mobile platforms, internet banking, correspondent relationships and other third-party arrangements.

Higher delivery channel risk may arise where customers are onboarded or serviced on a non-face-to-face basis, where third parties are involved, where verification is remote or automated, or where the institution has limited visibility over the customer, transaction or source of funds. Institutions should assess the extent to which these channels increase inherent ML/TF/PF risk and whether controls are adequate to mitigate that risk.

Geographic Risk

Geographic risk arises from the institution's exposure to jurisdictions or regions that present elevated ML/TF/PF risk. This exposure may arise from the institution's operating locations, branches, affiliates, customer base, counterparties, source or destination of funds, transaction corridors or cross-border business relationships.

Assessing Inherent Risk

Institutions should measure inherent risk as the level of ML/TF/PF risk that exists before the application of mitigating controls. The methodology used should be appropriate to the institution's business model, risk profile and available data.

Institutions should analyse both quantitative and qualitative information when assessing inherent risk. Quantitative data should be reliable, relevant and sufficiently current. Qualitative judgement should be clearly explained and supported by evidence.

There is no single prescribed model for assessing risk. Institutions may assess risk using likelihood, impact, vulnerability, threat, consequence, uncertainty or other appropriate measures. Regardless of the approach used, the institution should be able to explain the methodology and demonstrate that it is reasonable, proportionate and consistently applied.

Examples of acceptable approaches include:

- assessing the likelihood of an ML/TF/PF event occurring;
- assessing both likelihood and potential impact;
- considering the interaction between threat, vulnerability and consequence; or

- assessing how uncertainty may affect the institution's exposure to risk.

The institution should document the basis for its risk determinations, including the evidence, assumptions, data sources, weighting decisions and expert judgement used. The methodology should be capable of review by senior management, the board, supervisors and independent assurance functions.

Weighting of Risk Factors

Institutions may weight risk factors differently to reflect their relative importance to the overall risk assessment. The weighting applied to each factor should be appropriate to the institution's business model, risk profile and exposure. Weightings should be documented and periodically reviewed.

Institutions should select a risk-rating scale, define the parameters for each rating and establish clear criteria for scores, weightings and overrides. Any manual override should be supported by documented rationale and appropriate approval.

Stage 2: Assessing the AML/CFT/CPF Control Environment

After assessing inherent risk, institutions should evaluate the design and operating effectiveness of controls intended to mitigate identified ML/TF/PF risks. Controls may include governance and oversight arrangements, policies and procedures, customer due diligence, enhanced due diligence, transaction monitoring, sanctions screening, suspicious transaction reporting, recordkeeping, training, independent testing and audit.

Institutions should assess both whether controls are appropriately designed and whether they operate effectively in practice. The assessment may include business-unit self-assessments, compliance testing, audit findings, quality assurance reviews, management information, supervisory feedback and other relevant evidence.

Evidence used to assess control effectiveness may include policy approvals, customer due diligence files, enhanced due diligence records, screening and monitoring alerts, suspicious transaction reports, quality assurance results, compliance testing, audit findings, training records, management information and remediation tracking.

Control effectiveness ratings should be defined in advance and applied consistently. For example, controls may be rated as effective, partially effective, needs improvement or deficient. The institution should explain how individual control ratings are combined to determine the overall effectiveness of the control environment.

Stage 3: Determining Residual Risk

Institutions should determine residual risk after considering inherent risk and the effectiveness of mitigating controls. Residual risk represents the level of ML/TF/PF risk that remains after controls are applied.

The residual risk rating should be compared with the institution's approved ML/TF/PF risk appetite. Where residual risk exceeds appetite, management should determine whether to accept the risk with justification, strengthen controls, restrict activity, exit relationships or take other risk-reduction measures.

The residual risk assessment should inform management decisions, including risk acceptance, remediation, enhanced controls, resource allocation, customer exits, product restrictions or other risk-reduction measures. Where residual risk is higher than expected or exceeds the institution's risk appetite, the institution should document the reasons and implement appropriate corrective action. Previous assessments should be retained to demonstrate how inherent risk, control effectiveness and residual risk have evolved over time.

E. Reporting and Use of Results

Reporting to Senior Management and the Board

The results of the ML/TF/PF risk assessment should be presented to senior management and the board. The report should clearly set out the institution's inherent risk, control effectiveness, residual risk, key vulnerabilities, required actions, responsible owners and implementation timelines.

The report may present results by business line, branch, product, service, customer type, geography, delivery channel, legal entity or any other relevant assessment unit. Reporting should not rely only on averaged or aggregated results; it should identify where higher inherent risk, weaker controls or elevated residual risk arise within the institution.

The report should include clear action points to address identified weaknesses. Actions should be prioritised according to risk, assigned to accountable owners and tracked to completion.

Reporting to the Central Bank of Kenya

Institutions should submit to the Central Bank of Kenya, where required, the latest results of their ML/TF/PF institutional risk assessment on an annual basis and within the timelines prescribed by the Central Bank of Kenya. The submission should provide a clear summary of inherent risk, mitigating controls, residual risk, key findings and actions being taken to address identified weaknesses.

Key Regulatory References

i. Prevention of Terrorism Act (POTA) and Regulations.
ii. Proceeds of Crime and Anti-Money Laundering Act (POCAMLA) and Regulations.
iii. Financial Action Task Force Recommendations.
iv. Basel Committee on Banking Supervision - Core Principles for Effective Banking Supervision.
v. Basel Sound Management of Risks Related to Money Laundering and Financing of Terrorism.
vi. Central Bank of Kenya (CBK) Prudential Guidelines.
vii. Guidance notes issued by CBK on AML/CFT/CPF matters.
viii. Financial Reporting Centre (FRC) Guidelines.
ix. United Nations Security Council Resolutions (UNSCRs).

13.0 THIRD-PARTY RISK MANAGEMENT GUIDELINE

1.0 Introduction

Third-party risk refers to the risks to a financial institution's earnings and operational resilience arising from business and strategic arrangements with external entities that perform activities, functions, or services on its behalf.

Third-party arrangements can significantly enhance an institution's operational efficiency, promote innovation, and optimize cost structures. However, they also introduce systemic vulnerabilities, introduce third-party risks, and alter the risk profile of the participating bank.

2.0 Materiality assessment

Institutions shall establish an approved policy that should document how it will conduct an assessment of material services. Every prospective third-party relationship must undergo a rigorous materiality assessment prior to contract execution. This assessment must be repeated during contract renewals or whenever the scope of the vendor's service expands significantly.

To determine whether an arrangement is material/critical, institutions must evaluate the following dimensions:

- Criticality of the function: Whether the service directly powers a core banking function, payment gateway, treasury channel, or customer-facing digital app.
- Operational disruption and recovery: The immediate operational impact if the service provider suffers a prolonged 48-hour outage.
- Data complexity and sensitivity: Whether the vendor will access, process, transmit, or store customer personal information, regulatory logs, or proprietary financial algorithmic models.
- Financial and capital implications: The projected direct financial loss, operational risk capital charge increase, and potential customer restitution expenses in the event of vendor failure or malicious fraud.
- Regulatory compliance: The potential that a vendor's actions or failures could cause the bank to violate anti-money laundering protocols, consumer protection frameworks, or any other regulation.Sub-outsourcing Dependency: The extent to which the third party relies on a web of complex sub-contractors to deliver their core service to the institution.

3.0 Board and Senior Management Oversight

3.1 Responsibilities for the Board

The board of directors holds the ultimate responsibility for the management of third-party risk and holding senior management accountable for implementation of the risk-management framework. In this regard, the board will undertake the following responsibilities:

a) Approving a framework to evaluate the risks and materiality of all existing and prospective third-party service provider arrangements and the policies that apply to such arrangements;
b) Laying down appropriate approval authorities for third-party service provider arrangements depending on risks and materiality;
c) Undertaking regular review of third-party service provider arrangements and strategies for their continued relevance, safety and soundness;
d) Deciding on business activities of a material nature to be provided by third-party service providers, and approving such arrangements;
e) Establishing a comprehensive third-party service provider arrangements risk management programme to address third party arrangements and the relationship with the service providers;
f) Assessing how the third-party service arrangements will support the institutions' objectives and strategic plan; and
g) Assessing management competencies for developing sound and responsive third-party service arrangements management policies and procedures as commensurate with the nature, scope and complexity of the arrangements.

3.2 Senior management responsibilities

In ensuring effective third-party risk management within an institution, senior management should, among other things: –

a) Ensure communication of the Institution's third-party strategy and policy to all relevant stakeholders, including Institution personnel and intragroup entities.
b) Implement policies and procedures clearly define roles and responsibilities to manage TPSP arrangements throughout the third-party arrangement life cycle.
c) Ensure that roles and responsibilities of all staff are appropriately defined, including those related to third-party service arrangements and based on risk and complexity, establish a central function to monitor all third-party service arrangements.
d) Evaluate the risks and materiality of all existing and prospective third-party service arrangements, based on the framework approved by the board;
e) Develop and implement sound and prudent third-party service policies and procedures commensurate with the nature, scope and complexity of the outsourcing;

f) Review periodically the effectiveness of policies and procedures;
g) Providing regular reports to the board on the institution's third-party risk strategy and implementation in a timely manner;
h) Ensuring that contingency plans are in place and tested, including availability of alternative service providers, based on realistic and probable disruptive scenarios;
i) Undertaking periodic review of third-party service arrangements to identify new material outsourcing risks as they arise;
j) Ensuring that there is independent review and audit for compliance with set policies regarding third-party service arrangements.
k) Ensuring that the internal audit function has the authority to assess and audit any outsourced functions;
l) Ensuring that regulatory requirements on third-party service arrangements are complied with at all times.

4.0 Policies and Procedures and Limits

Institutions shall establish and maintain comprehensive, Board-approved policies, procedures, and limits governing the management of third-party risks. The policies, procedures and limits to be established should ensure the objective evaluation of and responsiveness to an institution's business environment.

Policies on third-party arrangements are important in defining the services that the institution will procure from third parties. There should be clear guidelines on frequency and procedure for review of the institution's third-party service arrangement's strategy.

Institutions shall implement comprehensive and well-documented procedures to operationalize the third-party risk management policy across the entire lifecycle of third-party arrangements, including onboarding, monitoring, review, and termination.

As part of these procedures, institutions shall ensure that third-party engagements are aligned with the institution's overall business strategy and risk profile. In this regard, institutions shall establish processes to periodically evaluate the strategic rationale for outsourcing arrangements, taking into account the following factors:

- The institution's core competencies and inherent strengths, and whether the outsourced function supports or enhances these capabilities.
- The institution's identified weaknesses or resource constraints, and whether outsourcing appropriately mitigates such limitations.
- External opportunities, including access to specialized expertise, technology, or efficiencies that may improve service delivery and competitiveness.
- External risks and threats, including operational, legal, regulatory, technological, and market risks that may arise from reliance on third-party service providers.

Institutions shall ensure that such assessments are conducted at the pre-engagement stage and on a periodic basis, and that the outcomes are formally documented and integrated into decision-making processes. Institutions should establish quantitative and qualitative limits to manage third-party risk exposures as follows:-

a) Institutions should set limits on exposure to a single service provider as well as reduce dependence on a single provider.
b) Institutions should limit outsourcing of critical functions and ensure that adequate contingency arrangements and alternative providers are available.
c) Define thresholds for acceptable levels of operational risk exposure, Data risk exposure and Reputational risk exposure.
d) Clearly define authority levels for approval of third-party arrangements and material outsourcing arrangements.
e) Institutions should restrict uncontrolled sub-outsourcing and require prior approval before a third party can subcontracting critical services.

5.0 Risk Management Cycle

Effective third-party service risk management generally follows the stages of the life cycle. Controls should be designed proportionally to the risks and criticality of each third-party service arrangements. The stages of the life cycle typically include risk assessment, due diligence, contracting, onboarding, ongoing monitoring, and termination. The bank's governance, risk management and strategy are integral to each stage of the life cycle.

5.1 Risk identification

Banks should perform a comprehensive risk identification and assessment under the third-party service risk management framework to evaluate and manage identified and potential risks before entering into and throughout the life cycle of a third-party service arrangement.

The risk identification process should at minimum include the review of these core risks:

a) **Operational and Cyber Risk:** Systemic hardware or software failures, communication network drops, physical or logical security breaches, distributed denial-of-service (DDoS) attacks, ransomware injections, and cascading downtime across the vendor's secondary service infrastructure.

b) **Data Privacy, Security, and Cross-Border Exposure:** Unauthorized interception, structural leakage, or malicious infiltration of sensitive bank records or client personal data. This requires identifying exactly where data is stored "at rest" and how it is protected "in transit."

c) **Legal, Compliance, and Regulatory Risk:** The risk that the third party fails to comply with domestic banking regulations, consumer protection laws, data privacy

frameworks, or labor standards—resulting in the bank facing secondary regulatory sanctions, structural litigation, or contract enforceability failures.

d) **Reputational Risk:** Public backlash, loss of deposit holder confidence, or systemic brand degradation resulting from visible vendor operational failures, data breaches, public scandals, or unethical corporate behavior by the third-party entity.

e) **Systemic Concentration Risk:** Dual-layered vulnerabilities arising from:

- *Intra-Bank Concentration:* Relying on a single vendor for multiple disparate business operations.
- *Inter-Bank/Sectoral Concentration:* Relying on a market-dominant vendor that simultaneously supports multiple major commercial banks, creating a systemic single point of failure for the entire national financial infrastructure.

f) **Strategic and Lock-In Risk:** Financial burden or loss of competitive agility resulting from restrictive vendor contracts, excessive termination costs, unfeasible technology integration hurdles, or business alignment deviations where the provider's long-term corporate roadmap shifts away from the bank's needs.

g) **Conflict of Interest Risk:** Governance vulnerabilities introduced when an outsourced entity maintains dual, conflicting roles.

Banks should perform risk assessments on a regular basis and whenever there are major changes impacting the arrangement and maintain a documented risk-scoring matrix that evaluates the Inherent Risk of the service and the effectiveness control of the vendor to arrive at a Residual Risk Rating. The assigned Residual Risk Rating should inform required internal approval thresholds (e.g., High risk requires full Board approval).

5.2 Due diligence

Banks should have an appropriate and proportionate process for selecting and assessing the prospective third-party service provider before entering into a third-party service arrangement. The risk associated with a specific third-party service provider could affect the overall risk assessment of a bank’s existing third-party service arrangements profile. Institutions must at minimum review the following factors:

- **Financial solvency and viability:** Review of financial statements, capital structure metrics, credit ratings, and liquidity indicators to ensure the vendor will not face financial distress during the contract term.
- **Technical and Cybersecurity Resilience:** Review of the provider's information security policies, vulnerability scanning frequencies, encryption deployment, patch management protocols, and evaluating independent third-party assurance certificates.
- **Operational Capacity and Business Continuity:** Evaluation of the vendor's physical data centers, technology redundancy, disaster recovery location distances, maximum

historical uptimes, and verifying documentation of their latest successful full-scale business continuity failover test.

- **Jurisdictional and Cross-Border Risk Profile:** Where a vendor utilizes cloud infrastructure or operations located outside Kenya, the bank must formally evaluate the destination country's geopolitical risk, data localization laws, judicial independence, and verify whether foreign law enforcement can seize bank data without the explicit knowledge or consent of the domestic regulator.

5.3 Contracting

The contract stage of the life cycle occurs when the terms and conditions of the delivery of services are agreed upon. Contracts must clearly define roles, responsibilities, and safeguards to support risk management and regulatory compliance. The nature and detail of contracts should be appropriate to the institution and the criticality of service. Further:-

a) All third-party arrangements must be documented in a legally binding, enforceable written contract. The contracts must at minimum incorporate the following clauses:

   - A precise definition of the services provided, processing boundaries, and comprehensive Service Level Agreements (SLA) detailing measurable performance indicators (e.g., system availability percentages, transaction processing latency caps, error rate tolerances).
   - Explicit remedies and escalating financial penalties triggered automatically by vendor SLA failures or extended downtime windows.
   - Explicit, non-revocable clauses granting unconditional, timely access to all systems, premises, records, and personnel for information gathering, physical inspections, and independent testing by the Institution's internal and external auditors and the Central Bank of Kenya.
   - Legal mandates binding the vendor to confidentiality, prohibiting the monetization or unauthorized secondary aggregation of bank data, and requiring compliance with domestic data protection regulations.
   - A contract clause prohibiting the vendor from sub-outsourcing or subcontracting any material portion of their service to a fourth party without receiving the prior, explicit written consent of the bank's Senior Management. The primary vendor remains fully liable for the actions and control environment of any approved subcontractors.

b) Institutions should prevent structural self-review risks. Any professional firm or vendor engaged to perform an independent assurance role, governance audit, or specialized assessment should not provide concurrent non-audit services that could compromise their analytical objectivity or introduce conflicts of interest.

5.4 Monitoring

- Banks should, on an ongoing basis, assess and monitor the performance and changes in the risks and criticality of third-party service arrangements and report accordingly to the board and senior management.
- Ongoing monitoring should be aligned with banks' governance, risk management and strategy and the risks considered when the third-party service provider was selected. Any new risks that have emerged since onboarding and contractual obligations of the third-party service providers should also be considered
- Monitoring should include performance-related metrics, such as ongoing key performance indicators and scorecards in line with banks' policies and procedures.
- Banks should keep updated registers of all third-party arrangements reflecting their risks and criticality. Banks should leverage this information to identify and monitor bank-level concentration risk at a frequency commensurate with the changes to the operating environment.
- In arrangements involving shared responsibility, banks should monitor third-party service providers performance and operational implementation to ensure that obligations and responsibilities are clearly understood and fulfilled by the providers. Banks should also monitor their internal control environment and processes to meet their obligations and responsibilities.
- Third-party providers managing critical or material operations must integrate their Disaster Recovery Plans (DRPs) with the bank's own internal BCP frameworks. The bank must participate in or demand documented proof of annual, active, full-scale scenario testing to validate the vendor's recovery time objectives (RTO) and recovery point objectives (RPO).

5.5 Exit Strategies and termination Management

Institutions must document, and maintain a custom, comprehensive Exit Strategy for every material arrangement. The exit strategy must be actionable and distinct, accounting for two primary termination environments:

- **Planned Exit:** Orderly termination at the end of a contract term or a planned migration to a new platform due to strategic corporate shifts.
- **Unplanned Exit:** Sudden, rapid termination forced by a catastrophic vendor event, such as a major data leak, immediate corporate insolvency, regulatory enforcement action against the provider, or a severe, unresolved breach of contractual SLAs.

The exit plan must detail the exact operational roadmap required to ensure the absolute continuity of the bank's critical services during the transition phase. The plan should at minimum define:

- The technological and operational steps required to seamlessly transfer all data, historical logs, and front-end channels to a pre-vetted alternative service provider, or
- The specific timeline, headcount, and infrastructure requirements necessary to safely re-integrate the function back into the bank's internal IT and operational environment without causing system downtime, transaction processing delays, or customer friction.
- Upon the termination or expiration of a third-party contract, the exit plan must execute a formal, legally binding data clawback.
- The vendor must be contractually and operationally obligated to securely return and transfer all bank data, database records, master files, and user logs back to the institution in a standardized, usable format.
- Following verified data transfer, the vendor must execute an absolute purging, of all copies and backups of the bank's data across its primary servers, cloud environments, and physical backup systems.

6.0 Internal controls

Institutions need strong internal control systems to ensure that they are not unduly exposed to third-party risks.

6.1 Risk Management and Compliance functions

The Second line shall remain structurally independent from daily procurement and operational vendor management, and is tasked with:

a) Reviewing third-party risk policies, risk scoring methodologies, and defining institutional risk appetite and tolerance limits (e.g., maximum allowable vendor downtime, maximum concentration limits with a single provider).

b) Reviewing the risk assessments, materiality classifications, and mitigation plans generated by the First Line.

c) Monitoring the institution's aggregate third-party risk exposure, including identifying systemic operational concentrations.

d) Ensuring that all third-party arrangements comply with macro regulatory standards, identifying potential corporate conflicts of interest, and verifying that the structural independence of outsourced control support functions is preserved.

6.2 Internal Audit function

The Third Line of Defence provides independent, objective assurance to the Board of Directors regarding the overall adequacy, integrity, and operational effectiveness of the third-party risk management Framework and is responsible for:

a) Conducting comprehensive, regular, and independent audits of the bank's entire third-party ecosystem, ensuring that policies are being adhered.

b) Validating the completeness and truthfulness of the institution's Outsourcing Register.

c) Presenting findings, highlighted control deficiencies, and vendor-related governance gaps directly to the Board Audit Committee, ensuring that remediation tracks are monitored and executed by executive management.

7.0 Stress Testing

Institutions should assess the potential impact of extreme but plausible scenarios on third-party arrangements and determine the institution’s ability to absorb shocks, maintain critical operations, and implement contingency measures.

Institutions should ensure that stress testing results, and any other relevant findings, are effectively used in accordance with the objectives and internal policies and procedures of the stress testing framework. These uses should provide insight to the board and senior management, to inform key decisions in the direction and management of the bank. For that purpose, the stress test results should be reported to the board and senior management on a regular basis, at relevant levels of aggregation.

The reports should include the main modelling and scenario assumptions as well as any significant limitations. Results of stress tests should, where appropriate, inform banks’ calibration of risk appetite and limits, financial and capital planning, contingency planning and recovery and resolution planning.

14.0 ENVIRONMENTAL, SOCIAL AND GOVERNANCE RISK MANAGEMENT

14.1 Introduction

Environmental, Social, and Governance (ESG) risks are the risks of negative financial impact on institutions stemming from the current or prospective impacts of ESG factors on its counterparties or invested assets, that is, the risks arising from the core activities of institutions.

ESG factors are environmental, social or governance factors that may have a positive or negative impact on the financial performance or solvency of an institution, sovereign or individual.

ESG risks materialise through the traditional categories of financial risks (credit risk, market risk, operational and reputational risks, liquidity and funding risks). Institutions should therefore consider the potential impacts of ESG risk drivers on their individual business models and assess the financial materiality of these risks. Institutions should manage ESG risks in a manner that is proportionate to the nature, scale and complexity of their activities and the overall level of risk that each institution is willing to accept.

This Guideline should be read together with the Central Bank of Kenya's existing sustainability-related regulatory framework, including the Guidance on Climate-Related Risk Management, the Climate Risk Disclosure Framework (CRDF) for the banking sector, and the Kenya Green Finance Taxonomy (KGFT). While the CRDF focuses on the disclosure of climate-related risks and opportunities, and the KGFT provides a classification system for environmentally sustainable economic activities, this Guideline establishes supervisory expectations for the identification, assessment, monitoring, management and disclosure of broader Environmental, Social and Governance (ESG) risks. The Guideline therefore complements and builds upon these earlier initiatives by promoting an integrated approach to sustainability-related risk management within institutions.

14.2 Environmental Risks

Environmental risks are the financial risks posed by an institution’s exposures to counterparties or invested assets that may be affected by or contribute to the negative impacts of environmental factors. Environmental factors include climate change and other forms of environmental degradation (for example, air pollution, water pollution, waste production and management (water, solid, hazardous), impact scarcity of fresh water, land contamination, biodiversity loss and deforestation, and corrective policy actions aimed at addressing such

factors among others. Subcategories of environmental risks include; climate-related risks, nature-related risks and other environmental risks.

14.3 Climate-Related Risks

Climate-related risks refer to the set of potential risks that may result from climate change and that could potentially impact on the safety and soundness of institutions and have broader financial stability implications for the banking system.

Climate-related risks can arise through physical risk and transition risk channels.

- Physical risks refer to the potential economic costs and financial losses resulting from the increasing severity and frequency of either:

    a. extreme climate change-related weather events such as heatwaves, landslides, floods, wildfires and storms (i.e. acute climate-related physical risks); or
    b. longer-term gradual shifts of the climate such as changes in precipitation, extreme weather variability, ocean acidification, and rising sea levels and average temperatures (i.e. chronic climate-related physical risks).

- Transition risks refer to financial risks which can result from the process of adjustment towards a lower-carbon economy, prompted, for example, by changes in climate and environmental policies, technology or market sentiment and preferences.

14.4 Nature-Related Risks

Nature-related risks encompass a broad range of potential threats and impacts linked to the degradation of ecosystems, biodiversity loss, and other environmental changes. These risks specifically focus on how an institution or society depends on and impacts natural systems. For example, a company may depend on healthy forests for raw materials or water filtration, while its own operations or supply chain can degrade habitats or emit pollutants.

Nature-related risks can be physical risks, transition risks or systemic risks.

- Nature-related physical risks are risks to an institution that result from the degradation of nature and consequential loss of ecosystem services. These risks can be acute or chronic. Nature-related physical risks arise as a result of changes in the biotic (living) and abiotic (non-living) conditions that support healthy, functioning ecosystems. These

risks are usually location specific.

a. Acute risks are the short term, specific events that change the state of nature. For example, oil spills, forest fires or pests affecting harvests.
b. Chronic risks are the gradual changes to the state of nature. For example, pollution stemming from pesticide use or climate change.

- Nature-related transition risks are risks to an institution that result from a misalignment of economic actors with actions aimed at protecting, restoring and/or reducing negative impacts on nature. These risks can be prompted, for example, by changes in regulation and policy, legal precedent, technology or investor sentiment and consumer preferences. Categories of nature-related transition risks include policy risk, market risk, technology risk, reputational risk and liability risk.

- Nature-related systemic risks are risks to an institution that arise from the breakdown of the entire system, rather than the failure of individual parts. These risks are characterised by modest tipping points combining indirectly to produce large failures, where one loss triggers a chain of others, and prevents the system from reverting to its prior equilibrium.

  There are two categories of nature-related systemic risk:

  a. Ecosystem stability risk: Risk of the destabilisation of a critical natural system, so it can no longer provide ecosystem services in the same manner as before. For example, tipping points are reached and regime shifts and/or ecosystem collapses occur that generate forms of physical and/or transition risk.
  b. Financial stability risk: Risk that a materialisation and compounding of nature related physical and/or transition risks leads to the destabilization of an entire financial system.

The five drivers of nature-related risks, include, climate change, land/ freshwater/ ocean use change, resource exploitation, pollution, and invasive species. Currently land use change - transforming land from its natural habitat for agriculture, habitation or infrastructure - is the largest driver of nature loss.

14.5 Social Risks

Social risks are the risks of any negative financial impact on the institution stemming from the current or prospective impacts of social factors on its counterparties or invested assets. Social factors relate to the rights, well-being, and interests of individuals and communities.

They include factors such as, equality and inclusion, public health, labour relations, workplace health and safety, community impacts, training and education, customer privacy and safety, freedom of association, poverty reduction, and responsible supply chain management.

Social risks can be driven by environmental risks, changes in social policy and changes in market sentiment regarding social factors, as illustrated below:

- Environmental degradation caused by climate-related physical change can exacerbate migration, social and political unrest in the most affected regions. In addition, while global warming is not the sole factor influencing migration decisions, it may amplify existing socioeconomic and political drivers, including income inequality, human rights violations, and civil conflict.

- The second driver of social risks is the change in policies and market sentiment linked to the social transformation towards a more inclusive, equitable society. For example, labour rights - which relate to a wide range of core values that should be guaranteed for all individuals, including working hours, minimum wage and health and safety in the workplace - are important social factors that may impact institutions' counterparties. Counterparties that apply a lower standard of labour rights (or other social standards) or operate a business in or are dependent on suppliers with poor labour rights and protection, may face increased costs of compliance in the future, which could have a potential impact on their financial position.

14.6 Governance Risks

Governance risks are the risks of any negative financial impact on the institution stemming from the current or prospective impacts of governance factors on its counterparties or invested assets.

Governance factors cover governance practices, including board diversity and structure, executive leadership, executive pay, audits, internal controls, tax avoidance, codes of conduct and business principles, accountability, transparency and disclosure, board independence, shareholder rights, corruption and bribery, and also the way in which companies or entities include environmental and social factors in their policies and procedures.

Governance risks can be driven by a variety of risk drivers, such as the inadequate management of environmental and social issues, as well as non-compliance with corporate governance frameworks or codes.

14.7 Strategy and Business Model

- Institutions should develop and implement a sound process for understanding and assessing the potential impacts of ESG risks on their businesses and on the environments in which they operate.
- Institutions should consider material ESG risks that could materialise over various time horizons and incorporate these risks into their overall business strategies and risk management frameworks.
- Institutions should understand and evaluate how these risks could impact the resilience of an institution's business model over the short, medium and longer terms and considering how these drivers may affect a bank's ability to achieve its business objectives.
- Institutions should understand and assess their exposure to structural changes in the economy, financial system and competitive landscape in which the institution operates as a result of ESG risks. The board and senior management should be involved at relevant stages of the process, and the approach established by the board for assessing and managing ESG risks should be clearly communicated to managers and employees.
- Institutions' risk management frameworks should be consistent with their stated goals and objectives. Hence, the board and senior management should ensure that their internal strategies and risk appetite statements are consistent with any publicly communicated ESG strategies and commitments.

14.8 Board and Senior Management Oversight

Institutions should integrate ESG risks into governance structures, establishing clear working procedures and responsibilities for business lines, internal control functions, the relevant committee(s) and management body, with a view to ensuring a sound and comprehensive approach to the incorporation of ESG risks into business strategy, business processes and risk management.

The board has the primary responsibility to oversee effective management of ESG risks of an institution. To fulfil this responsibility, the board should consider ESG risks when developing the institution's overall business strategy, business objectives and risk management framework and exercise effective oversight on their implementation.

It is the responsibility of the board of directors to:-

i. ensure that both the Board and Senior Management possess the appropriate skills,

knowledge, and expertise to effectively understand and oversee ESG risks;

ii. approve and periodically review the strategy and risk management framework for ESG risks and opportunities;
iii. clearly set the roles and responsibilities of senior management, internal organisational structures as well as board sub-committees, as applicable, for the management of ESG risks;
iv. ensure adequate and timely reporting to the board and board sub-committee on ESG risks opportunities; and
v. require relevant capacity development and training programmes on ESG risks.

The senior management shall:

i. develop and implement ESG risks management framework, strategy and policies.
ii. regularly review the effectiveness of the framework, strategy, policies, tools and controls;
iii. provide periodic reports, to the board on ESG risks opportunities as well as on the effectiveness and adequacy of the framework;
iv. require that the internal structures responsible for managing ESG risks are clearly defined and have adequate resources, skills and expertise;
v. ensure the adequacy and appropriateness of training and capacity-building programmes to equip staff, particularly frontline personnel, with sufficient awareness, knowledge, and skills to identify potential ESG risks.
vi. and ensure that material ESG risks are addressed in a timely manner.

14.9 Policies and Procedures

Institutions should have documented policies and procedures which enable ESG risks, to be managed in a proactive manner, which at minimum should include:

i. lines of authority and responsibility for managing ESG risks;
ii. a framework for identification, measurement, monitoring, and control of ESG risks; and
iii. contents and frequency of management reports to the Board on ESG risks.

Management of material ESG risks should be embedded in policies, procedures, processes and controls across all relevant functions and business units, including, for example, in client onboarding and transaction assessment.

Given the evolving nature of ESG risks, relevant risk management framework, policies

and procedures, as well as the effectiveness of related internal controls, should be reviewed regularly to keep pace with the changing environment.

14.10 Identification, Measurement, Monitoring and Reporting

Institutions should identify, monitor and manage all ESG risks that could materially impair their financial condition, including their capital resources and liquidity positions.

Institutions should ensure that their risk appetite and risk management frameworks define and consider all material ESG risks to which they are exposed.

Institutions should ensure that their ESG risk management approaches remain comprehensive and proportionate to the nature, scale and complexity of their activities. All institutions should effectively identify and monitor the ESG risks to which they might be exposed in the short, medium and long run, and implement adequate measures to address them.

Institutions should regularly carry out a comprehensive assessment of ESG risks and set clear definitions and thresholds for materiality.

14.10.1 Risk Identification and Measurement

Risk identification can be done by classifying assets according to their ESG characteristics in order to support the identification of ESG risks based on specific qualitative and quantitative indicators. This can be done, for example, through the categorisation of exposures (if applicable, combined) across asset classes, sectors, counterparties, geographies or on the basis of their length of maturity or position in the life cycle of the asset.

- For instance, a geographic classification would help to identify the proportion of assets that are particularly vulnerable to the impact of climate-related physical risks in the form of higher sea levels, droughts or other climate-related hazards in given regions, while a sector classification could be used to enhance understanding of the share of exposures vulnerable to climate-related transition risks, for instance, in the form of regulatory changes and technological progress affecting those specific sectors.

- The identification can be carried out during client on-boarding, credit initiation and underwriting, credit evaluation, credit review and investment decision process.
- Institutions should develop appropriate ESG risk indicators and metrics that enable effective identification, assessment and monitoring of material ESG risks and support risk management decision-making, internal reporting and external disclosures. The indicators

and metrics should be proportionate to the nature, scale and complexity of the institution's activities and should be reviewed periodically to ensure continued relevance. ESG factors, indicators and metrics are set out in Tables I, II and III.

14.10.2 Climate-Related Risks stress testing and scenario analysis

Given the relatively advanced methodologies and data availability for climate-related risks, climate stress testing and scenario analysis are currently more developed than similar approaches for other ESG risks. Institutions should progressively incorporate other material ESG risks into their stress testing and scenario analysis frameworks, where appropriate.

Institutions should make use of stress testing to assess the resilience of their business models and strategies to a range of plausible climate-related pathways and determine the impact of climate-related risk drivers on their overall risk profile. The scenarios should consider both physical and transition risks as drivers of credit, market, operational and liquidity risks over a range of relevant time horizons.

It is critical for institutions to develop requisite capabilities in scenario analysis and stress testing. They should identify and simulate scenarios, which are plausible and relevant, while factoring in the interlinkages between climate related risk and other risks. For stress testing purposes, institutions should incorporate these risks both qualitatively and quantitatively into the scenarios and project their financial condition under a base scenario and stress scenario.

In view of the dynamism that characterizes climate related risks, scenario analysis practices are expected to evolve rapidly, especially as climate science advances. Climate scenario models, frameworks and results should, therefore, be subject to challenge and regular review by a range of internal and/or external experts and independent functions.

14.10.3 Limits

The risk appetite for ESG risks would be implemented with the support of ESG risks metrics and limits. These metrics and limits could cover key aspects of the risk appetite associated with the risk in question, as well as counterparty segments, collateral types and risk mitigation instruments among others. The metrics would mostly be a combination of backward looking and forward-looking indicators, tailored to the business model and complexity of the institution.

For example, in relation to climate-related physical risks, institutions may set exposure limits that reflect the potential effects of climate-related events, including floods and droughts, on

land, real estate, infrastructure, and counterparties' business operations throughout their production cycles.

Similarly, from both a social and a governance perspective, institutions could follow strict measures to exclude from their portfolio counterparties that use child labour or do not respect social and employment safeguards.

14.10.4 Risk Monitoring and Reporting

Institutions should ensure that their internal reporting systems are capable of monitoring material ESG risks and producing timely information to ensure effective board and senior management decision making.

Institutions should have systems in place to collect and aggregate ESG risks data across the organisation as part of their overall data governance.

- Risk data aggregation should incorporate ESG risks to facilitate the identification and reporting of risk exposures, concentrations and emerging risks.
- An appropriate mix of qualitative and quantitative analytic tools and metrics should be employed to monitor relevant risk indicators and ESG risk exposures against the overall strategy and risk appetite.
- Institutions should also put in place adequate processes to ensure that the aggregated data is accurate and reliable.
- Institutions should consider actively engaging clients and counterparties and collecting additional data in order to develop a better understanding of their risk profiles.
- Where reliable or comparable ESG data are not available, institutions may consider using reasonable proxies and assumptions as alternatives in their internal reporting as an intermediate step.

The reporting should be timely and updated regularly, taking into account the evolving nature of ESG risks.

Further, additional channels for transmitting these risks to traditional financial risk categories may yet be undiscovered. As such, institutions should monitor future developments and seek to understand and, where possible, manage the impacts of ESG risk drivers on other material risks should additional transmission channels be identified.

14.11 Risk Management

Institutions should conduct assessment of how the risks posed by ESG risk drivers, whether quantifiable or non-quantifiable, may affect the institution through the traditional risk categories. Institutions can manage the risks as indicated below:

i. Management of Credit Risk

ESG risk drivers may reduce collateral value, borrowers' repayment ability or institutions' recovery of the loan outstanding in the event of default.

Institutions should understand the impact of ESG risk drivers on their credit risk profiles and ensure that credit risk management systems and processes consider ESG risks.

- Institutions should have clearly articulated credit policies and processes to address material ESG related credit risks. This includes prudent policies and processes to identify, measure, evaluate, monitor, report and control or mitigate the impacts of material ESG risk drivers on their credit risk exposures (including counterparty credit risk) on a timely basis.
- Institutions should incorporate consideration of material ESG risks into the entire credit life cycle, including client due diligence as part of the onboarding process and ongoing monitoring of clients' risk profiles.
- Institutions should also identify, measure, evaluate, monitor, report and manage the concentrations within and between risk types associated with ESG. For example, institutions could use metrics or heatmaps to assess and monitor concentration of exposure to geographies and sectors with higher climate-related risks.
- Institutions should consider a range of risk mitigation options to control or minimise material ESG related credit risks. These options may include adjusting credit underwriting criteria, deploying targeted client engagement, or imposing loan limitations or restrictions such as shorter-tenor lending, lower loan-to-value limits or discounted asset valuations.
- Institutions could also consider setting limits on or applying appropriate alternative risk mitigation techniques to their exposures to companies, economic sectors, geographical regions, or segments of products and services that do not align with their business strategy or risk appetite.

ii. Management of Market Risk

A large, sudden and negative price adjustment may be triggered when ESG risks, which have not yet incorporated into prices or valuation, is materialized.

Institutions should understand the impact of ESG risk drivers on their market risk positions and ensure that market risk management systems and processes consider material ESG risks.

- Institutions should identify and understand how ESG risk drivers could affect the value of the financial instruments in their portfolios, evaluate the potential risk of losses on and increased volatility of their portfolio, and establish effective processes to control or mitigate the associated impacts.
- Given the specific characteristics of market risk, analysis of a sudden shock scenario could serve as a useful tool for better understanding and assessing the relevance of ESG risks to a bank's trading book. Such a scenario could, for example, feature variation in liquidity across assets exposed to ESG risk and assume variation in the speed at which exposures could reasonably be closed out.

iii. Management of Liquidity Risk

Access to funding sources could be reduced as market conditions change, where ESG risk drivers, may cause counterparties of institutions to withdraw deposits and draw down credit lines. ESG factors can also affect the availability and/or stability of funding (e.g. hampered or more expensive access to market funding, unstable deposits due to changing customer preferences), thereby creating funding risk. In this context it is important to acknowledge the potential effect of reputational issues on the funding of institutions.

- Institutions should understand the impact of ESG risk drivers on their liquidity risk profiles and ensure that liquidity risk management systems and processes consider ESG risks.
- Institutions should assess the impacts of ESG risks on net cash outflows (e.g. increased drawdowns of credit lines, accelerated deposit withdrawals) or the value of assets comprising their liquidity buffers. Where material and appropriate, institutions should incorporate these impacts into their calibration of liquidity buffers and into their liquidity risk management frameworks.

iv. Management of Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. ESG risks can give rise to operational risks, including legal and reputational risks, arising from an institution's activities. For example, an institution engaged in lending activities that are publicly controversial may experience reputational damage or become exposed to legal claims.

Another example is where institutions are directly exposed to physical risks arising from climate-related factors. Institutions should ensure that their operational risk management adequately considers physical risk impacts, with a view to ensuring their business continuity and ability to recover from disasters, taking into account their geographical location, physical assets and outsourcing arrangements. Institutions should consider physical risk drivers when developing business continuity and disaster recovery plans.

Institutions should understand the impact of ESG risk drivers, on their operational risk and ensure that risk management systems and processes consider material risks.

v. Other risks

Institutions should assess the impact of ESG risk drivers, on other risks, such as strategic, reputational, regulatory compliance and liability risk, and take such risks, where material, into account as part of their risk management and strategy-setting processes.

14.12 Capital and Liquidity Adequacy

Institutions should identify and quantify ESG risks and incorporate those assessed as material over relevant time horizons into their internal capital and liquidity adequacy assessment processes, including their stress testing programmes where appropriate.

- Institutions should develop processes to evaluate the solvency impact of ESG risks that may materialise within their capital planning horizons.
- Institutions should assess ESG risks, over relevant time horizons that may negatively affect their capital position (i.e. through their impact on traditional risk categories) in their internal capital adequacy assessment process (ICAAP).
- Institutions should assess whether ESG risks, could cause net cash outflows or depletion of liquidity buffers, assuming both business-as-usual and stressed conditions (considering severe yet plausible scenarios). Institutions should include risks assessed as material over relevant time horizons that may impair their liquidity position in their internal liquidity adequacy assessment process (ILAAP).

14.13 Internal control and Audit

Institutions should incorporate ESG risks, into internal control frameworks across the three lines of defence, ensuring their sound and comprehensive identification, measurement, and mitigation. The internal control framework should clearly define and assign responsibilities and reporting lines across the three lines of defence.

The internal audit function should periodically review the institution's ESG risk management framework using a risk-based approach and the review, where applicable, should assess:

- the adequacy of governance arrangements for ESG risks;
- the effectiveness of ESG-related policies, procedures and controls;
- the reliability and integrity of ESG data, metrics, risk assessments and disclosures;
- the incorporation of ESG risks into business processes, risk management frameworks and risk appetite statements;
- compliance with applicable regulatory requirements, including climate-related risk management and disclosure requirements; and
- the effectiveness of remedial actions taken to address identified weaknesses.

Material weaknesses, control deficiencies and audit findings relating to ESG risks should be reported to senior management and the board in a timely manner, together with appropriate remediation plans and progress updates.

TABLE I: ENVIRONMENTAL FACTORS		
FACTOR	**INDICATOR**	**METRIC**
Emissions	Financed emissions	Tonnes CO2e attributable to financed activities
	Total GHG emissions (broken down by scope 1, 2 and 3 carbon emissions)	Tonnes of CO2e
	Emissions of air pollutants	Weight in tonnes of air pollutants
	Emissions of water pollutants	Weight in tonnes of water pollutants
	Emissions of inorganic pollutants	Weight in tonnes of inorganic pollutants
	Carbon footprint	Tonnes CO2e
	Exposure to carbon-intensive sectors	% of portfolio or total
	Reduction policies or initiatives on the use and production of fossil fuels	Presence/lack of reduction policies or initiatives in place on the use and production of fossil fuels
	Alignment with climate-transition targets	Percentage reduction in financed and operational emissions against baseline year
	Reduction policies or initiatives on emissions	Presence/lack of reduction policies or initiatives in place on emissions
Energy efficiency	Energy consumption intensity	GWh per employee, branch, or KSh of revenue
	Use of renewable sources of energy	% or total
		Existence of energy transition strategy and targets
Water usage	Water consumption intensity	% or total - weight in Cubic metres of water consumption
Waste production	Production of hazardous waste	% or total - weight in tonnes of hazardous waste
	Reusability/Recyclability	% or total - weight in tonnes of non- recycled waste production
		Presence/lack of initiatives to reduce the production of waste
Biodiversity and ecosystems	Exposure of the institution's operations, counterparties, financed assets and investments in geographic areas impacted by soil degradation	% of portfolio or total
	Exposure of the institution's operations, counterparties, financed assets and investments in geographic areas and industries that are particularly dependent on biodiversity and ecosystem services	% of portfolio or total
	Exposure of the institution's operations, counterparties, financed assets and investments in protected areas or areas of high biodiversity value outside protected areas	% of portfolio or total
Environmental hazards	Exposure to sectors vulnerable to climate impacts	% of portfolio
	Estimated losses under climate stress scenarios	Amount or % of capital
	Exposure of the institution's operations, counterparties, financed assets and investments to areas likely to be affected by heatwaves	% of portfolio or total
	Exposure of the institution's operations, counterparties, financed assets and investments to areas likely to be affected by water scarcity	% of portfolio or total
	Exposure of the institution's operations, counterparties, financed assets and investments to areas likely to be affected by floods	% of portfolio or total
	Exposure of the institution's operations, counterparties, financed assets and investments to areas likely to be affected by coastal erosion	% of portfolio or total

	Exposure of the institution's operations, counterparties, financed assets and investments to areas likely to be affected by wildfires	% of portfolio or total

TABLE II: SOCIAL FACTORS

FACTOR	INDICATOR	METRIC
Financial Inclusion	Relations with local communities (networks)	Establishment of branches in rural and economically and socially underdeveloped areas
	Lending to youth-owned businesses	% of portfolio
	Lending to Medium and Small Enterprises	% of portfolio
	Lending to women-owned businesses	% of portfolio
	Social impact of products and services	Products' potential to reach rural areas and groups of society where development gaps exist
Employee relationships/labour standards	Freedom of association and right to organize	Percentage of employees covered by collective bargaining agreements
	Forced labour	Number of confirmed forced labour incidents
		Overall compliance with labour laws as laid down under the Labour Act and Regulations
	Minimum age and child labour	Percentage of employees above the legal minimum working age
	Equal representation	Average ratio of female to male board members
		Average ratio of females to males in total workforce
	Equal remuneration	Average gender pay gap
		Average ratio of the annual total compensation for the highest individual to the median annual total compensation for all employees (excluding the highest-compensated individual)
		Ratio of annual total compensation for the highest compensated individual to the median annual total compensation for all employees (excluding the highest compensated individual)
	Discrimination	Number of incidents of discrimination (i) reported and (ii) leading to sanctions
	Human capital management and employee relations (training and development opportunities)	Share of employees attending training courses in a given year
		Frequency of performance assessment per employee
	Workplace health and safety	Rate of accidents
		Compliance with guidelines as laid down under the Occupational Safety and Health Act and Regulations.
		Number of workdays lost to injuries, accidents, fatalities and illness
Consumer Protection	Customer protection and product responsibility	Extent to which product recall procedures are in place
		Number of incidents of product recalls/withdrawals
	Personal data security and privacy	Number/rate of data security incidents in which personally identifiable information (PII) was at risk
		Explanation/disclosure of policies and practices relating to user privacy
		Monetary losses incurred as a result of legal proceedings associated with user privacy

	Rights of customers to obtain information about ESG factors	Percentage of significant product/service categories that comply with information and labelling that includes information on sourcing, content (i.e. substances that could have an environmental or social impact), safe use of the product or service, disposal of the product and environmental or social impacts
		Degree of transparency on the management's approach to marketing and labelling ESG-related information
		Publication of information on ESG performance (in the form of stand-alone reports or by integration into Annual Reports)
	Quality and innovation in customer relations	Number of customer complaint incidents
Human Rights	Contribution to human rights projects	Engagement in social projects aimed at supporting and advancing human rights issues
		Number of cases of severe human rights issues and incidents
		Presence/lack of processes and measures for preventing trafficking in human beings
Poverty/famine	Contribution to poverty reduction	Engagement in poverty reduction/aid programmes
		Employment opportunities for economically less advantaged groups

TABLE III: GOVERNANCE FACTORS		
FACTOR	**INDICATOR**	**METRIC**
Ethical considerations	Bribery and Corruption	Convictions and violations of anti-corruption and anti-bribery laws (number of cases and amount of fines)
		Presence/lack of anti-corruption and anti-bribery policies
Strategy and risk management	Strategy implementation, operational execution and monitoring	Percentage of overall loan portfolio classified as green under Kenya Green Finance Taxonomy.
	Internal controls and risk management policies and procedures	Percentage of overall annual loan portfolio assessed using ESG risk criteria
		Existence of formal risk management framework and approved internal control policies across key processes
Inclusiveness	Discrimination	Number of discrimination grievances or complaints
		Lack of a diversity strategy in place (e.g. age, gender, minority groups)
Transparency	Observance of disclosures information rules and practices	Compliance with Disclosure Guideline/Directives
		Publication of sustainability report
Board Oversight	Board oversight of ESG risks	Presence/lack
	Board members trained on ESG risks	Number or %
	Board committees overseeing ESG issues	Presence/lack
ESG Governance	ESG strategy approved by Board	Presence/lack
	ESG targets incorporated into strategic planning	Presence/lack
	ESG risk appetite established	Presence/lack

Please note that: The factors, indicators and metrics presented in Tables I, II and III are illustrative and are intended to assist institutions in identifying, assessing, monitoring and reporting ESG risks and opportunities. Institutions should determine the relevance and materiality of specific indicators taking into account their business model, size, complexity, risk profile and sectoral exposures.

15. CYBERSECURITY RISK MANAGEMENT

This Risk Management Guideline should be read together with the Cybersecurity Guidance Note.

Definition

Cybersecurity Risk refers to the risk of financial loss, operational disruption, regulatory sanctions, legal liability, or reputational damage arising from cyber threats, cyber-attacks, system vulnerabilities, or unauthorized access, disclosure, alteration, or destruction of information assets or information systems.

Institutions should establish and maintain an effective cybersecurity risk management framework to ensure the confidentiality, integrity, and availability of information assets and information systems. The framework should be proportionate to the nature, scale, and complexity of the institution's operations and should be integrated into the overall enterprise risk management framework.

This Section should be read in conjunction with the provisions on Guidance Note on Cyber Security, Operational Risk, Outsourcing Risk, Digital Financial Services Risk, and Legal and Compliance Risk.

Risk Management Process

(a) Risk Identification

Institutions should identify cybersecurity risks arising from their systems, networks, applications, digital channels, and third-party service providers. At a minimum, institutions should identify:

- Critical information assets, systems, and supporting infrastructure;
- Internal and external cyber threats, including malicious actors and insider threats;
- System vulnerabilities and configuration weaknesses;
- Risks arising from emerging technologies including cloud computing, artificial intelligence, Application Programming Interfaces (APIs), and digital platforms; and
- Risks arising from third-party ICT and cybersecurity service providers.

(b) Risk Assessment and Measurement

Institutions should assess cybersecurity risks on an ongoing basis, including:

- Periodic vulnerability assessments and penetration testing;
- Evaluation of likelihood and impact of cyber incidents;

- Classification of information assets based on criticality and sensitivity; and
- Assessment of cyber risk exposure under normal and stressed conditions.

(c) Risk Control and Mitigation

Institutions should implement appropriate cybersecurity controls, including:

- Board-approved cybersecurity governance frameworks;
- Identity and access management controls, including multi-factor authentication;
- Encryption of data at rest and in transit;
- Secure system development lifecycle (SDLC) practices;
- Continuous monitoring, detection, and threat intelligence capabilities;
- Incident response and recovery capabilities; and
- Cybersecurity awareness and training programmes.

(d) Monitoring and Reporting

Institutions should:

- Continuously monitor cybersecurity threats, vulnerabilities, and incidents;
- Maintain cybersecurity key risk indicators (KRIs);
- Conduct regular independent security assessments and penetration tests; and
- Report material cybersecurity incidents to the Central Bank within prescribed timelines.

(e) Governance and Oversight

The Board should approve the cybersecurity risk management framework and risk appetite. Senior management should be responsible for implementation, allocation of resources, and ongoing oversight of cybersecurity risk management.

16. DATA GOVERNANCE RISK MANAGEMENT

Definition

Data governance risk is the risk of financial loss, operational disruption, regulatory sanctions, legal exposure, cyber compromise, strategic misalignment, or reputational damage arising from weak data governance frameworks, poor data quality, ineffective data management practices, or inadequate data controls and stewardship. It also arises from failure to ensure the accuracy, completeness, integrity, confidentiality, availability, timeliness, consistency, reliability, and traceability of data throughout its lifecycle.

Effective data governance forms a critical component of the institution's cybersecurity and operational resilience framework by ensuring that information assets are appropriately classified, protected, monitored, and managed throughout their lifecycle. Weaknesses in cybersecurity controls may compromise confidentiality, integrity, or availability of data and should therefore be considered a source of data governance risk.

The framework should promote data quality, integrity, accountability, transparency, traceability, and accessibility throughout the data lifecycle and should clearly define data ownership, stewardship responsibilities, governance structures, policies, standards, and control mechanisms to ensure that data remains fit for purpose and aligned with the institution’s business objectives, risk appetite, and strategic priorities.

The data governance framework should be integrated with the institution's cybersecurity, information security, operational risk management, technology risk management, business continuity, third-party risk management, and privacy frameworks to ensure that data risks are identified, assessed, protected, monitored, and remediated in a coordinated manner throughout the data lifecycle.

Risk Management Process

(a) Risk Identification

Institutions should establish processes to identify and document data governance risks arising from their business activities, products, services, systems, and third-party arrangements. At a minimum, institutions should identify:

- Critical data assets, data elements, and data flows across the institution;
- Data quality deficiencies, including issues relating to accuracy, completeness, consistency, timeliness, validity, and reliability;
- Gaps in data ownership, stewardship, accountability, and governance arrangements;

- Risks arising from data collection, aggregation, storage, processing, transmission, sharing, retention, archival, and disposal;
- Risks associated with the use of third-party service providers, cloud services, and data-sharing arrangements; and
- Risks arising from fragmented, duplicated, or inconsistent data across systems and business functions.
- Risks arising from cyber threats, including unauthorized access, malware, ransomware, phishing, insider threats, data manipulation, and other cyber events that may compromise the confidentiality, integrity, or availability of data;
- Risks arising from weaknesses in identity and access management, privileged access, encryption, authentication, logging, and monitoring controls;
- Risks associated with emerging technologies, artificial intelligence, digital channels, APIs, and interconnected systems that process or exchange data.

(b) Risk Assessment and Measurement

Institutions should assess and measure data governance risks on an ongoing basis, taking into account the significance, criticality, and intended use of data. The assessment should include:

- Evaluation of data quality dimensions, including accuracy, completeness, consistency, timeliness, validity, integrity, and reliability.
- Assessment of data architecture, data lineage, data aggregation capabilities, and data dependencies.
- Identification and assessment of cybersecurity vulnerabilities, threats, and control weaknesses that may compromise the confidentiality, integrity, availability, authenticity, or resilience of data and supporting information systems.
- Assessment of the effectiveness of cybersecurity controls protecting critical data assets, including access management, encryption, network security, endpoint protection, security monitoring, vulnerability management, and incident response capabilities.
- Assessment of the potential financial, operational, legal, regulatory, strategic, and reputational impacts arising from data quality failures or governance weaknesses.
- Evaluation of the institution's ability to produce accurate, complete, and timely information for decision-making, risk management, and regulatory reporting.

(c) Risk Control and Mitigation

Institutions should establish and maintain appropriate controls to manage and mitigate data governance risks. Such controls should include, at a minimum:

- An enterprise-wide data governance framework approved by the Board or its delegated committee.

- Clearly defined data ownership, stewardship, accountability, and escalation arrangements.
- Data governance policies, standards, procedures, and control frameworks.
- Data quality management processes including validation, reconciliation, cleansing, and remediation procedures.
- Data classification, retention, archival, and disposal policies.
- Data protection, privacy, confidentiality, and access management controls.
- Controls to ensure the integrity and traceability of data throughout its lifecycle.
- Procedures for managing data-related incidents, breaches, and remediation activities.
- Appropriate controls over data obtained from, processed by, or shared with third parties.
- Integration of data governance controls with the institution's cybersecurity and information security frameworks.
- Identity and access management controls based on the principle of least privilege and segregation of duties.
- Encryption of sensitive data during storage, processing, and transmission, commensurate with the sensitivity and criticality of the data.
- Security monitoring, logging, and audit trails sufficient to detect unauthorized access, alteration, or destruction of critical data.
- Regular vulnerability assessments, penetration testing, and security reviews of systems supporting critical data.
- Backup, recovery, and resilience controls to preserve the availability and recoverability of critical data following cyber incidents.
- Procedures to ensure data integrity following cybersecurity incidents, including validation, reconciliation, and restoration of data.

(d) Monitoring and Reporting

Institutions should establish mechanisms to monitor the effectiveness of their data governance framework and controls. At a minimum, institutions should:

- Monitor key data quality indicators and metrics.
- Conduct periodic assessments of compliance with data governance policies, standards, and procedures.
- Track and report material data quality issues, cybersecurity incidents affecting data, unauthorized access events, data breaches, data integrity failures, and remediation activities.
- Monitor remediation actions and emerging data-related risks.
- Provide regular management and Board reporting on material data governance risks, issues, and control effectiveness.

- Monitor cybersecurity risk indicators relating to critical data assets, including privileged access, failed authentication attempts, unauthorized data access, malware events, and data exfiltration attempts.

(e) Governance and Oversight

The Board should approve the institution's data governance framework and ensure that adequate resources, governance arrangements, and control mechanisms are in place to manage data governance risks effectively.

Senior management should be responsible for implementing the approved framework, establishing clear accountability for data management, and ensuring that data governance supports effective risk management, business operations, strategic decision-making, and regulatory reporting.

The institution should establish appropriate governance structures that provide effective oversight of data governance risks and ensure that data governance practices remain proportionate to the institution's risk profile, business activities, and regulatory obligations.

The Board and senior management should ensure that the institution's data governance framework is integrated with its cybersecurity strategy, information security framework, and enterprise risk management framework. Governance arrangements should promote effective coordination among business units, information technology, cybersecurity, risk management, compliance, and internal audit functions to safeguard the confidentiality, integrity, availability, quality, and resilience of data throughout its lifecycle.

Institutions should ensure that data governance risk management and cybersecurity risk management operate as complementary control functions. Material cybersecurity incidents affecting the confidentiality, integrity, or availability of data should be treated as data governance events and managed in accordance with the institution's incident management, operational resilience, business continuity, and regulatory reporting frameworks.

17. LEGAL AND COMPLIANCE RISK MANAGEMENT

This Risk Management Guideline should be read together with the Compliance Risk Management Guideline.

Definition

Legal and Compliance Risk refers to the risk of financial loss, regulatory sanctions, supervisory enforcement actions, litigation, contractual disputes, operational disruption, or reputational damage arising from failure to comply with applicable laws, regulations, prudential standards, supervisory requirements, codes of conduct, contractual obligations, internal policies, or regulatory expectations.

Institutions should establish and maintain an effective legal and compliance risk management framework to ensure ongoing compliance with applicable legal, regulatory, and supervisory requirements in all jurisdictions in which they operate. The framework should support the identification, assessment, monitoring, reporting, and mitigation of legal and compliance risks and promote a culture of integrity, ethical conduct, and compliance throughout the institution.

This Section should be read in conjunction with all relevant provisions of these Guidelines, including those relating to Corporate Governance, Operational Risk, Outsourcing, Consumer Protection, and Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF).

Risk Management Process

(a) Risk Identification

Institutions should establish processes to identify legal and compliance risks arising from their business activities, products, services, delivery channels, systems, outsourcing arrangements, and strategic initiatives. At a minimum, institutions should identify:

- Applicable laws, regulations, prudential standards, supervisory requirements, industry codes, and contractual obligations.
- Regulatory changes, legislative developments, and emerging legal requirements;
- Potential areas of non-compliance with legal, regulatory, or supervisory obligations.
- Litigation, dispute, enforcement, and regulatory investigation exposures.
- Risks arising from new products, services, technologies, business models, and market expansion initiatives.
- Risks associated with third-party service providers and outsourcing arrangements.

- Conduct-related risks that may result in legal, regulatory, or reputational consequences.

(b) Risk Assessment and Measurement

Institutions should assess and measure legal and compliance risks on an ongoing basis, taking into account the nature, scale, complexity, and risk profile of their operations. The assessment should include:

- Evaluation of compliance gaps and control weaknesses.
- Assessment of actual and potential legal liabilities and contractual exposures.
- Analysis of the likelihood and potential impact of regulatory breaches, enforcement actions, or litigation.
- Assessment of the adequacy and effectiveness of compliance controls and monitoring mechanisms.
- Evaluation of the potential financial, operational, legal, strategic, and reputational consequences of non-compliance.

(c) Risk Control and Mitigation

Institutions should establish and maintain appropriate controls to manage and mitigate legal and compliance risks. Such controls should include, at a minimum:

- A documented compliance management framework approved by the Board.
- Policies, procedures, and controls designed to ensure compliance with applicable legal and regulatory requirements.
- Effective legal review and advisory processes for material business activities, products, contracts, and transactions.
- Regulatory change management processes to identify, assess, and implement new legal and regulatory requirements in a timely manner.
- Compliance training and awareness programmes for directors, senior management, and staff.
- Mechanisms for reporting, escalating, investigating, and remediating compliance breaches.
- Independent compliance monitoring and testing programmes.
- Appropriate record-keeping and documentation processes to demonstrate compliance with legal and regulatory obligations.

(d) Monitoring and Reporting

Institutions should establish processes for the ongoing monitoring and reporting of legal and compliance risks. At a minimum, institutions should:

- Monitor changes in laws, regulations, prudential standards, and supervisory expectations;
- Conduct periodic compliance reviews and compliance risk assessments;
- Track compliance breaches, regulatory findings, litigation matters, and remediation actions;
- Monitor the effectiveness of compliance controls and corrective measures; and
- Provide timely and accurate reporting of material legal and compliance risks, breaches, investigations, enforcement actions, and litigation exposures to senior management and the Board.

(e) Governance and Oversight

The Board should approve the institution's legal and compliance risk management framework and ensure that adequate governance arrangements, resources, and control mechanisms are in place to manage legal and compliance risks effectively.

Senior management should be responsible for implementing the framework, fostering a strong compliance culture, and ensuring that legal and compliance risks are appropriately identified, assessed, monitored, and managed across the institution.

Institutions should maintain an independent and adequately resourced compliance function with clearly defined authority, responsibilities, and reporting lines. The compliance function should have unrestricted access to relevant information and should report material legal and compliance matters to senior management and the Board, or a Board committee, on a timely basis.

The internal audit function should periodically review the effectiveness of the legal and compliance risk management framework and associated controls.

18. TRANSFER PRICING RISK MANAGEMENT

Definition

Transfer pricing risk is the risk of financial loss, tax adjustments, regulatory sanctions, or reputational damage arising from inappropriate pricing of transactions between related entities.

Institutions with related-party transactions should ensure compliance with arm's length principles and applicable tax laws through documented policies and governance.

Risk Management Process

(a) Risk Identification

Institutions should identify:

- Related-party transactions.
- Cross-border intra-group transactions.
- Transactions involving shared services, intellectual property, funding arrangements, and management fees.

(b) Risk Assessment and Measurement

Institutions should assess:

- Compliance with applicable transfer pricing requirements.
- Materiality of related-party transactions.
- Potential tax and regulatory exposures.

(c) Risk Control and Mitigation

Institutions should:

- Establish transfer pricing policies.
- Maintain arm's-length pricing methodologies.
- Maintain adequate documentation supporting transfer pricing arrangements.
- Obtain independent reviews where necessary.

(d) Monitoring and Reporting

Institutions should regularly monitor:

- Changes in tax laws and transfer pricing requirements.

- Material transfer pricing exposures.
- Regulatory and tax authority findings.

(e) Governance and Oversight

Senior management should ensure transfer pricing arrangements are transparent, appropriately documented, and consistent with regulatory and tax requirements.

19. ENVIRONMENTAL AND CLIMATE-RELATED FINANCIAL RISK MANAGEMENT

This Risk Management Guideline should be read together with the Environmental, Social and Governance Risks Management Guideline.

Definition

Environmental and climate-related financial risk refers to the risk arising from physical climate events, environmental degradation, and the transition to a low-carbon economy that may affect an institution's financial condition, operations, or business model. Climate risk is increasingly recognized as a distinct risk driver by supervisory authorities.

Institutions should integrate environmental and climate-related risks into their risk management frameworks, including credit, market, and operational risk assessments. This Section should be read together with Sections on Credit Risk, Market Risk, and Operational Risk.

Risk Management Process

(a) Risk Identification

Institutions should identify:

- Physical risks arising from acute and chronic climate events.
- Transition risks arising from policy, legal, technological, and market changes.
- Environmental risks associated with clients, sectors, and geographic concentrations.

(b) Risk Assessment and Measurement

Institutions should:

- Assess climate-related exposures across portfolios.
- Conduct climate scenario analysis and stress testing.
- Evaluate impacts on credit, market, liquidity, operational, and reputational risks.

(c) Risk Control and Mitigation

Institutions should:

- Integrate climate considerations into risk management frameworks.
- Establish sectoral risk limits where appropriate.

- Incorporate environmental and climate factors into lending and investment decisions.
- Develop transition and adaptation strategies.

(d) Monitoring and Reporting

Institutions should:

- Monitor climate risk indicators and emerging developments.
- Report material climate-related exposures to the Board.
- Maintain appropriate climate-related disclosures.

(e) Governance and Oversight

The Board should oversee climate risk strategy and ensure climate-related risks are integrated into enterprise risk management.

20. DIGITAL FINANCIAL SERVICES AND FINTECH RISK MANAGEMENT

Definition

Digital financial services risk refers to the risk arising from the provision of financial services through digital technologies, digital products and delivery channels, innovative financial products and services, fintech partnerships, fintech business models, and other technology-enabled business models. An institution should establish and maintain a comprehensive digital financial services risk management process that is commensurate with the nature, size, complexity and risk profile of its digital financial services and fintech activities. The process should be integrated into the institution's Enterprise Risk Management Framework to ensure effective identification, measurement, assessment, monitoring, control, mitigation and reporting of risks arising from digital financial services and fintech activities.

Institutions offering digital financial services should implement robust governance, cybersecurity, operational resilience, third-party risk management and consumer protection measures to ensure the safe, secure and reliable delivery of digital financial services.

This Section should be read together with Sections on Legal and Compliance Risk, Outsourcing Risk, Data Governance Risk, Cybersecurity Risk and Operational Risk.

Risk Management Process

a) Risk Identification

An institution should establish processes to identify, on an ongoing basis, risks arising from the development, acquisition, deployment, operation and delivery of digital financial services and fintech-enabled activities.

Risk identification should include risks arising from:

i. digital financial service delivery channels, including mobile, internet, agency banking, digital payments, electronic money services, digital wallets and digital lending platforms;
ii. digital technologies and innovation, including Application Programming Interfaces (APIs), cloud computing, artificial intelligence, machine learning, distributed ledger technologies, open banking, Banking-as-a-Service (BaaS), embedded finance and other emerging technologies;
iii. fintech partnerships, outsourcing arrangements, technology vendors, payment service providers, mobile network operators and other digital ecosystem participants;

iv. digital customer onboarding, electronic Know-Your-Customer (e-KYC), digital identity solutions and automated decision-making processes;
v. cybersecurity threats, digital fraud, financial crime, data governance, data privacy and information security weaknesses;
vi. operational disruptions, technology failures and deficiencies in business continuity and operational resilience;
vii. legal, regulatory, consumer protection and compliance risks associated with digital financial services; and
viii. reputational risks arising from failures in digital financial services, technology platforms or fintech partnerships.

Risk identification should be undertaken before entering into fintech partnerships, introducing new digital products or technologies, or implementing material changes to existing digital services.

b) Risk Assessment

An institution should assess the inherent and residual risks associated with digital financial services and fintech activities and determine whether such risks remain within the Board-approved risk appetite. The assessment should consider:

i. the operational complexity and criticality of digital financial services, fintech solutions and supporting technology infrastructure;
ii. the adequacy of governance arrangements, including oversight of fintech partnerships, outsourcing arrangements and other third-party service providers;
iii. cybersecurity resilience, data confidentiality, integrity and availability, and the effectiveness of technology and information security controls;
iv. interoperability, technology integration and operational resilience, including business continuity and disaster recovery capabilities;
v. legal, regulatory, consumer protection and compliance requirements;
vi. concentration risk arising from reliance on critical technology providers, fintech partners or other digital ecosystem participants; and
vii. the potential financial, operational and reputational impact of risks arising from digital financial services and fintech activities.

c) Risk Measurement

An institution should establish methodologies for measuring digital financial services risk associated with digital operations and fintech arrangements. Measurement should include, where applicable:

i. Digital service availability, system resilience, recovery performance and transaction processing reliability.

ii. Fraud attempts and losses, cybersecurity incidents, and operational losses arising from digital service failures.
iii. Service disruptions, concentration risk and performance of fintech partners, technology providers and other critical third-party service providers.
iv. Customer complaints relating to digital financial services and fintech activities.
v. Legal, regulatory and compliance breaches associated with digital financial services.
vi. Application Programming Interface (API) availability and technology integration performance.
vii. Other board-approved key risk indicators.

d) Risk Control and Mitigation

An institution should establish appropriate controls to mitigate risks arising from digital financial services and fintech activities. Such controls should include:

i. Governance frameworks for digital financial services, including oversight of fintech partnerships and other third-party service providers.
ii. Due diligence, ongoing monitoring and contractual arrangements for fintech partners and critical technology service providers.
iii. Secure systems development, change management, identity and access management, encryption, cybersecurity controls, vulnerability management and independent security testing.
iv. Fraud prevention, detection and transaction monitoring controls;
v. Operational resilience measures, including business continuity, disaster recovery and contingency arrangements for critical digital services and third-party disruptions.
vi. Customer awareness programmes on the secure use of digital financial services and fraud prevention.
vii. Periodic review of digital products, technologies, fintech partnerships and associated risks.

The institution should remain fully accountable for all financial services delivered through fintech partnerships, outsourcing arrangements or digital ecosystem participants and should ensure that such arrangements do not impair effective risk management or regulatory oversight.

e) Monitoring

An institution should establish continuous monitoring processes for digital financial services risk and fintech-related risk exposures. Monitoring should include:

i. Performance of digital channels and critical systems.

ii. Compliance with service level agreements by fintech partners and technology providers.
iii. Cybersecurity alerts and threat intelligence.
iv. Fraud trends and suspicious transaction activity.
v. Operational incidents affecting digital services.
vi. Api performance and connectivity.
vii. Cloud service performance and resilience.
viii. Customer complaints and service quality indicators.
ix. Compliance with regulatory obligations.
x. Performance against approved key risk indicators.
xi. Emerging risks associated with new technologies, digital business models and fintech innovations.

Material incidents involving fintech partners or outsourced digital services should be escalated promptly to Senior Management and the Board.

f) Reporting

An institution should establish management information systems to provide timely, accurate and comprehensive reports on Digital Financial Services Risk and fintech-related risk exposures. Reports should include:

i. Material operational, cybersecurity and fraud incidents, including emerging fraud typologies and their impact.
ii. Digital service availability, operational resilience, business continuity and resilience testing results.
iii. The performance of fintech partners, outsourced service providers and other critical third-party service providers.
iv. Customer complaints, service quality trends, regulatory and compliance breaches, and remediation actions.
v. Emerging risks arising from fintech activities, technological developments and the digital operating environment.
vi. The status of corrective actions arising from audits, supervisory reviews, risk assessments and significant incidents.

(e) Governance and Oversight

The Board and senior management should ensure digital innovation is undertaken within approved risk appetite and governance frameworks, and that appropriate corrective measures are implemented where necessary.