RISK MANAGEMENT GUIDELINES FOR BANKS AND FINANCIAL INSTITUTIONS, 2026

TABLE OF CONTENTS

1.0. RISK MANAGEMENT GUIDELINES

1.1. Introduction

1.1.1. In the course of conducting banking business, banks and financial institutions (herein after referred to as 'institutions') assume risks to realize investment returns. However, these risks have the potential to wipe out expected returns and lead to financial losses, which are categorized as either expected or unexpected. Expected losses are anticipated with reasonable certainty, such as projected loan defaults, and are covered by financial provisions. Unexpected losses arise from unforeseen events such as economic downturns, interest rate fluctuations, or natural disasters. Institutions rely on their capital as buffers to absorb these volatile shocks.

1.1.2. Consequently, an effective risk management framework is essential for institutions. By implementing such a risk management framework, institutions can effectively optimize their risk-return trade-off and ensure long-term stability.

1.2. Objectives

1.2.1. Bank of Tanzania (the Bank) has a vested supervisory interest in ensuring that institutions operate in a safe and sound manner. This can be achieved when institutions maintain effective risk management practices.

1.2.2. The Bank has revised a Supervisory Risk Assessment Framework that integrates the CAMELS Rating System and the Risk-Based Supervision Framework, 2010, into a single rating system. The revised approach strengthens supervisory judgment, broadens the scope of risk coverage, and modernizes the assessment process to ensure a more consistent, forward-looking evaluation of banking institutions.

1.2.3. The adoption of the Supervisory Risk Assessment Framework, 2026, necessitates a revision of the Risk Management Guidelines for Banks and Financial Institutions, 2010. The Risk Management Guidelines for Banks and Financial Institutions, 2026 (the Guidelines) are therefore issued and shall replace the Risk Management Guidelines for Banks and Financial Institutions, 2010. The Guidelines incorporate recent market developments, evolving risk dynamics, and applicable international best practices. All institutions are hereby required to comply with the Risk Management Guidelines for Banks and Financial Institutions, 2026, in the conduct of their banking business.

1.3. Risk Description

1.3.1. These guidelines cover the seven most common risks in the banking business: credit, liquidity, interest rate, foreign exchange, operational, strategic, and compliance risks. A description of each risk is as follows:

(a) Credit Risk

Credit risk arises from the potential that an obligor is either unwilling to perform on an obligation or unable to do so due to impaired capacity, resulting in economic loss to the banking institution.

(b) Liquidity Risk

Liquidity risk is the potential for loss to earnings and capital arising from a institution's inability to meet obligations as they fall due or to fund asset growth without incurring unacceptable costs. This includes the inability to manage unplanned fluctuations in funding sources, and the failure to address market conditions that hinder the rapid liquidation of assets with minimal loss in value.

(c) Interest Rate Risk

Interest rate risk is the potential for loss to earnings and capital that arises when there is a mismatch between positions subject to interest rate adjustments within a specified period.

(d) Foreign Exchange Risk

Foreign exchange risk is the potential for loss to earnings and capital arising from adverse movements in currency exchange rates. Specifically, it refers to the impact of these movements on the value of open foreign currency positions.

(e) Operational Risk

Operational risk is the potential for loss to earnings and capital resulting from inadequate or failed internal processes, people, and systems, or from external events.

(f) Strategic Risk

Strategic risk is the potential for loss to earnings, capital or reputation arising from poor business decisions, improper implementation of those decisions, or a lack of responsiveness to industry, economic, or technological changes. This risk is a function of the compatibility of an organization’s strategic goals, the strategies developed to achieve them, the resources deployed, and the quality of implementation.

(g) Compliance Risk

Compliance risk is the potential for loss to earnings, capital, or reputation arising from violations ofor non-compliance withlaws, rules, regulations, agreements, prescribed practices, or ethical standards. It also stems from the incorrect interpretation of these laws and regulations.

1.4. Risk Management

1.4.1. Risk management is a core discipline within every institution, encompassing all activities that influence its risk profile. Contrary to common perception, the goal of risk management is not to minimize risk, but to optimize the risk-reward trade-off. This is achieved by implementing an effective risk management framework that identifies and manages all risk exposures. Risk Management entails four key processes:

(a) **Risk Identification:** To manage risks effectively, an institution shall identify both existing and emerging risks from existing and new business initiatives. For example, risks inherent in lending activities include credit, liquidity, interest rate, foreign exchange, compliance risk and operational risks. Risk identification shall be a continuous process, occurring at both the transaction and portfolio levels.

(b) **Risk Measurement:** Upon identification, risks shall be quantified to determine their potential impact on the institution's earnings and capital. This requires a range of techniques, from simple methodologies to sophisticated models. Accurate and timely measurement is critical; without it, an institution's ability to control and monitor risk is severely limited. Furthermore, measurement tools shall be periodically validated to ensure accuracy. Effective measurement systems assess risks at both the transaction and portfolio levels.

(c) **Risk Control:** Upon measuring risk, an institution shall establish and communicate clear limits through policies, standards, and procedures that delineate responsibility and authority. Beyond setting limits, institutions shall employ diverse mitigation strategies to minimize exposure. A formal process must exist to authorize exceptions or adjustments to these limits when necessary.

(d) **Risk Monitoring:** An institution shall implement a robust Management Information System (MIS) to monitor risk levels and facilitate the timely review of positions and exceptions. To be effective, reports must be accurate, frequent, and actionable, reaching relevant stakeholders timely to ensure prompt intervention when necessary.

1.5. Risk Management Framework

1.5.1. A risk management framework defines the scope of risks, processes and systems for risk management, and the specific roles of personnel involved. The framework shall be comprehensive enough to capture all exposures while remaining flexible to accommodate changes in business activities. The effectiveness of risk management depends on the effective execution of responsibilities across five key oversight functions: the Board of Directors, Senior Management, Risk Management, Internal Audit, and Operations Management, adapted to the institution depending on its size and complexity.

1.5.2. The sophistication of a risk management framework, including its processes and internal controls, should be commensurate with the nature, size, and complexity of the institution's activities. However, certain fundamental principles apply to all institutions regardless of scale. Adherence to these principles reflects the strength of an institution's risk management practices.

1.6. Oversight Functions of Risk Management

1.6.1. Board of Directors

1.6.1.1. The board of directors has ultimate responsibility for the level of risk taken by the institution. While all directors are responsible for understanding the nature of significant risks and ensuring that management takes the necessary steps to identify, measure, monitor, and control them, the level of technical knowledge required may vary depending on the institution's specific circumstances.

1.6.1.2. Directors must possess a clear understanding of the risks their institutions face and receive reports that quantify these risks in meaningful terms. Directors shall actively seek insights into the institution's risk profile from external auditors and experts, and provide clear guidance on acceptable exposure levels, and ensure senior management implements the necessary procedures and controls to adhere to adopted policies. Specifically, the Board of Directors' key responsibilities include:

(a) **Strategic Governance:** Establishing and communicating the institution's corporate culture, values, business strategy, significant policies and enterprise-wide risk appetite framework;

(b) **Stakeholders Protection:** Safeguarding the legitimate interests of all stakeholders;

(c) **Oversight and Compliance:** Monitoring the implementation of approved policies, including the Internal Capital Adequacy Assessment Process (ICAAP), Internal

Liquidity Adequacy Assessment Process (ILAAP), liquidity plans, and internal control frameworks.;

(d) **Leadership Management:** Selecting and appointing a qualified Chief Executive Officer, Internal Auditor, and key senior management, while providing ongoing oversight and independent assessment of their performance; and

(e) **Fiduciary Duties:** Approving financial statements, compensation policies, and succession plans.

1.6.2. **Senior Management**

1.6.2.1. Senior management is responsible for implementing strategies while mitigating associated risks and ensuring ongoing compliance with laws, regulations, and internal policies. Consequently, management shall be actively engaged in institutional operations and possess sufficient knowledge of all major business lines to maintain effective policies, controls, and risk monitoring systems, ensuring clear lines of accountability and authority. Furthermore, senior management shall champion a culture of effective internal controls and high ethical standards. Fulfilling these duties requires a thorough understanding of banking and financial markets, as well as detailed knowledge of the institution's specific operations and necessary risk controls. Specifically, key responsibilities include:

(a) Designing business strategies and objectives tailored to the institution for Board approval;

(b) Creating risk management policies that align with risk appetite and adapt to regulatory changes;

(c) Building a management structure that ensures transparency and accountability, including recruitment of competent staff;

(d) Directing daily operations to ensure adherence to Board policies; and

(e) Keeping the Board fully informed through timely and comprehensive reporting.

1.6.3. **Risk Management**

1.6.3.1. A single line of defence is insufficient for effective risk management. Institutions shall establish distinct oversight functions commensurate with the nature, size, and complexity of their business. The Risk Management Function serves as the second line of defense, providing independent, enterprise-wide oversight of operations management (the first line). Furthermore, this function is responsible for developing and implementing internal

control frameworks and facilitating effective oversight by the Board and its committees. The Risk Management Function typically encompasses the following key activities:

(a) Recognizing significant individual, enterprise-wide, and emerging risks;

(b) Creating and implementing comprehensive enterprise-wide risk management frameworks;

(c) Formulating management policies and procedures to effectively manage identified risks;

(d) Assisting and overseeing the implementation of risk management procedures by operations management;

(e) Developing systems or models for quantifying risk exposure;

(f) Establishing risk metrics, such as stress tests, along with associated tolerance limits;

(g) Implementing an early warning system to detect breaches of risk limits or appetite;

(h) Ongoing surveillance of risk-taking activities to ensure alignment with business strategies, risk limits, and corresponding capital or liquidity levels;

(i) Promptly escalating significant breaches to Senior Management and the Board or Board Committees; and

(j) Periodically presenting reports to Senior Management and the Board or Board Committees regarding risk management activities.

1.6.4. **Operations Management**

1.6.4.1. As the first line of defence, operations management owns and manages risks in a banking institution. Operations management is responsible for planning, directing, and controlling the day-to-day operations of an institution’s activities/business lines in line with the policies and processes approved by the board of directors. Operations management shall ensure that policies and procedures are implemented; control systems and resources are adequate to effectively manage and mitigate inherent risks in an activity/business line. Their key responsibilities include:

(a) Overseeing and directing the day-to-day operations of the institution's activities and business lines, ensuring alignment with policies and processes approved by the Board of Directors;

(b) Establishing and maintaining adequate control systems and resource allocations to effectively manage and mitigate inherent risks associated with specific activities and business lines; and

(c) Actively identifying, assessing, and addressing risks to ensure that operational activities remain within acceptable risk thresholds.

1.6.5. **Internal Audit**

1.6.5.1. As the third line of defense, the Internal Audit Function is responsible for providing independent oversight and objective assurance regarding the effectiveness of the institution's organizational and procedural controls. Key mandates include:

(a) Evaluating the effectiveness of the first and second lines of defense to ensure robust risk management and control environments;

(b) Maintaining the highest level of independence exceeding that of the second line of defense to guarantee unbiased reporting and assessment; and

(c) Ensuring that internal auditors are competent and appropriately trained. To preserve objectivity, they must strictly avoid involvement in developing, implementing, or operating risk management functions or any activities falling under the first or second lines of defense.

1.7. Integration of Risk Management

1.7.1. Risks must not be viewed or assessed in isolation. A single transaction often encompasses multiple risks, and the realization of one risk can trigger others. Because these interactions can either escalate or mitigate overall exposure, the risk management process must explicitly recognize and reflect these interdependencies across all business activities. Management must maintain a holistic view of the institution’s risk profile, supported by a structural framework designed to evaluate risk interrelationships across the entire organization.

1.8. Independent Review of Risk Management

1.8.1. Institutions must ensure that an independent party is responsible for reviewing the effectiveness of and adherence to the institution’s risk management policies and practices. This function may be performed by internal auditors, external auditors, or other qualified professionals, provided they remain independent of risk-taking units and report directly to the Board or its designated committee. To ensure effectiveness, the independent reviewer must possess sufficient authority, expertise, and corporate stature to identify and report

findings without hindrance. Such an independent review shall be conducted at least once every three years, and the reviewer shall consider, among others, the following:

(a) Whether the institution's risk management system is appropriate to the nature, scope, and complexity of the institution and its activities;

(b) Whether the institution has an independent risk management function;

(c) Whether the board of directors and senior management are actively involved in the risk management process;

(d) Whether policies, controls and procedures concerning risk management are well documented and complied with;

(e) Whether the assumptions of the risk measurement system are valid and well documented, data accurately processed, and data aggregation is proper and reliable; and

(f) Whether the institution has adequate staffing to conduct a sound risk management process.

1.9. Contingency Planning and Stress Testing

1.9.1. Institutions must establish mechanisms to proactively identify potential stress situations and maintain plans to address such scenarios in a timely and effective manner. This principle applies to all categories of risks. Contingency planning activities should include, but are not limited to, disaster recovery, reputational risk management, litigation strategy, regulatory response, and liquidity crisis management. Contingency plans must be reviewed regularly to ensure they address reasonably probable events that could impact the institution. Furthermore, these plans should be tested to validate the appropriateness of responses, the efficiency of escalation and communication channels, and the potential impact on the broader institution.

2.0. CREDIT RISK MANAGEMENT

2.1. Introduction

2.1.1. Credit risk arises from the potential that an obligor is either unwilling to perform on an obligation or its ability to perform such obligation is impaired resulting in economic loss to the institution.

2.1.2. Credit risk arises from on balance sheet claims such as loans and overdrafts as well as off balance sheet commitments such as guarantees, letters of credit, and derivative instruments. For most institutions, loans are the largest and most obvious source of credit risk. It arises any time the institution's funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether reflected on or off-balance sheet.

2.1.3. Institution may also be exposed to credit risk when dealing with foreign exchange operations. This may arise when a domestic borrower involved in export business fails to compete in foreign markets due to domestic currency appreciation and thus resulting in inability to repay the domestic loan.

2.1.4. In an institution's portfolio, losses stem from outright default due to inability or unwillingness of a customer or counter party to meet commitments in relation to lending, trading, settlement, and other financial transactions. Losses may also result from reduction in portfolio value due to actual or perceived deterioration in credit quality.

2.1.5. Credit risk not necessarily occurs in isolation. The same source that endangers credit risk for the institution may also expose it to other risk. For instance, a bad portfolio may attract liquidity problems. Therefore, credit risk can trigger other risks, such as liquidity, interest rate risk or foreign exchange risk, highlighting the importance of a holistic approach to risk management.

2.1.6. **Common sources of credit risk are:**

(a) **Credit concentrations:** these are any exposures where the potential losses are large relative to the institution's capital, total assets or, where adequate measures exist, the institution's overall risk level. This concentration may arise from single borrowers, counterparties, a group of connected counterparties, and sectors or industries, such as trade and agriculture. Furthermore, they may arise from common or correlated factors (geographical location or currency); and

(b) **Credit process issues:** Credit risk may arise from weaknesses in the credit granting and monitoring processes. Deficiencies in credit underwriting and management of credit

exposures represent significant sources of credit losses to an institution. In many cases, a robust internal credit process may mitigate credit risk.

2.2. Management of Credit Risk

2.2.1. An institution shall establish a credit risk management framework that clearly defines the scope of credit risk across the organization. The framework shall articulate the institution's credit risk tolerance and the prioritization of credit risk management activities, including risk transfer and mitigation strategies such as guarantees, derivatives, and collateralization. It shall set out policies governing the identification, assessment, approval, administration, measurement, monitoring, reporting, and mitigation of credit risk across the full credit lifecycle. The level of sophistication of the framework shall be commensurate with the institution's overall risk profile and portfolio complexity, and consistent with regulatory expectations.

2.2.2. Credit risk is inherent in all lending activities, which represent a core function of any institution. Effective management of this risk is therefore a cornerstone of a sound and resilient risk management framework. Robust credit risk practices enable the institution to accurately identify, measure, monitor, and mitigate exposures. The quality of credit risk management reflects the strength of the institution's governance and oversight functions, including the board of directors, senior management, operations management, risk management, and internal audit, in fulfilling their respective responsibilities.

2.3. Board of Directors

2.3.1. The board of directors has a critical role to play in overseeing the credit risk management functions of the institution. The board shall have ultimate responsibility for approving the institution's credit risk strategy and significant policies relating to credit risk management, aligned with the institution's overall business strategy. Specifically, the board shall:

(a) describe and approve the credit risk strategy and significant credit risk policies of an institution. The strategy should reflect the institution's tolerance for risk and the level of profitability it expects to achieve by incurring various credit risks. The strategy shall be reviewed at least annually.

(b) provide oversight over the implementation of the institution's credit risk strategy and policies.

(c) ensure that new products and activities are subject to adequate risk management procedures and obtain prior approval of the board of directors or its appropriate committee before being introduced or undertaken.

(d) establish comprehensive credit limits for individual borrowers, counterparties, and groups of connected counterparties, ensuring that these limits aggregate different types of exposures in a consistent and meaningful manner across the banking and trading books, for both on and off-balance sheet items.

(e) set up the overall lending authority structure and explicitly delegate credit sanctioning authority, where appropriate, to senior management and the credit committee.

(f) appoint senior management with appropriate expertise and integrity, oversee their performance in implementing the credit risk framework, and take corrective action, including dismissal, where risk management objectives or policies are not met.

(g) ensure that internal audit periodically reviews the credit operations to assess adherence to policies, the adequacy of procedures, and the effectiveness of internal controls.

(h) ensure that the institution's credit risk management framework is subject to independent, objective, and periodic assessment, which may be conducted by the Internal Audit function or independent experts, covering the effectiveness of credit risk policies, controls, and processes.

(i) review and deliberate credit risk management reports, including portfolio quality and the adequacy of the institution's provisions for credit losses.

(j) ratify exposures exceeding management's delegated authority and being aware of exposures that, while worthy of consideration, fall outside existing credit policies.

(k) outline the content and frequency of management reports submitted to the Board on credit risk management, including but not limited to:

(i) loan book performance;

(ii) loan classification and provisioning;

(iii) stress-testing results;

(iv) large exposures and related-party exposures;

(v) concentration levels and mitigants;

(vi) limit breaches and compliance issues;

(vii) Internal control failures; and

(viii) Legal and regulatory concerns.

2.3.2. **Credit strategy**

2.3.2.1. The credit strategy shall determine the institution's risk appetite that optimises return while keeping credit risk within predetermined limits. The credit risk strategy shall reflect the institution's profitability, credit quality, and portfolio growth targets, and must be consistent with the credit risk tolerance, diversification policy and overall corporate strategy. At a minimum, the credit risk strategy shall spell out:

(a) plan to grant credit based on various client segments and products, economic sectors, geographical location, currency and maturity;

(b) target market within each lending segment and level of concentration; and

(c) pricing strategy.

2.3.2.2. The institution shall give due consideration to the target market while devising a credit risk strategy. The credit procedures shall aim to obtain an in-depth understanding of the institution's clients and their businesses.

2.3.2.3. The credit risk strategy shall be effectively communicated throughout the institution. All relevant personnel shall clearly understand the institution.

2.3.2.4. Institution's approach to granting and managing credit and shall be held accountable for complying with internal policies and procedures.

2.3.2.5. The institution shall ensure that 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.

2.3.3. **Credit Policy**

2.3.3.1. An institution shall have in place sound, comprehensive and clearly defined credit policies, processes, and procedures consistent with prudent standards, practices, and relevant regulatory requirements commensurate with the size, complexity, and scope of the institution's operations.

2.3.3.2. The credit policies describe a framework for investment and lending decisions and reflect an institution's tolerance for credit risk. To be effective, policies shall be communicated in a timely manner and shall be implemented through all levels of the institution by appropriate procedures. Any significant deviation/exception to these

policies must be communicated to the board, and corrective measures shall be taken. At a minimum, credit policies shall include:

(a) general areas of credit in which the institution is prepared to engage or is restricted from engaging, such as types of credit facilities, types of collateral security, types of borrowers, geographical areas, or economic sectors on which the institution may focus.

(b) detailed and formalized credit evaluation/appraisal process, administration, and documentation.

(c) credit approval authority at various hierarchical levels, including authority for approving exceptions such as credit extension beyond prescribed limits.

(d) clearly-established process for approving new credits as well as the amendment, renewal and refinancing of existing credits.

(e) concentration limits on single counterparties and groups of connected counterparties, particular industries or economic sectors, geographical areas, and specific products.

(f) insider and related-party credit-granting requirements and procedures.

(g) authority for approval of allowance for probable losses and write-offs.

(h) credit pricing.

(i) roles and responsibilities of units/staff involved in origination and management of credit.

(j) guidelines on the management of problem loans.

(k) guidance for internal rating systems, including the definition of each risk grade; criteria to be fulfilled while assigning a particular grade, as well as the circumstances under which deviations from criteria can take place. and

(l) the content and frequency of management reports submitted to the Board on credit risk management, including but not limited to loan book performance; loan classification and provisioning; stress-testing results; large exposures and related-party exposures; concentration levels and mitigants; limit breaches and compliance issues; Internal control failures; and Legal and regulatory concerns.

2.3.4. **Limit Setting**

2.3.4.1. An institution shall establish a comprehensive and prudent credit limit structure that supports effective credit risk management. This includes setting exposure limits for

individual borrowers, counterparties, groups of connected persons, aggregating exposures across products, economic activities, business lines and geographic regions on both banking and trading books, including on- and off-balance-sheet exposures.

2.3.4.2. The institution's internal limits shall comply with the exposure limits set by the Bank and are consistent with the institution's risk appetite, capital strength, borrower creditworthiness, economic conditions, and the genuine credit needs of borrowers.

2.3.4.3. An institution shall ensure credit limits are reviewed regularly, at least annually or more frequently when a counterparty's credit quality deteriorates. Any changes to credit limits shall be fully substantiated and supported by a sound credit assessment, including stress testing.

2.3.5. **Lending Authority**

2.3.5.1. An institution shall maintain a sound and well-governed credit portfolio through the establishment and oversight of a formal, robust evaluation and approval process for all credit decisions. The institution shall ensure that approvals are carried out in accordance with documented policies and delegated authorities, and that a clear audit trail exists to demonstrate compliance with these procedures and identify the individuals or committees involved in analysing and deciding on each credit proposal.

2.3.5.2. institution shall ensure that every credit proposal is subject to thorough analysis by qualified credit analysts with expertise appropriate to the size and complexity of the transaction.

2.3.5.3. institution shall ensure that the credit-granting approval process clearly defines accountability for decisions taken and specifies the levels of authority designated to approve new credits or changes in credit terms.

2.3.5.4. An institution shall establish proper procedures to mitigate abuses arising from credits granted to connected or related parties. The procedures shall ensure that such credits are extended strictly on an arm's-length basis, under terms and conditions no more favourable than those applied to comparable non-related borrowers. The institution shall impose rigorous limits on related-party exposures and require ongoing monitoring of these exposures. Importantly, all related-party transactions must be subject to the approval of the Board of Directors, and any board member with a personal interest in the transaction shall be excluded from the approval process.

2.4. Senior Management

2.4.1. Senior management shall be responsible for implementing the institution's credit risk management strategies and policies, as well as ensuring that the procedures are put in

place to manage and control credit risk and the quality of the credit portfolio in accordance with the approved policies. Specifically, Senior Management shall:

(a) implement the credit risk strategy approved by the board of directors.

(b) develop policies and procedures for identifying, measuring, monitoring, and controlling credit risk, which shall be submitted to the board of directors for approval prior to implementation.

(c) ensure that the credit-granting function is properly managed and that all credit exposures remain within prudential standards and approved internal limits.

(d) establish and enforce effective internal controls and related practices to ensure that any exceptions to credit policies, procedures, or limits are promptly identified and reported to the appropriate management level for timely corrective action.

(e) ensure that the credit risk inherent in all products and activities is properly identified, measured, monitored, and controlled. For any new product or activity, senior management shall ensure that appropriate risk assessments and controls are in place prior to introduction and that such product or activity is approved in advance by the board of directors or its designated committee.

(f) operate within sound and well-defined credit-granting criteria approved by the board.

(g) develop and implement an appropriate reporting system covering content, format, and frequency of information regarding the credit portfolio and credit risk management to ensure effective analysis of existing and potential credit risk exposure.

(h) ensure that the institution maintains an effective system for the early identification and remediation of deteriorating credits, as well as for the management and resolution of problem loans and workout situations.

(i) oversee the quality of the credit portfolio to ensure it is prudently valued and classified, adequate provisions for probable losses are made, and uncollectible exposures are written off.

(j) establish Management Information Systems (MIS) capable of generating high-quality, detailed, and timely information that supports oversight of credit risk, assess portfolio quality and composition, and enables accurate determination of the institution’s capital requirements. The system shall be able to capture credit exposures approaching or exceeding established limits, aggregate exposures to

individual borrowers and counterparties and report exceptions promptly, allowing senior management to take corrective action.

(k) develop effective lines of communication to ensure the timely dissemination of credit risk management policies, procedures, and other relevant information to all individuals involved in the credit risk management process.

2.4.2. **Credit Granting**

2.4.2.1. Establishing sound, well-defined credit-granting criteria is essential to approving credit in a safe and sound manner. The criteria shall specify eligibility requirements for granting credit, the amount to be granted, types of credit, the terms and conditions of the credit.

2.4.2.2. An institution shall obtain sufficient information to enable a comprehensive assessment of the risk profile of the potential borrower or counterparty. At a minimum, the factors to be considered in analyzing credit applications shall include:

(a) the purpose of the credit and source of repayment;

(b) the integrity and reputation of the borrower or counterparty

(c) 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;

(d) the borrower's repayment history and current capacity to repay, based on historical financial trends and cash flow projections;

(e) a forward-looking analysis of the capacity to repay based on various scenarios;

(f) the legal capacity of the borrower or counterparty to assume the liability;

(g) for commercial credits, the borrower's business expertise and the status of the borrower's economic sector and its position within that sector;

(h) the proposed terms and conditions of the credit, including covenants designed to monitor and manage changes in the future risk profile of the borrower; and

(i) where applicable, the adequacy and enforceability of collateral or guarantees.

2.4.2.3. Once credit-granting criteria have been established, it is essential for the institution to ensure that the information it receives is sufficient to make proper credit-granting decisions. This information may also serve as the basis for rating the credit under the institution's internal rating system.

2.4.2.4. Before granting credit, an institution shall understand the borrower or counterparty and ensure they are reputable and creditworthy. Policies shall prevent dealings with individuals involved in fraud or crime. The assessment can include checking references from known parties, consulting credit bureaus, and reviewing financial and personal background of key management. Credit shall not be granted solely based on familiarity or perceived reputation.

2.4.2.5. An institution shall establish procedures to identify circumstances in which two or more borrowers shall be classified as connected parties and consequently treated as a single borrower for credit risk purposes. The procedures shall ensure the aggregation of exposures to all corporate or non-corporate entities that exhibit common ownership, common control, or any other significant interconnections, including, inter alia, shared management or familial relationships.

2.4.2.6. In loan syndications, participants shall perform their own independent credit risk analysis and review of syndicate terms prior to committing to the syndication. Each institution shall analyze the risk and return on syndicated loans in the same manner as other loans.

2.4.2.7. In considering potential credits, institutions must recognize the necessity of establishing provisions for expected losses and holding adequate capital to absorb risks and unexpected losses. The institution should factor these considerations into credit-granting decisions, and the overall portfolio monitoring process.

2.4.2.8. An institution may utilize credit risk mitigants such as collateral, guarantees, and derivatives or on balance sheet netting to help mitigate risks inherent in individual credits. However, credit transactions shall be entered into primarily on the strength of the borrower’s repayment capacity. Credit risk mitigants shall not be a substitute for a comprehensive assessment of the borrower or counterparty, nor can it compensate for insufficient information. In addition, institutions need to be mindful that the value of collateral may as well be impaired by the same factors that have led to the diminished recoverability of the credit

2.4.2.9. An institution shall 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 realizable. With regard to guarantees, institutions shall evaluate the level of coverage being provided in relation to the credit quality and legal capacity of the guarantor. Institutions shall only factor explicit guarantees into the credit decision and not those that might be considered implicit, such as anticipated support from the government.

2.4.3. **Measurement and Monitoring**

2.4.3.1. An institution shall have methodologies that enable quantification of the risk involved in exposures to individual borrowers or counterparties. In addition, the institution shall be able to analyze credit risk at the product and portfolio level in order to identify any particular sensitivities or concentrations. The measurement of credit risk shall take into account of:

(a) specific nature of the credit and its contractual and financial conditions;

(b) exposure profile until maturity in relation to potential market movements

(c) existence of collateral or guarantees; and

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

2.4.3.2. An institution shall use measurement techniques that are appropriate to the complexity and level of the risks involved in its activities, based on robust data, and subject to periodic validation. The analysis of credit risk data shall be undertaken at an appropriate frequency, with the results reviewed against relevant limits.

2.4.3.3. An institution shall conduct periodic stress tests of credit risk and review the results of those tests to identify and respond to potential changes in market conditions that could adversely impact its performance.

2.4.3.4. An institution needs to develop and implement comprehensive procedures and information systems to monitor the condition of individual credits and single obligors across the institution's various portfolios. These procedures need to define criteria for identifying and reporting potential problem credits and other transactions to ensure they are subject to more frequent monitoring and possible corrective action, classification and/or provisioning. An effective credit monitoring system will include measures to ensure that:

(a) the institution understands the current financial condition of the borrower or counterparty;

(b) all credits are in compliance with existing covenants;

(c) customer's utilization are in line with the approved credit lines;

(d) projected cash flows on major credits meet debt servicing requirements;

(e) where applicable, collateral provides adequate coverage relative to the obligor's current condition; and

(f) identification and classification of problem credits is conducted timely.

2.4.3.5. Institutions shall establish a system to monitor the credit portfolio daily, ensuring loans are serviced as per facility terms, provisions are adequate, risk limits are maintained, and compliance with regulatory requirements. This enables senior management to track portfolio quality, identify trends, and adjust credit strategies proactively. The credit policy shall provide clear procedural guidelines for credit risk monitoring. At a minimum, it shall lay down procedures relating to:

(a) the roles and responsibilities of individuals responsible for credit risk monitoring;

(b) the assessment procedures and analysis techniques (for individual loans & overall portfolio);

(c) the frequency of monitoring;

(d) the periodic examination of collaterals and loan covenants;

(e) the frequency of site visits; and

(f) the identification of any deterioration in any loan.

2.4.4. **Credit Administration**

2.4.4.1. Credit administration is a critical element in maintaining the safety and soundness of an institution. Once a credit is granted, it is the responsibility of the business function, often in conjunction with a credit administration support team, to ensure that the credit is properly maintained. This includes keeping the credit file up to date, obtaining current financial information, sending out renewal notices and preparing various documents such as loan agreements.

2.4.4.2. In establishing credit administration areas, an institution shall ensure:

(a) efficiency and effectiveness of credit administration operations, including monitoring documentation, contractual requirements, legal covenants, collateral, etc;

(b) accuracy and timeliness of information provided to management information systems;

(c) adequacy of controls over all back office procedures; and

(d) compliance with prescribed policies and procedures as well as applicable laws and regulations.

2.4.4.3. For the various components of credit administration to function appropriately, the institution shall understand and demonstrate that it recognizes the importance of this element of monitoring and controlling credit risk.

2.4.4.4. The credit files shall include allthe information necessary to ascertain the current financial condition of the borrower or counterparty, as well as sufficient information to track the decisions made and the history of the credit. Specifically, the credit files shall include current financial statements, financial analyses, and internal rating documentation, internal memoranda, reference letters, and appraisals. The loan review function should determine that the credit files are complete and that all loan approvals and other necessary documents have been obtained.

2.4.5. **Internal Risk Rating and Provisioning**

2.4.5.1. An institution shall develop and utilize an internal risk rating system appropriate to the nature, size and complexity of the institution's activities. A well-structured internal risk rating system is a useful means of differentiating the degree of credit risk in the different credit exposures of an institution. The system shall facilitate the determination of the overall characteristics of the credit portfolio, concentrations, problem credits, and the adequacy of loan loss provisions. In determining loan loss provisions, institutions shall ensure that the Bank of Tanzania classification criteria are the minimum.

2.4.5.2. Internal risk rating system shall categorize credits into various classes designed to take into account the gradations in risk ranging from satisfactory to unsatisfactory, in order to differentiate the relative credit risk they pose. An effective rating system shall consider rating of both the riskiness of the borrower or counterparty and the risks associated with a specific transaction.

2.4.5.3. The ratings assigned to individual borrowers or counterparties when credit is granted shall be reviewed regularly, and each credit shall receive a new rating if conditions improve or deteriorate. To ensure that internal ratings remain consistent and accurately reflect the quality of each credit, the responsibility for assigning or validating these ratings should rest with a credit review function that is independent from the credit-origination process. Additionally, an independent unit shall periodically assess the consistency and accuracy of the ratings.

2.4.6. **Managing Problem Credits**

2.4.6.1. An institution shall establish a system for identification of problem credits at an early stage, when there may be more options available for remedial measures. Once the credit is identified as problem, it should be managed under a dedicated remedial process.

2.4.6.2. Responsibility for remediation of problem credits may be assigned to the originating

business function, a specialized workout section, or a combination of the two, depending upon the size and nature of the credit and the reason for its problems. When an institution has significant credit-related problems, it is important to segregate the workout function from the credit origination function. The additional resources, expertise and more concentrated focus of a specialized workout section normally improve collection results.

2.4.6.3. A problem credit management process encompasses the following basic elements:

(a) Negotiation and follow-up: Proactive effort should be taken in dealing with obligors to implement remedial plans, by maintaining frequent contact and internal records of follow-up actions. Often rigorous efforts made at an early stage prevent institutions from litigations and loan losses.

(b) Workout remedial strategies: Appropriate remedial strategies such as restructuring of loan facility, enhancement in credit limits or reduction in interest rates help improve obligor's repayment capacity. However, it depends upon business condition, the nature of problems being faced and most importantly obligor's commitment and willingness to repay the loan. While such remedial strategies often bring up positive results, institutions need to exercise great caution in adopting such measures and ensure that such a policy does not encourage obligors to default intentionally. The institution's interest shall be the primary consideration in case of such workout plans. It is important that competent authority approves such workout plans before their implementation.

(c) Review of collateral and security documents: An institution shall ascertain the loan recoverable amount by updating the values of available collateral with a formal valuation. Security documents shall be reviewed to ensure the completeness and enforceability of contracts and collaterals/guarantees.

(d) Status Report and Review: Problem credits shall be subject to more frequent review and monitoring. The review shall update the status and development of the loan accounts and progress of the remedial plans. Progress made on problem loans shall be reported to the senior management.

2.5. Operations Management

2.5.1. Operations Management refers to the business units and front-line staff who own and manage credit risk on a day-to-day basis. This is the first line of defence in credit risk management by an institution. They are responsible for ensuring that all credit exposures are properly identified, measured, controlled, and monitored. This includes

maintaining robust internal controls, adhering to credit policies, and ensuring compliance with approved lending limits and regulatory requirements.

2.5.2. Operations Management shall implement sound underwriting standards and effective credit administration, while also monitoring ongoing exposures to identify deteriorating credits and potential problem credit accommodations. Staff are expected to have sufficient skills and expertise to manage credit risks, and the institution shall provide them with clear policies, procedures, and adequate management information systems to support their responsibilities.

2.5.3. The first line of defence forms the foundation of effective credit risk management. By managing risks where they originate, the first line of defence ensures the institution operates within prudent risk limits,aligned with both internal policies and supervisory expectations. Other responsibilities of the Operations Management with regard to credit risk management shall include:

(a) ensuring that credit reviews incorporate updated information on the obligor's financial condition, business performance, and conduct of accounts. Exceptions identified during monitoring shall be assessed for their impact on creditworthiness, including on a consolidated group basis to account for interconnections within borrowing groups.

(b) identifying, measuring, and controlling material credit risks that may adversely affect the achievement of the institution's objectives.

(c) implementing control structures for credit activities, supported by credit control policies and procedures, and verify ongoing compliance with these requirements.

(d) effective communication of credit policies, procedures, and relevant guidance to staff, ensuring they understand their duties and responsibilities.

(e) implementing and maintaining robust credit information systems covering all lending activities. These systems must be secure, independently monitored, supported by adequate contingency arrangements, capable of identifying related borrowers, and able to provide accurate, timely, and comprehensive portfolio information.

(f) conducting internal rating of borrowers and ensuring timely and adequate review of the loan portfolio, including loan classifications and adequate provisioning for credit losses.

(g) Implementing and maintaining robust processes for managing non-performing and written-off loans, ensuring effective recovery, monitoring, and control procedures.

2.6. Risk Management

2.6.1. Risk Management is a second line of defence that serves as the independent oversight function in the institution, providing guidance, monitoring, and challenge to the first line of defence in managing credit risk.

2.6.2. The Risk management function shall be adequately staffed and equipped with necessary expertise, tools and resources to effectively oversee the credit risk management framework. The function must ensure continuous monitoring of the credit risk profile of the institution.

2.6.3. Risk Management function shall develop risk management frameworks, policies, and limits, and ensure that the institution's credit risk exposures are consistent with regulatory requirements and internal policy. Unlike the first line of defence, the second line shall not engage in revenue generation or direct credit risk-taking, but it shall have authority to access information and challenge the first line when necessary. Key responsibilities of the risk management function in credit risk management shall include:

(a) implementing independent and ongoing assessments of the credit risk management process. This includes reviewing credit administration, accuracy of credit ratings, adequacy of loan loss provisions, and overall portfolio quality. All credit facilities shall undergo at least quarterly risk reviews, with more frequent reviews for new or high-risk accounts.

(b) identifying, measuring, and monitoring credit risk in line with the approved policies and procedures and regulatory requirements.

(c) maintaining robust MIS capable of generating accurate and timely reports, including early warning indicators for deteriorating credits.

(d) regularly and promptly reporting key credit risk issues to senior management and the Board.

(e) conducting credit stress testing exercises to evaluate potential losses under adverse conditions, using realistic assumptions and demonstrating corrective management actions.

2.7. Internal Audit

2.7.1. The third line of defence in credit risk management is the institution's internal audit function. This line provides independent assurance on the adequacy and effectiveness of risk management controls. Internal audit evaluates whether the first and second lines

are operating as intended, confirms compliance with credit risk policies and procedures, and ensures that risks are accurately identified, measured, and reported.

2.7.2. The Internal audit function shall assess the adequacy of the institution's credit risk framework, including risk measurement models, credit approval processes, and monitoring mechanisms. It shall also review adherence to regulatory requirements and internal policies, and ensure that risk mitigation techniques, such as collateral and guarantees, are properly applied. By doing so, the internal audit provides assurance by highlighting potential blind spots or lapses in the first and second lines.

2.7.3. The internal audit function shall maintain independence and objectivity. Internal auditors shall not have operational responsibilities that may compromise their judgment, and they shall report directly to the board audit committee or board of directors. This structural independence helps ensure that audits of credit risk management processes are unbiased and credible.

2.7.4. The internal audit function is an integral part of robust credit risk management, ensuring that the institution remains resilient, transparent, and aligned with international best practices on sound risk management. By identifying control weaknesses, process gaps, and emerging credit risk trends, the internal audit provides actionable recommendations that strengthen risk management.

2.7.5. An institution shall ensure the internal audit function has a clear reporting line, sufficient skills, and adequate resources to carry out assignments effectively, independently, and objectively. Its expertise and experience shall be commensurate with the institution's business activities and the scale of credit risks, enabling thorough assessment and evaluation of credit risk management practices.

2.7.6. An institution's Board of Directors or its audit committee shall appoint, evaluate performance, and, where necessary, dismiss the internal auditor, strengthening governance and oversight. Key responsibilities of the internal audit function in credit risk management shall include:

(a) developing and implementing a risk-based audit plan that adequately covers all areas posing significant credit risk. The audit plan must define an appropriate scope and frequency of reviews, ensuring higher-risk areas are assessed more frequently and comprehensively.

(b) evaluating the design, implementation, and effectiveness of the institution’s credit risk management framework, including policies, procedures, controls and risk monitoring processes.

(c) Internal Audit shall evaluate the effectiveness of key credit risk processes, including credit origination, approval, administration, monitoring, classification, provisioning, and recovery.

(d) reviewing the design and implementation of credit risk management systems and governance processes across the first and second lines of defense, including an assessment of the second line's independence.

(e) reporting directly to the Board or Audit Committee on credit risk matters.

(f) tracking and monitoring implementation of recommendations arising from internal audits, external audits, and supervisory authority reviews related to credit risk. This includes ensuring that business units respond to raised issues promptly, accurately, and adequately, and that regular reports are provided to the Board of Directors or its relevant committees on both pending and resolved matters.

3.0. OPERATIONAL RISK MANAGEMENT

3.1. Introduction

3.1.1. Operational risk is 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.

3.1.2. The development of the global financial systems, combined with rapid financial innovation and emerging technologies, increases the complexity of institutions' and overall risk profiles. As a result, operational risk is becoming more significant. Examples of these developments include:

(a) The increased use of highly automated technology which has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on automated systems;

(b) Growth of digital banking brings with it potential risks (e.g. internal and external fraud and system security issues) that are not yet fully understood;

(c) Acquisitions, mergers, and consolidations bring the risk of system incompatibility and loss of staff morale;

(d) Engagement in risk mitigation techniques (e.g. collateral and derivatives) by institutions to optimize their exposure to market risk and credit risk, but which in turn may produce other forms of risk (e.g. legal risk); and

(e) Growing use of outsourcing arrangements and participation in clearing and settlement systems, which can mitigate some risks but can also present other significant risks to institutions.

3.1.3. Operational risk may arise from a number of sources as follows:

(a) **People:** Events that may result in substantial loss include fraud like intentional misreporting of positions, employee theft, insider dealings, robbery, forgery, and damage from computer hacking. Some of the contributing factors are as follows:

(i) Lack of adequate skills and knowledge;

(ii) Inadequate training and development;

(iii) Improperly aligned compensation schemes and incentives;

(iv) Lack of integrity;

(v) Lack of understanding of performance standards or expectations; and

(vi) Inadequate human resource control (including supervision and segregation of incompatible duties)

(b) Internal processes and systems: Business disruption and system failures, such as hardware and software failures, telecommunication problems, and utility outages, data entry errors, collateral management failures, cyber-attacks, non-client counterparty misperformance, and vendor disputes, are examples of operational risk resulting from internal processes and systems. Some of the contributing factors are as follows:

(i) Damage to physical assets;

(ii) Inadequate or obsolete technology;

(iii) Lack of proper documentation;

(iv) Lack of or inadequate policies, procedures and controls;

(v) Poor management information system; and

(vi) Lack of or inadequate contingent plans.

(c) External events: Terrorism, vandalism, earthquakes, fires and floods are examples of events that may cause operational risk in an institution.

3.1.4. Operational risk differs from other risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and that this affects the risk management process. At the same time, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to significant losses.

3.2. Management of Operational Risk

3.2.1. An institution shall establish an operational risk management framework that clearly defines the scope of operational risk within the organization. This framework must articulate the institution's risk tolerance and the prioritization of operational risk management activities, including strategies for transferring risk. Additionally, it shall include policies for identifying, assessing, monitoring, and mitigating risk. The framework's level of sophistication should be commensurate with the institution's overall risk profile. At a minimum the framework shall include the following:

(a) identify the governance structures used to manage operational risk, including reporting lines and accountabilities, and the mandates and members of the operational risk governance committees;

(b) describe the tools for risk identification, assessment and control as well as roles and responsibilities of the three lines of defence in using them;

(c) describe the institution's accepted operational risk appetite and tolerance; material activity triggers or limits for inherent and residual risk; and the approved risk mitigation strategies and instruments;

(d) describe the institution's approach to ensure controls are designed, implemented and operating effectively;

(e) describe the institution's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

(f) establish risk reporting and management information systems (MIS) producing timely, and accurate data;

(g) provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives across all business units. The taxonomy can distinguish operational risk exposures by event types, causes, materiality and business units where they occur; it can also flag those operational exposures that partially or entirely represent legal (including conduct), model and ICT (including cyber) risks, as well as exposures in the credit or market risk boundary;

(h) provide for appropriate independent review and challenge of the outcomes of the risk management process; and

(i) require the policies to be reviewed and revised as appropriate based on continued assessment of the quality of the control environment, addressing internal and external environmental changes or whenever a material change in the operational risk profile of the institution occurs.

3.2.2. Operational risk is inherent in all institutional products, activities, processes, and systems. Therefore, effective management of this risk is a fundamental element of a robust risk management program. Sound operational risk management enables the institution to better understand and mitigate its risk profile, and it reflects the effectiveness of oversight

functions, specifically the board of directors, senior management, operations management, risk management, and internal audit in fulfilling their responsibilities.

3.3. Board of Directors

3.3.1. The Board of Directors has ultimate responsibility for the level of operational risk taken by an institution. The board shall establish, approve and periodically review the operational risk management framework of an institution. In addition, the Board shall oversee material operational risks and effectiveness of key controls, and ensure that senior management implements the policies, processes, and systems of the Operational risk management framework effectively at all decision levels. At a minimum, the Board shall:

(a) establish a comprehensive Code of Conduct or Ethics Policy governing both staff and board members which set clear expectations for the highest standards of integrity, define acceptable business practices and strictly prohibit conflicts of interest or the inappropriate provision of financial services. The Board shall regularly review and approve the policy, requiring mandatory employee attestation. Implementation must be overseen by a Senior Ethics Committee or an equivalent board-level body, and the document must be publicly accessible (e.g., via the institution's website). Additionally, specialized codes of conduct may be adopted for specific high-risk roles, such as treasury dealers or senior management.

(b) appoint senior management with appropriate expertise and integrity, oversee their performance in implementing the operational risk framework, and take corrective action, including dismissal, where risk management objectives or policies are not met.

(c) ensure senior management implements a sound third-party risk management program. In addition, the board shall provide appropriate oversight, reporting and an independent review mechanism to address outsourcing-related risks and dependencies.

(d) approve the business resilience and continuity plan of an institution and review them periodically to ensure that they remain aligned with the institution's operational risk appetite, risk profile, and critical business functions. Moreover, these plans should be tested periodically to ensure that the institution can execute the plans in the unlikely event of a severe business disruption.

(e) approve and periodically review the core policies, including remuneration and compensation policies that support a strong risk management culture of an institution. The remuneration and compensation policies shall be aligned with the institution's risk appetite and tolerance limits.

(f) approve disclosure policy of its operational risk management framework that allows stakeholders to assess whether the institution effectively identifies, assesses, monitors and mitigates operational risk. The amount and type of disclosure shall be commensurate with the size, complexity and risk profile of an institution's operations and evolving industry practice.

(g) ensure that the institution's operational risk management framework is subject to independent, objective and periodic assessment, which may be conducted by Internal Audit function or independent experts, covering the effectiveness of operational risk policies, controls and processes.

(h) receive and make deliberation on operational risk reports from senior management, which are comprehensive, accurate, consistent and actionable across business units and products. Reports shall reflect the outlook on the institution's operational risk profile and adherence to the operational risk appetite and tolerance statement to enable effective decision-making. At a minimum, operational risk reports shall include:

3.4. Senior Management

3.4.1. Senior Management plays a critical role in ensuring that the operational risk management framework approved by the Board of Directors is fully embedded into the institution's strategic objectives, day-to-day operations, and internal control environment.

3.4.2. Senior management shall be responsible for ensuring that operational risk is effectively managed across the institution. At a minimum, senior management shall:

(a) implement the operational risk management framework approved by the Board of Directors by translating it into clear, effective, and robust policies, processes and procedures that are enforceable and verifiable across all business units.

(b) Develop robust governance structure that assign authority, responsibility and reporting relationships throughout the institution, thus embedding accountability and ensuring adequate resources are provided to manage operational risk in line with the

institution's risk appetite and tolerance limits. The governance structure shall be submitted to board for approval prior to implementation.

(c) implement and maintain institution policies, processes and systems for managing operational risk across all material products and activities, ensuring alignment with the institution's risk appetite and tolerance.

(d) advise the Board on operational risk strategies, policies and plans, and ensure that the policies, processes and systems remain sufficiently robust to manage and ensure that operational losses are adequately addressed in a timely manner.

(e) establish and maintain robust challenge mechanisms and effective issue-resolution processes. These should include systems to report, track and, when necessary, escalate issues to ensure resolution.

(f) ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those within the institution who are responsible for the procurement of external services such as insurance risk transfer and other third-party arrangements (including outsourcing).

(g) review and deliberate on operational risk reports received from all business units, including key risk indicators, operational incidents, and control effectiveness, to assess the institution's operational risk profile.

(h) provide timely, accurate and comprehensive operational risk reports to the Board or board committee for effective oversight and decision making. This includes providing the Board with comprehensive information on the institution's operational risk profile, emerging risks, mitigation actions, and the overall effectiveness of the operational risk management framework.

(i) ensure that institution activities are conducted by staff with the necessary experience and technical capabilities.

(j) implement directives and recommendations as well as resolving weaknesses or findings provided by oversight functions, including regulatory authorities, external audit, internal audit and risk management.

(k) ensure outsourcing arrangements and third-party relationship are properly governed, monitored and integrated in the institution's operational risk management framework.

Also, senior management shall ensure that contingency and exit plans for critical outsourced function are in place.

(l) ensure that the institution's change management process is comprehensive, appropriately resourced and includes continuous risk and control assessment, adequately articulated between the relevant lines of defence. As operational risk evolves with new activities, products, process modifications or technology systems, this process must assess associated risks throughout the initiative's entire lifecycle, from inception to termination.

(m) Establish and maintain a comprehensive complaint-handling mechanism that ensures operational risks related to customer complaints are effectively managed. Senior Management shall be responsible for embedding this process across the organization, monitoring trends, and using insights from complaints to strengthen controls, improve processes and mitigate future operational risks.

(n) establish and maintain comprehensive, effective operational risk tools that support proactive identification, assessment, monitoring, and mitigation of operational risk. The tools shall be embedded within business processes, promoting a strong risk culture, and ensuring that operational risk information is accurate, timely and escalated appropriately.

(o) implement a robust ICT risk management programme aligned with the operational risk management framework. Strong ICT infrastructure performance and security are essential to a sound control environment and critical for successful business operations.

(p) establish business continuity plans to ensure operational resilience and minimize losses during severe business disruptions. These plans shall be fully integrated with the bank's operational risk management framework.

3.4.3. **Risk measurement and Tools**

3.4.3.1. Tools that may be used by institutions for identifying and assessing operational risk include:

(i) **Self-Risk Assessment:** The assessment evaluates inherent risk, the effectiveness of the control environment and residual risk as well as quantitative and qualitative elements. A risk register can be maintained to collate this information to form a meaningful view of the overall effectiveness of

controls and facilitate oversight by senior management, risk committees, and the board.

(ii) **Risk Indicators/Metrics:** These metrics may be simple indicators, such as event counts, or result from more sophisticated exposure models when appropriate. Metrics provide early warning information to monitor ongoing performance of the business and the control environment, and to report the operational risk profile. Effective metrics clearly link to the associated operational risks and controls. Monitoring metrics and related trends over time against agreed thresholds or limits provides valuable information for risk management and reporting purposes.

(iii) **Risk Mapping:** in this process, various business units, institution functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritize subsequent management actions.

(iv) **Event management:** When institutions experience an operational risk event, the process of identification, analysis, end-to-end management and reporting of the event follows a predetermined set of protocols. A sound event management approach typically includes analysis of events to identify new operational risks, understanding the underlying causes and control weaknesses, and formulating an appropriate response to prevent recurrence of similar events. This information is an input to the self-assessment and, in particular, to the assessment of control effectiveness.

(v) **Scenario Analysis:** Institutions may use structured scenario analysis to evaluate the potential impact of extreme but plausible operational risk events. This involves identifying hypothetical events, estimating their frequency and severity, and assessing the effectiveness of existing controls. Scenario analysis can help management prepare contingency plans, strengthen internal controls, and prioritize risk mitigation efforts.

(vi) **Benchmarking and comparative analysis:** Benchmarking and comparative analysis are comparisons of the outcomes of different risk measurement and management tools deployed within the institution. Such comparisons can be performed to enhance understanding of the institution's operational risk profile. For example, comparing the frequency and severity of internal losses with self-assessments can help an institution determine whether its self-assessment

processes are functioning effectively. Scenario data can be compared to internal and external loss data to gain a better understanding of the severity of an institution's exposure to potential risk events.

(vii) **Event database:** The use of data on an institution's historical loss experience could provide meaningful information for assessing the institution's exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events. Institutions may also combine internal loss data with external loss data (from other institutions), scenario analyses, and risk assessment factors.

3.5. Operations Management

3.5.1. Operations Management refers to the business units and front-line staff who own and manage operational risk on a day-to-day basis. This is the first line of defence in operational risk management by an institution. They are responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which they are accountable. Institutions shall have a policy that defines clear roles and responsibilities in relevant business units. At a minimum, the business units shall:

(a) identify and assess the materiality of operational risks inherent in their respective business units through the use of operational risk management tools;

(b) advising senior management on establishment of appropriate and effective controls to mitigate inherent operational risks;

(c) reporting whether the business units lack adequate resources, tools and training to ensure identification and assessment of operational risks;

(d) monitoring and reporting the business units' operational risk profiles, and ensuring their adherence to the established operational risk appetite and tolerance statement.

(e) reporting operational incidents and control breaches promptly to the Risk Management function. Maintain operational risk registers and ensure data is complete and accurate.

(f) Implementing clearly defined workflows, segregation of duties, authorization controls, reconciliation processes, incident management procedures, and escalation

mechanisms. These measures support sound operational discipline and minimize the likelihood of errors, fraud, service disruptions, and control failures

(g) ensuring that operational activities are supported by a reliable Management Information System (MIS), competent personnel, and adequate technological infrastructure to maintain service quality and operational continuity.

(h) monitoring of key risk indicators, address control deficiencies in a timely manner, and maintain complete and accurate operational records to support transparency and accountability.

(i) perform operational risk and control assessments of new products, activities, processes and systems, including the identification and evaluation of the required change through the decision-making and planning phases to the implementation and post-implementation review.

3.5.2. Operations management shall ensure that operational-risk decisions are supported by comprehensive, relevant, reliable, and timely information. This includes internal data (financial, operational, and compliance) and relevant external information (market events, regulatory developments, and emerging threats). Information must be accessible to the relevant staff and sufficiently detailed to support effective risk identification, monitoring, and mitigation, as well as reporting to the second line and senior management.

3.6. Risk Management

3.6.1. Risk management function as a second line of defence, has the responsibility of providing independent oversight, guidance and challenge to operational units. The function shall be responsible for systematically identifying and assessing operational risks, measuring the institution’s exposure, and monitoring the effectiveness of controls.

3.6.2. The Risk management function shall be adequately staffed and equipped with necessary expertise, tools and resources to effectively oversee the operational risk management framework. The function must ensure continuous monitoring of the operational risk profile. For effective management of operational risk in an institution. At a minimum, risk management function shall:

(a) independently oversee, monitor and challenge operational risks in business units and enterprise-wide, including identified material operational risk, design and effectiveness of key controls and risk tolerance.

(b) ensure that the risk policies, appetite and tolerance levels are clearly communicated and applied across the institutions.

(c) provide timely, accurate and comprehensive reports on key operational risk issues, emerging risks, control gaps and recommended mitigations actions to Senior management and the Board or the relevant Board committee.

(d) challenge relevance and consistency of the business unit's implementation of the operational risk management tools, measurement activities and reporting systems, and provide evidence.

(e) provide inputs in developing and maintaining operational risk management policies, and guidelines.

(f) review and contribute to the monitoring and reporting of the operational risk profile.

(g) designing and providing operational risk training and instilling risk awareness

(h) ensure that the institution maintains a reliable Management Information System (MIS) capable of generating accurate, timely, and relevant reports to support the monitoring and control of operational risks. The MIS must generate early-warning indicators, red flags, and trigger alerts to facilitate the prompt identification of breaches and emerging risks, thereby supporting effective monitoring and control of operational risk.

(i) verify that outsourcing activities are undertaken in full compliance with regulatory requirements and internal approval processes, including due diligence, risk assessment and contractual safeguards.

3.7. Internal Audit

3.7.1. The Internal Audit function serves as the third line of defence in the management of operational risk and plays a critical role in providing an independent assurance to the board and senior management. Internal audit evaluates the effectiveness of the operational risk management framework, verifies that operational risks are properly identified, assesses, monitored and mitigated and ensures that the first and second lines of defence are operating in accordance with the institution's policies, risk appetite and regulatory requirements.

3.7.2. An institution shall have an Internal Audit Charter that clearly defines the authority, responsibilities, and scope of the internal audit function. The charter shall ensure that internal audit function operates independently, has direct reporting lines to the board or audit committee, and possesses unrestricted access to records, personnel, and processes

necessary to assess the effectiveness of governance, risk management, and internal controls, including operational risk management. This access includes information held by business units, support functions, and any third-party or outsourced service providers. At minimum the internal audit function shall:

(a) evaluate the design, implementation, and effectiveness of the institution's operational risk management framework, including policies, procedures, controls and risk monitoring processes.

(b) report directly to the Board or Audit Committee on operational risk matters.

(c) provide timely, accurate and comprehensive reports on operational risk exposures, control effectiveness, emerging risks, and significant issues requiring corrective actions.

(d) review operational risk management practices related to outsourcing and critical third party services.

(e) track and monitor the implementation of recommendations arising from internal audits, external audits, and supervisory authority reviews related to operational risk. This includes ensuring that business units responds to raised issues promptly, accurately, and adequately, and that regular reports are provided to the Board of Directors or its relevant committees on both pending and resolved matters.

(f) review the design and implementation of operational risk management systems and governance processes across the first and second lines of defense, including an assessment of the second line's independence.

(g) review validation processes to ensure they are independent and implemented in a manner consistent with established institution policies.

(h) ensure that an institution's quantification systems are sufficiently robust to guarantee the integrity of inputs, assumptions, processes, and methodologies, and produce operational risk assessments that accurately reflect the institution's risk profile.

(i) develop and implement a risk-based audit plan that adequately covers all areas posing significant operational risk. The audit plan must define an appropriate scope and frequency of reviews, ensuring higher-risk areas are assessed more frequently and comprehensively.

4.0. LIQUIDITY RISK MANAGEMENT

4.1. Introduction

4.1.1. Liquidity risk is the potential for loss to an institution arising from either its inability to meet its obligations as they fall due or to fund increases in assets without incurring unacceptable cost or losses.

4.1.2. Liquidity risk is considered a major risk for an institution. It arises when the liquid assets are not sufficient to meet maturing obligations. In such a situation, an institution often meets its liquidity requirements from the market which depends upon liquidity in the market and the creditworthiness of an institution. Accordingly, an institution short of liquidity may have to undertake transactions at heavy cost resulting in a loss of earnings or in worst-case scenario, the liquidity risk could result in insolvency of the institution if it is unable to undertake transactions even at current market prices.

4.1.3. Liquidity risk shall not be assessed in isolation, as risks are not mutually exclusive. Liquidity risk is often triggered by consequences of other risks such as credit, interest rate and foreign exchange risks. For instance, an institution increasing its credit risk through asset concentration may be increasing its liquidity risk as well. Similarly, a large loan default or changes in interest rate can adversely impact an institution's liquidity position. Further, if management misjudges the impact on liquidity of entering into a new business or product line, the institution's strategic risk would increase.

4.2. Management of Liquidity Risk

4.2.1. Liquidity risk management involves analyzing institution's on and off-balance sheet positions to forecast future cash flows, as well as how the funding requirement would be met. The latter involves identifying the funding market the institution has access to, understanding the nature of those markets, evaluating institution's current and future use of the market and monitoring signs of confidence erosion.

4.2.2. The formality and sophistication of risk management processes established to manage liquidity risk shall reflect the nature, size and complexity of an institution's activities. Sound liquidity risk management employed in measuring, monitoring and controlling liquidity risk is critical to the viability of any institution. An institution shall have a thorough understanding of the factors that could give rise to liquidity risk and put in place mitigating controls.

4.2.3. An incipient liquidity problem can be initially revealed in the institution's financial monitoring system as a downward trend with potential long-term consequences for

earnings or capital. Early warning indicators do not always lead to a liquidity issue, but they can trigger a liquidity problem. Management shall monitor early warning indicators closely and conduct further analysis as needed. Early warning indicators can be qualitative or quantitative in nature and may include, but are not limited to:

(a) Negative trends or heightened risk associated with a particular product line or any risk area;

(b) Growing concentrations in assets or liabilities;

(c) Significant deterioration in the institution's earnings, asset quality, and overall financial condition;

(d) Increasing retail deposit outflow;

(e) Rapid asset growth funded by volatile large deposit;

(f) A large off-balance sheet exposure;

(g) Heavy reliance on large corporate deposits; and

(h) Deteriorating creditworthiness of the institution.

4.2.4. Effective liquidity risk management enables an institution to better understand and mitigate its risk profile, and it reflects the effectiveness of oversight functions specifically the board of directors, senior management, operations management, risk management, and internal audit in fulfilling their responsibilities.

4.3. Board of Directors

4.3.1. Effective board of directors' oversight is a critical element of an institution's liquidity risk management framework. The board holds ultimate responsibility for liquidity risk management and is charged with establishing the institution's risk tolerance. To fulfil these responsibilities, the board shall have an appropriate mix of skills, qualifications, expertise, and depth of understanding sufficient to effectively oversee the institution's liquidity risk management activities. At minimum, the board shall:

(a) develop, approve and oversee implementation of the institution's liquidity risk management framework including strategy, policies, risk appetite and limits, ensuring they are consistent with the institution's overall business strategy and risk profile.

(b) approve a comprehensive liquidity risk governance framework, including clearly defined roles, responsibilities, and lines of authority for managing liquidity risk across the institution.

(c) approve and regularly review the Contingency Funding Plan (CFP), ensuring it contains clear triggers, roles and responsibilities, funding options and communication strategies, and that it is periodically tested for effectiveness.

(d) approve methodologies and assumptions used to identify, measure, monitor and control liquidity risk, including those covering on and off-balance sheet exposures, intraday liquidity risk and liquidity risk across different currencies.

(e) appoint senior management with appropriate expertise and integrity, oversee their performance in implementing the liquidity risk framework, and take corrective action, including dismissal, where risk management objectives or policies are not met.

(f) approve the Internal Liquidity Adequacy Assessment Process (ILAAP) framework and ensure it is well integrated into business and strategic plans, management processes and the institution's decision-making culture.

(g) Periodically review and deliberate reports from senior management to understand and assess the performance of senior management in monitoring and controlling liquidity risk management.

(h) ensure periodic independent review of liquidity risk management framework is conducted, covering the:

(i) Effectiveness of risk management and compliance functions

(ii) Quality and adequacy of reporting to the board and senior management

(iii) Reliability of Management Information Systems (MIS) and internal controls

(iv) control systems to identify and prevent internal control deficiencies including segregation of duties and delegation of authority; and

(v) timely and effective remediation of audit and supervisory findings.

4.3.2. **Liquidity Strategy**

4.3.2.1. An institution shall have a documented strategy for the day-to-day management of liquidity. The liquidity strategy shall be set out in a liquidity policy and communicated throughout the institution. It shall be evaluated periodically to ensure that it remains valid and aligned with the institution's risk profile and operating environment. The strategy shall outline the general approach to liquidity management, including goals and objectives, as well as specific aspects of liquidity management such as:

(a) Composition of assets and liabilities: The strategy shall outline the mix of assets and liabilities to maintain liquidity. Liquidity risk management and

asset/liability management shall be integrated to avoid high costs associated with having to rapidly reconfigure the asset liability profile from maximum profitability to increased liquidity.

(b) Diversification and stability of liabilities: A funding concentration exists when a single decision or a single factor has the potential to result in a significant and sudden withdrawal of funds. Since such a situation could lead to an increased risk, the board of directors and senior management shall specify guidance relating to funding sources and ensure that the institution has diversified sources of funding day-to-day liquidity requirements. An institution would be more resilient to tight market liquidity conditions if its liabilities were derived from more stable sources.

(c) Managing liquidity in different currencies: The institution shall have a strategy for managing liquidity in different currencies.

(d) Dealing with liquidity disruptions: The institution shall put in place a strategy on how to deal with the potential for both temporary and long-term liquidity disruptions. The strategy shall consider the fact that in crisis situations access to the interbank market could be difficult as well as costly.

4.3.3. **Liquidity Policies**

4.3.3.1. An institution shall have in place sound, comprehensive, and clearly defined liquidity policies, processes, and procedures that are consistent with prudent standards, practices, and relevant regulatory requirements, and are commensurate with the size, complexity, and scope of the institution's operations. The policy shall be reviewed at least annually to reflect changes in the institution's risk profile, business activities, and prevailing market conditions. At a minimum, the policy shall:

(a) prescribe the institution's liquidity risk appetite, including limits and tolerances, and specify management procedures and approval authorities for policy exceptions;

(b) prescribe 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);

(c) delineate the lines of authority and the responsibilities of the personnel responsible for managing liquidity risk;

(d) prescribe a general liquidity strategy (short- and long-term), in relation to liquidity risk management, process for strategy formulation and the level within the institution it is approved;

(e) Include a contingency plan for handling liquidity crises

(f) indicate the content and frequency of management reports submitted to the board and senior management on interest rate risk management. At a minimum, the report to the Board shall include:

i. levels of liquidity compared to established targets and resultant variance analysis;
ii. alternative funding sources and funds available, including lines of credit and stand-by facilities, and associated costs
iii. a cash flow analysis highlighting short-term liquidity needs;
iv. structure, level and trend of assets and liabilities;
v. level and trend of liquidity ratios;
vi. undrawn commitments;
vii. limit breaches;
viii. stress testing results;
ix. status and effectiveness of Contingency Funding Plan (CFP);
x. computation of cost of funds and yield on assets;
xi. maturity gap analysis;
xii. implementation status of the findings of internal and external auditors and regulatory authorities.

4.3.4. **Liquidity Risk Management Tools**

4.3.4.1. An institution shall have a sound process for identifying, measuring, monitoring and controlling liquidity risk. This process shall include a robust framework for comprehensively projecting cash flows arising from assets, liabilities and off-balance sheet items over an appropriate set of time horizons.

4.3.4.2. An institution shall use a range of liquidity metrics for identifying, measuring, and analyzing liquidity risk. The metrics shall enable the institution to understand its day-today liquidity positions and structural liquidity mismatches, as well as its resilience under stressed conditions. An institution shall use metrics and tools that are appropriate for the nature of its business, size, complexity, and risk profile. The metrics discussed in this section include the following:

(a) Contractual maturity mismatch

(b) Concentration of funding

(c) Available unencumbered assets

(d) Liquidity Coverage Ratio by significant currency

(e) Market-related monitoring tools

4.3.5. **Contingency funding plans (CFP)**

4.3.5.1. An institution shall have a contingency funding plan (CFP) that clearly sets out the strategies for addressing liquidity shortfalls under stress scenarios. The strategies shall address liquidity and funding shortfalls to the extent beyond the levels estimated from the stress tests performed by the institution under institution-specific, market-wide and combined stress scenarios and beyond the level covered by the institution's liquidity cushion.

4.3.5.2. Further, the CFP shall outline procedures to manage a range of stress environments, establish clear lines of responsibility, include clear invocation and escalation procedures and be regularly tested and updated to ensure that it is operationally robust. Internal procedures for liquidity stress management shall cover:

(a) The authority to invoke the CFP and the establishment of a formal 'crisis management team' to facilitate internal coordination and communication across different business lines and locations, and decision-making by senior management in a stress situation;

(b) Clear escalation and prioritization procedures detailing what actions to take, who can take them, and when and how each of the actions can and should be activated;

(c) Names and contact details of members of the team responsible for implementing the CFP and the locations of team members; and

(d) The designation of alternates for key roles.

4.3.5.3. The CFP shall be commensurate with the institution's complexity, risk profile, scope of operations and its systemic importance in the financial system. The design of the CFP, including its action plans and procedures, shall be closely integrated with the institution's ongoing liquidity risk analysis. The CFP shall address liquidity issues over a range of different time horizons.

4.3.5.4. The CFP shall prescribe a diversified set of viable, readily deployable potential contingency funding measures for preserving and making up liquidity shortfalls in

emergency situations. All available potential sources of funding shall be outlined, along with the estimated amount of funds that can be derived from these sources, their expected degree of reliability, under what conditions these sources shall be used, and the lead time needed to access additional funds from each of the sources. Contingency funding measures identified in the CFP shall take into consideration the following factors:

(a) The impact of stressed market conditions on an institution's ability to raise funding through different sources;

(b) The interaction between asset markets and funding liquidity, especially in situations where there is an extensive or complete loss of typically available market funding options;

(c) Any second-round effects, as well as reputation, legal, regulatory and operational constraints, related to the execution of such measures;

(d) Any peculiarities (including special terms and conditions) associated with particular funding sources; and

(e) Operational procedures needed to transfer liquidity, collateral across group entities, borders and business lines, taking into account legal, regulatory, operational, time zone restrictions, and controls governing such transfers.

4.4. Senior Management

4.4.1. Senior management is responsible for the implementation of sound policies and procedures, keeping in view the strategic direction and risk appetite specified by the board. To effectively oversee the daily and long-term management of liquidity risk, at a minimum senior management shall:

(a) develop and implement operating standards and procedures in line with the approved policies, strategy, risk appetite, limits and risk tolerances, and ensuring they are clearly understood by staff and consistently applied across the institution.

(b) ensure that daily and intraday liquidity risk management practices operate within board approved strategies and policies.

(c) ensure that personnel responsible for liquidity risk management have adequate expertise, experience, and sufficient staffing resources are allocated to effectively carry out their responsibilities

(d) ensure that all liquidity risk management activities and decisions remain aligned with the board’s risk appetite and governance expectations, including regulatory

liquidity metrics such as the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR), and take timely corrective action where deviations, breaches or emerging risks are identified.

(e) oversee the implementation, maintenance, and effectiveness of Management Information Systems (MIS), models and analytical tools used to identify, measure, monitor, and control liquidity risk across the institution, currencies, and business lines, including intraday liquidity risk.

(f) establish and maintain effective internal controls over the liquidity risk management framework, ensuring segregation of duties, independent monitoring, appropriate escalation mechanisms and clear communication of roles and responsibilities to all staff.

(g) promptly identify, assess, and effectively address existing and potential liquidity risk threats, including taking corrective actions to mitigate emerging vulnerabilities, market disruptions, funding concentration risk and adverse stress-testing outcomes.

(h) ensure that liquidity risk monitoring reports are comprehensive, accurate, timely and contain all information necessary to support effective oversight decision-making and regulatory compliance.

(i) ensure the establishment, regular testing and ongoing maintenance of an effective contingency Funding Plan (CFP) that set out clear triggers, roles and responsibilities, funding sources and communication strategies to address institutions specific and market wide liquidity stress events.

(j) put in place an effective mechanism for the prompt and adequate resolution of findings raised by oversight functions, including risk management, compliance, internal audit, and regulators, and ensure that remediation actions are tracked, completed, and validated.

(k) develop and implement the Board-approved Internal Liquidity Adequacy Assessment Process (ILAAP), as well as ensure ongoing appropriateness of the ILAAP, maintain an understanding of its design and operation, and provide regular reports on the institution's ILAAP to the Board.

4.4.2. **Liquidity Management Structure**

4.4.2.1. The responsibility for managing the overall liquidity of the institution shall be delegated to a specific function or an identified committee within the institution. This may take the

form of an Asset Liability Committee (ALCO) comprising senior management or the treasury function.

4.4.2.2. Liquidity management requires specialized knowledge and expertised, it is important that responsible officers not only have relevant expertise but also have a good understanding of the nature and level of liquidity risk assumed by the institution and the means to manage that risk.

4.4.2.3. It is critical to maintain close coordination between those individuals responsible for liquidity and those monitoring market conditions, as well as other individuals with access to critical information. This is particularly important in developing and analyzing stress scenarios.

4.5. Operations Management

4.5.1. As the first line of defense, Operations Management is responsible for the ownership and day-to-day management of liquidity risks within the institution. This includes planning, directing, and controlling operational activities and business lines in accordance with policies and procedures approved by the Board of Directors.

4.5.2. Operations Management shall ensure that operational controls are robust, and resources are adequate to identify, monitor, and mitigate inherent liquidity risks in line with the approved policies. Operations Management supports the implementation of the liquidity risk framework by ensuring compliance with internal standards and regulatory requirements, and contributing to the safety, soundness, and resilience of the institution's liquidity position. At a minimum, the operations management function shall:

(a) identify, measure, and control material liquidity risks at all levels of the institution, including structural, intraday, and contingent risks.

(b) maintain segregation of duties across front, middle, and back-office treasury function, with clear approval hierarchies and ensure conflict of interest are identified, mitigated, and monitored.

(c) Implement and maintain robust, reliable, comprehensive, and secure Management Information System (MIS) for liquidity risk monitoring.

(d) Operate adequate tools and processes for periodic liquidity risk monitoring, including stress testing and scenarios analysis, to capture emerging or evolving risk.

(e) Actively manage liquidity positions in individual and aggregate major currencies, ensuring sufficient liquidity under normal and stressed conditions.

(f) monitor regulatory compliance and reporting, including Liquidity Coverage Ratio, Net Stable Funding Ratio and other supervisory requirements.

4.5.3. **Liquidity Risk Measurement and Monitoring**

4.5.3.1. An effective measurement and monitoring process is essential for adequately managing liquidity risk. At a very basic level, liquidity measurement involves assessing all an institution's cash inflows against its outflows to identify the potential for any net shortfalls going forward, including funding requirements for off-balance sheet commitments. A few techniques can be used for measuring liquidity risk, ranging from simple gap calculations to sophisticated modelling.

4.5.3.2. An institution shall track and evaluate its current and anticipated liquidity position and capacity to fund potential gaps. A monitoring system shall consist of limits, guidelines and trend analysis that enable management to monitor compliance with approved risk tolerances and track variances.

4.5.3.3. Effective liquidity risk monitoring shall be supported by clear reporting criteria that define the scope, format, responsible parties, and frequency of liquidity risk reports. Liquidity reports can be submitted on a daily, weekly, and monthly basis, as appropriate, to those responsible for managing liquidity risk, and presented to senior management, the Board, or its relevant delegated committee(s).

4.5.4. **Management Information Systems**

4.5.4.1. Effective Management Information Systems (MIS) shall be able to measure, monitor, control and report liquidity risk under normal and stressed situations. The MIS shall encompass all significant aspects of liquidity risk, including those associated with new products and business initiatives, and be capable of evaluating their effect on cash flows and liquidity ratios. In particular, the MIS shall be capable of:

(a) analyzing cashflows and maturity mismatch positions in all major currencies, both individually and on an aggregate basis arising from the full range of an institution's assets, liabilities and off-balance sheet positions on a day-to-day basis; and

(b) monitoring various limits and ratios in relation to liquidity for both statutory and internal risk management purposes, as well as generating exception reports; and

4.5.5. **Managing Market Access**

4.5.5.1. An institution shall maintain an active presence in funding markets relevant to its funding strategies through adequate processes and information systems. It shall regularly test its ability to access these markets by using established arrangements and documentation,

estimate its normal borrowing capacity, particularly, in the interbank market and limit reliance on wholesale funding in both local and foreign currencies. Strong, continuous relationships with funding providers, especially major depositors, are essential to support timely access to liquidity when needed.

4.5.5.2. An institution shall take a prudent and forward-looking view of funding vulnerabilities under stress situations. Stress scenarios and contingency funding plans shall assume that key funding sources, including large depositors, may withdraw and markets may become inaccessible. These plans shall also consider how adverse market perceptions and capital erosion during stress could weaken counterparties' willingness to provide funding, recognizing the role of a strong capital position in sustaining funding relationships.

4.5.6. **Intraday Liquidity Management**

4.5.6.1. An institution shall actively manage its intraday liquidity positions and risks to meet payment and settlement obligations on a timely basis under both normal and stressed conditions and thus contribute to the smooth functioning of payment and settlement systems.

4.5.6.2. An institution may also incur intraday liquidity risk through its provision of correspondent and custodian banking services. Where an institution relies on other correspondent or custodian banks to conduct payment and settlement activities, operational or financial disruptions at those banks will also affect the bank's own liquidity position and it should have alternate arrangements in place to ensure it is able to meet its obligations.

4.5.6.3. A key challenge in intraday liquidity risk management lies in the uncertainty in both the amount and timing of a bank's gross cash inflows and outflows during the day, in part because such cash flows may reflect the activities of its customers or counterparties, which are beyond the bank's control, especially where the bank provides correspondent or custodian services.

4.6. Risk Management

4.6.1. The risk management function as the second line of defense shall provide independent, enterprise-wide oversight over the first line's operational management. It shall design and implement robust internal controls and risk systems; develop and enforce comprehensive liquidity risk frameworks; define policies and procedures; and build risk-measurement tools (e.g., stress-testing models) and early-warning mechanisms with defined risk-tolerance thresholds.

4.6.2. The second line of defense shall continuously monitor liquidity exposures, ensure alignment of all material risks with business strategy and approved risk appetite, and escalate any serious breaches to Senior Management and the Board (or their delegated Committees). At minimum, the risk management function shall:

(a) Maintaining adequate skills, expertise and depth of understanding to conduct daily liquidity risk oversight effectively.

(b) remain independent from business lines that take liquidity risk or generate revenue, to preserve objectivity in risk oversight.

(c) continuously monitor risk taking activities related to liquidity and assessing the effectiveness of processes for identifying, measuring and managing liquidity risk.

(d) develop and monitor implementation of the enterprise-wide risk governance frameworks including policies, limits, risk appetite definitions and controls standards subject to board review and approval.

(e) maintain a reliable Management Information System (MIS) capable of generating accurate and timely reports for liquidity risk control, including adherence to internal limits and regulatory requirements. The reports shall include early warning, red flags or triggers to monitor breaches of liquidity limits.

(f) monitor and apply macroeconomic variables and market trends such as inflation, interest rates, exchange rates, fiscal or monetary policy shifts that might affect liquidity and assessing their impact on the institution's liquidity risk.

(g) conduct regular liquidity stress testing using credible assumptions about future funding needs and defining contingency or remedial measures to address potential liquidity shortfalls.

4.7. Internal Audit

4.7.1. The internal audit function plays a critical role in ensuring sound liquidity risk management within the banking institution. Serving as the third line of defense, internal audit provides independent oversight, evaluating both the effectiveness of liquidity-risk-related controls and the institution's adherence to established organizational and procedural requirements. Unlike the second line of defense, internal audit operates with the highest level of independence, enabling it to deliver objective assurance on the adequacy and performance of the first and second lines of defense.

4.7.2. An institution shall have an Internal Audit Charter that clearly defines the authority, responsibilities, and scope of the internal audit function. The charter shall ensure that the

internal audit function operates independently, has direct reporting lines to the board or audit committee, and possesses unrestricted access to records, personnel, and processes necessary to assess the effectiveness of governance, risk management, and internal controls, including liquidity risk management.

4.7.3. For effective management of liquidity risk, the internal audit function shall:

(a) provide independent, objective and risk-based assurance to the board and senior management on the adequacy, effectiveness, and integrity of the institution's liquidity risk management framework, including governance, risk appetite, strategies, policies, processes, systems, models, data, assumptions, reporting, and internal controls.

(b) ensure the function maintains sufficient authority, professional competence, and resources to assess liquidity risk management practices effectively. Audit staff shall possess appropriate expertise in liquidity risk, treasury and funding activities, liquidity stress testing, financial markets, model risk and relevant regulatory standards.

(c) establish and implement a risk-based audit plan that covers all material aspects of liquidity risk management, ensuring that all significant risk areas are reviewed as planned and emerging or evolving liquidity risks arising from market conditions new products or strategic changes are appropriately assessed. The scope and frequency of audits shall be commensurate with the institution's risk profile and complexity.

(d) assess the design, implementation, and effectiveness of liquidity risk models, stress testing frameworks, behavioural assumptions, management overlays, and related governance and validation processes.

(e) prepare and submit audit reports to the Board or Audit committee on liquidity risk management, highlighting material deficiencies, control weaknesses, governance issues, and regulatory concerns, together with prioritized and actionable recommendations.

(f) track and monitor the implementation of recommendations arising from internal audits, external audits, and supervisory authority reviews related to liquidity risk. This includes ensuring that business units respond to raised issues promptly, accurately, and adequately, and that regular reports are provided to the Board of Directors or its relevant committees on both pending and resolved matters.

5.0. INTEREST RATE RISK MANAGEMENT

5.1. Introduction

5.1.1. Interest rate risk refers to exposure of an institution's financial condition resulting from adverse movements in interest rates.

5.1.2. While institutions are exposed to interest rate risk in both the trading and banking books, a clear distinction between the two is essential. Institutions must document and disclose their policies for assigning instruments to either book. Once designated, instruments generally cannot be reclassified; switching is permitted only in exceptional circumstances and remains subject to the Bank’s approval.

5.1.3. Changes in interest rates may have adverse effects to both an institution’s earnings and its economic value. Changes in interest rate risk affect the underlying value of an institutions’ rate-sensitive assets, liabilities, and off-balance sheet items and hence, their economic value. This has given rise to two separate, but complementary perspectives of earnings and economic value for assessing an institution's interest rate risk exposure.

5.1.4. The earnings perspective provides short-term perspective and focuses on the impact of changes in interest rates on accrued or reported earnings. Variation in earnings is an important focal point for interest rate risk analysis because reduced earnings or outright losses can threaten the financial stability of an institution by undermining its capital adequacy and reducing market confidence. An institution shall assess the impact of interest rate changes on net interest income and activities that generate fee-based and other non-interest income such as loan servicing and asset securitization, which can be highly sensitive to interest rates.

5.1.5. Variation in market interest rates can also affect the economic value of an institution's assets, liabilities, and off-balance sheet positions. The economic value of an instrument represents an assessment of the present value of its expected net cash flows, discounted to reflect market rates. Economic value perspective reflects one view of the sensitivity of the net worth of the institution to fluctuations in interest rates. Under the economic value perspective, an institution shall assess the potential long-term effects of changes in interest rates on their overall position.

5.1.6. Interest rate risk is often interconnected with other risks such as credit and liquidity risks. For example, increased defaults among borrowers necessitates the institution to increase provisions for loan losses. In order to maintain capital adequacy, the institution may need to raise additional funds at higher interest rates. Likewise, insufficient liquidity can require a institution to borrow at unfavourable rates, resulting to increased costs.

5.1.7. There are four sub-types of interest rate risk which potentially change the price or /value or earnings/costs of interest rate sensitive assets, liabilities and/or off-balance sheet items in a way, or at a time, that can adversely affect an institution's capital and earnings. The primary forms of interest rate risk to which institutions are typically exposed includes:

(a) Repricing risk: This is a form of interest rate risk arising from timing differences in the maturity (for fixed-rate) and repricing (for floating-rate) of institution assets, liabilities, and off balance sheet positions. Repricing mismatches can expose an institution's income and underlying economic value to unanticipated fluctuations in interest rates. For instance, an institution that funded a long-term fixed-rate loan with a short-term deposit could see both the future income from the position and its underlying value decline if interest rates increase. These declines arise because the cash flows on the loan are fixed over its lifetime, while the interest paid on the funding is variable, and increases after the short-term deposit matures.

(b) Yield curve risk: This is a form of interest rate risk arising from unanticipated shifts of the yield curve, which may have adverse effects on an institution's income or underlying economic value. For instance, the underlying economic value of a long position in 10-year Government bonds hedged by a short position in 5-year Government notes could decline sharply if the yield curve steepens, even if the position is hedged against parallel movements in the yield curve.

(c) Basis risk: This is a form of interest rate risk arising from imperfect correlation in the adjustment of the rates earned and paid on different instruments with otherwise similar repricing characteristics. When interest rates change, these differences can give rise to unexpected changes in the cash flows and earnings spread between assets, liabilities and off balance sheet instruments of similar maturities or repricing frequencies.

(d) Option risk: This is a form of interest rate risk arising from option derivative positions or from optional elements embedded in a institution's assets, liabilities and/or off-balance sheet items, where the bank or its customer can alter the level and timing of their cash flows. Option risk can be further characterized into automatic option risk and behavioural option risk.

5.2. Management of Interest Rate Risk

5.2.1. An institution shall establish a comprehensive management framework for interest rate risk. The framework shall be clearly documented and commensurate with the nature, size, and complexity of the institution's operations. It shall clearly define roles and

responsibilities for monitoring interest rate risk exposures against approved limits, authority to approve any variations to those limits, and procedures for escalating any breaches. The management of interest rate risk shall be integrated within an institution's overall risk management framework.

5.2.2. Effective interest rate risk management enables an institution to understand, monitor, and mitigate its interest rate exposures, it also demonstrates the effectiveness of the institution's governance and oversight functions, specifically the Board of Directors, Senior Management, Operations Management, Risk Management, and Internal Audit in fulfilling their respective responsibilities.

5.3. Board of Directors

5.3.1. The board of directors has the ultimate responsibility for understanding the nature and the level of interest rate risk taken by an institution. The board shall review the overall objectives of the institution with respect to interest rate risk and ensure the provision of clear guidance on the level of risk acceptable to the institution. The Board shall possess detailed technical knowledge of complex financial instruments, relevant legal matters, and advanced risk management techniques.

5.3.2. The board shall approve strategies and policies with respect to interest rate risk management and ensure that senior management takes the steps necessary to monitor and control the risk consistent with the approved strategies and policies. The board shall be informed regularly of the interest rate risk exposure of an institution in order to assess whether such risk is being effectively monitored and controlled in line with the board's guidance on the institution's acceptable risk levels. At minimum, the board shall:

(a) approve and oversee the implementation of the institution's interest rate risk management framework including strategy, policies, risk appetite, and limits, ensuring they are consistent with the institution's overall business strategy and risk profile. The interest rate risk policies and strategy shall be reviewed at least annually.

(b) appoint senior management with appropriate expertise and integrity to manage interest rate risk, oversee their performance in implementing the interest rate risk management framework, and take corrective action, including dismissal, where risk management policies are not observed.

(c) receive and deliberate reports from senior management on interest rate risk management.

(d) ensure that the institution's interest rate risk management is subject to independent, objective and periodic assessment, which may be conducted by the internal audit

function or independent experts, covering the effectiveness of interest rate risk policies, controls and processes.

(e) ensure that an institution has a robust Internal Capital Adequacy Assessment Process (ICAAP) that sufficiently covers all material exposures to interest rate risk.

(f) ensure that information on the level of interest rate risk exposure and practices for measuring and controlling interest rate risk must be disclosed to the public on a regular basis.

(g) Approve methodologies and assumptions used to identify, measure, monitor and control interest rate risk, including those covering on and off-balance sheet exposures.

5.3.3. **Interest Rate Risk Strategy**

5.3.3.1. An institution's strategy to manage interest rate risk shall determine the level of interest rate risk the institution is prepared to assume. The interest rate risk strategy shall be periodically reviewed at least annually, taking into consideration its financial performance and market developments, and effectively communicated to the relevant staff. In setting the interest rate risk strategy, an institution shall consider the following factors:

(a) economic and market conditions and their impact on the institution's interest rate risk;
(b) expertise in specific markets that enables an institution to identify, monitor and control the interest rate risk in those markets; and
(c) portfolio mix and how it would be affected by interest rate volatility.

5.3.4. **Interest Rate Risk Policy**

5.3.4.1. An institution shall have in place sound, comprehensive and clearly defined credit policies, processes and procedures consistent with prudent standards, practices, and relevant regulatory requirements commensurate with the size, complexity and scope of the institution's operations. At a minimum the policy shall:

(a) prescribe the institution's interest risk appetite, including limits and tolerances, and specify management procedures and approval authorities for policy exceptions.

(b) prescribe interest rate risk management tools and procedures for identifying, measuring, monitoring and controlling Interest rate risk (including the types of Interest rate limits and ratios in place and rationale for establishing limits and ratios);

(c) delineate the lines of authority and the responsibilities of the personnel responsible for managing interest rate risk.

(d) indicate the content and frequency of management reports submitted to the board andsenior management on interest rate risk management. At a minimum, the report to the Board shall include:

(i) interest rate risk position, highlighting significant movements since the last reporting period, confirming whether exposures remain within board-approved limits and identifying any issues requiring board attention.

(ii) main sources of interest rate risk arising from the structure of the balance sheet, including repricing mismatches, yield curve and basis risks, embedded options, together with the key behavioral assumptions applied;

(iii) impact of regulatory and stress testing on earnings, equity, and capital, and identifies material vulnerabilities under adverse interest rate conditions.

(iv) implementation status of the findings of internal and external auditors, and regulatory authorities.

(v) results of core risk measures, including the sensitivity of earnings and economic value to interest rate movements, and highlights notable trends or changes compared to prior periods.

5.4. Senior Management

5.4.1. Senior management shall be responsible for ensuring that the structure of the institution's business and the level of interest rate risk assumed are effectively managed. Senior management shall be responsible for implementing the institution's interest rate risk management strategies and policies, and ensuring that the procedures are put in place to manage and control interest rate risk. At a minimum, senior management shall:

(i) implement policies and procedures approved by the Board for management of interest rate risk.

(ii) establish and maintain effective internal controls over the interest rate risk management framework, ensuring segregation of duties, independent monitoring, appropriate escalation mechanisms and clear communication of roles and responsibilities to all staff.

(iii) ensure that personnel responsible for interest rate risk management have adequate expertise, experience, and sufficient staffing resources are allocated to effectively carry out their responsibilities.

(iv) monitor interest rate risk positions continuously and ensure regular reports are comprehensive and timely submitted to the board for deliberation on the level of interest rate risk and effectiveness of controls.

(v) assess the impact of interest rate risk exposures on the institution's capital and earnings, considering both existing conditions and potential stress scenarios.

(vi) oversee the implementation, maintenance, and effectiveness of Management Information Systems (MIS), models and analytical tools used to identify, measure, monitor, and control interest rate risk across the institution.

(vii) implement directives and recommendations as well as resolving weaknesses or findings provided by oversight functions, including regulatory authorities, external audit, internal audit, and risk management.

(viii) put in place adequate arrangements for the prompt, effective and sustainable resolution of findings raised by oversight functions, including risk management, compliance, internal audit, and regulators, and ensure that remediation actions are tracked, completed, and validated.

5.5. Operations Management

5.5.1. Operations Management refers to the business units that own and manage interest rate risk on a day-to-day basis. This is the first line of defence responsible for management, monitoring, and oversight of interest rate risk within the institution. This includes ensuring that interest rate exposures are properly identified, measured, and controlled across all business units.

5.5.2. Operations Management shall ensure that operational controls are robust, and resources are adequate to identify, monitor, and mitigate inherent interest rate risks in line with the approved policies. Operations Management supports the implementation of the interest rate risk framework by ensuring compliance with internal standards and regulatory requirements, and contributing to the safety, soundness, and resilience of the institution to interest rate exposure. At a minimum, the business units shall:

(a) identify, measure, and control interest rate risks at all levels of business activities across the institution.

(b) ensure that there are adequate internal controls around interest rate risk related activities that includes top level reviews over interest rate activities, checking compliance with exposure limits and follow up on non-compliance, a system of approvals and authorizations and a system of verification and reconciliation.

(c) assess the interest rate risks inherent in new products and activities and ensure that such risks are subject to adequate review and approval prior to their introduction or undertaking.

(d) monitor interest rate risk positions continuously and ensure regular reports are comprehensive and timely submitted to senior management for deliberation on the level of interest rate risk and effectiveness of controls.

(e) notify the senior management on the material changes or exceptions from established policies that could have an impact on the implementation of interest rate risk framework including the capital allocated to cover losses arising from interest rate risk.

(f) implement and maintain a robust, reliable, comprehensive, and secure Management Information System (MIS) for interest rate risk monitoring.

5.6. Risk Management

5.6.1. Risk management function serves as the second line of defense within the institution's interest rate risk management framework. Its primary role is to provide oversight, guidance, and independent review to the first line of defense, ensuring that interest rate risks are properly identified, assessed, and managed across all business activities.

5.6.2. The Risk management function shall be adequately staffed and equipped with necessary expertise, tools and resources to effectively oversee the interest rate risk management framework. The risk management function shall be responsible for advising on interest rate risk policies, monitoring frameworks, and reporting mechanisms, as well as challenging and validating the adequacy of controls. At a minimum, the risk management function shall:

(i) define and maintain comprehensive risk management policies related to interest rate risk, ensuring they are consistent with the institution's overall risk appetite and strategy.

(ii) develop and monitor implementation of the enterprise-wide risk governance frameworks including policies, limits, risk appetite definitions and controls standards subject to board review and approval.

(iii) ensure that interest rate risk policies, appetite and tolerance levels are clearly communicated and applied across the institutions.

(iv) monitor compliance with established interest rate risk policies, limits, and regulatory requirements.

(v) Identify, measure, and assess interest rate risk in the banking book across all relevant business lines and markets. Provide timely and accurate information on risk exposures to support informed decision-making by the board and senior management.

(vi) independently validating interest rate risk assessments submitted by operations management to ensure accuracy, completeness, and consistency across the institution.

(vii) provide inputs in developing and maintaining operational risk management policies and guidelines.

(viii) ensuring that interest rate risk is integrated into the institution's enterprise risk management framework, including risk appetite, capital planning, operational risk assessments and strategic planning.

(ix) frequently reporting to senior management and the board on all key interest rate risk issues, including risk exposures, limit utilizations, stress-testing results, and breaches to enable effective oversight, timely decision-making, and appropriate risk mitigation actions.

(x) maintain a reliable Management Information System (MIS) capable of generating accurate and timely reports for interest rate risk control, including adherence to internal limits and regulatory requirements. The reports shall include early warnings, red flags, or triggers to monitor breaches of interest rate limits.

(xi) Conduct regular interest rate stress testing exercises using plausible assumptions about future volatility of interest rates.

5.6.3. The IT systems and applications used by the institution to carry out, process and record operations, to identify, measure and aggregate IRRBB exposures, and to generate reports should be capable of supporting the management of IRRBB in a timely and accurate manner. In particular, the systems should:

(a) Capture interest rate risk data on all the institution's material IRRBB exposures, including exposures to gap, basis, and option risk. This should support the institution's measurement system identifying, measuring and aggregating the major sources of IRRBB exposures.

(b) Be capable of fully and clearly recording all transactions made by the institution, considering their IRRBB characteristics.

(c) Be tailored to the complexity and number of transactions creating IRRBB.

(d) Offer sufficient flexibility to accommodate a reasonable range of shock and stress scenarios and any additional scenarios.

(e) Enable the institutions to fully measure, assess and monitor the contribution of individual transactions to their overall exposure.

(f) Be able to compute economic value and earnings-based measures of IRRBB, as well as other measures of IRRBB prescribed by their competent authorities, based on the interest rate shock and stress scenarios set out in sections 4.4.3 and 4.4.4.

(g) Be sufficiently flexible to incorporate supervisory-imposed constraints on institutions' internal risk parameter assumptions.

5.7. Internal Audit

5.7.1. Internal Audit function serves as the third line of defence in the management of interest rate risk and plays a critical role in providing an independent assurance to the board and senior management on the risk management framework. Internal audit evaluates the effectiveness of the interest rate risk management framework, verifies that interest rate risk is properly identified, assessed, monitored, and mitigated and ensures that the first and second lines of defence are operating in accordance with the institution's policies, risk appetite and regulatory requirements.

5.7.2. An institution shall have an Internal Audit Charter that clearly defines the authority, responsibilities, and scope of the internal audit function. The charter shall ensure that the internal audit function operates independently, has direct reporting lines to the board or audit committee, and possesses unrestricted access to records, personnel, and processes necessary to assess the effectiveness of governance, risk management, and internal controls. At a minimum, the internal audit function shall:

(a) provide independent, objective and risk-based assurance to the board and senior management on the adequacy, effectiveness, and integrity of the institution's interest rate risk management framework, including governance, risk appetite, strategies, policies, processes, systems, models, data, assumptions, reporting, and internal controls.

(b) ensure the function maintains sufficient authority, professional competence, and resources to assess interest rate risk management practices effectively. Audit staff shall possess appropriate expertise in interest rate risk, treasury and funding activities, stress testing, financial markets, model risk and relevant regulatory standards.

(c) ensure that an institution's quantification systems are sufficiently robust to guarantee the integrity of inputs, assumptions, processes, and methodologies, and produce interest rate risk assessments that accurately reflect the institution's risk profile.

(d) verify if interest rate risk limits are properly set, monitored, and adhered to, and that any breaches are appropriately escalated and resolved.

(e) establish and implement a risk-based audit plan that covers all material aspects of interest rate risk management, ensuring that all significant risk areas are reviewed as planned and that emerging or evolving interest rate risk arising from market conditions, new products, or strategic changes is appropriately assessed. The scope and frequency of audits shall be commensurate with the institution's risk profile and complexity.

(f) prepare and submit audit reports to the board or audit committee on interest rate risk management, highlighting material deficiencies, control weaknesses, governance issues, and regulatory concerns, together with prioritized and actionable recommendations.

(g) track and monitor the implementation of recommendations arising from internal and external audits, and supervisory authority reviews related to liquidity risk. This includes ensuring that business units respond to raised issues promptly, accurately, and adequately, and that regular reports are provided to the Board of Directors or its relevant committees on both pending and resolved matters.

6.0. FOREIGN EXCHANGE RISK MANAGEMENT

6.1. Introduction

6.1.1. Foreign exchange risk refers to the potential adverse impact on a bank's earnings and capital arising from movements in foreign exchange rates. Such risk may be amplified by the bank's exposure to other financial risks, including credit and liquidity risks.

6.1.2. The foreign exchange risk factors cited above are not exhaustive. Depending on the instruments traded by an institution, exposure to other factors may also arise. The institution's consideration of foreign exchange risk shall capture all risk factors to which it is exposed , and it must manage these risks soundly.

6.1.3. Sources of Foreign Exchange Risk

6.1.4. Foreign exchange risk in an institution arises from several key sources;

(a) open currency positions, which occur when an institution's foreign currency assets and liabilities are not perfectly matched, exposing it to losses when exchange rates move unfavourably.

(b) transaction or settlement exposure, especially in international payments, where time-zone differences or counterparty failures can lead to losses before the full settlement is completed.

(c) market making of foreign currency-denominated financial instruments or speculative trading in currencies, where sudden or unexpected market fluctuations may result in adverse effects on the institution's positions.

(d) balance sheet or structural exposure arises from holding foreign currency-denominated loans, deposits, or investments whose values change with exchange rates.

(e) economic exposure which may arise from long-term impact of exchange rate movements on earnings from foreign branches or cross-border operations.

(f) Off-balance sheet exposures, including derivatives such as forwards, swaps, and options, create foreign exchange obligations that can generate losses when markets shift.

(g) counterparty credit risk and regulatory or policy actions, such as currency devaluations or capital controls, can abruptly alter exchange-rate conditions and expose an institution to unexpected foreign exchange losses.

6.2. Management of Foreign Exchange Risk

6.2.1. An institution shall establish a comprehensive risk management framework for foreign exchange risk. The framework shall be clearly documented and commensurate with the nature, size, and complexity of the institution's operations. It shall clearly define roles and responsibilities for monitoring foreign exchange risk exposures against approved limits, authority to approve any variations to those limits, and procedures for escalating any breaches. The management of foreign exchange risk shall be integrated within an institution's overall risk management framework.

6.2.2. An institution shall establish a risk management system capable of accurately identifying, quantifying, and monitoring foreign exchange risk exposures, and of tracking changes in key foreign exchange risk drivers, including foreign exchange rates, interest rates, and equity prices, as well as other relevant market conditions, on a daily basis. Institutions with foreign exchange risk profiles that exhibit significant intra-day volatility shall implement systems and controls to monitor exposures on an intra-day basis.

6.2.3. The risk management system shall, where practicable, incorporate forward-looking capabilities to assess the likelihood and potential magnitude of future losses, including through appropriate risk measurement and stress-testing techniques. Furthermore, the system shall facilitate the timely identification of emerging risks and enable the prompt escalation and implementation of remedial actions in response to adverse movements in foreign-exchange risk factors.

6.2.4. Effective foreign exchange risk management enables an institution to understand, monitor, and mitigate its foreign exchange risk exposures. It also reflects the effectiveness of the institution's governance and oversight functions, specifically the Board of Directors, Senior Management, Operations Management, Risk Management, and Internal Audit in fulfilling their respective responsibilities.

6.3. Board of Directors

6.3.1. The board of directors has the ultimate responsibility for understanding the nature and the level of foreign exchange risk taken by an institution. The board shall review the overall objectives of the institution with respect to foreign exchange risk and ensure the provision of clear guidance on the level of risk acceptable to the institution. The Board shall possess detailed technical knowledge of complex financial instruments, relevant legal matters, and advanced risk management techniques.

6.3.2. The board shall approve strategies and policies with respect to foreign exchange risk management and ensure that senior management takes the steps necessary to monitor and control the risk consistent with the approved strategies and policies. The board shall be regularly informed of the foreign exchange risk exposure of an institution to assess whether such risk is being effectively monitored and controlled in line with the board's guidance on the institution's acceptable risk levels. At a minimum, the board shall:

(a) approve the institution's business strategies and policies governing foreign exchange risk, ensuring they provide a clear framework for identifying, measuring, monitoring, and controlling foreign exchange risk exposures. The Board shall ensure that these strategies and policies are consistent with the institution's overall risk appetite, regulatory requirements, and internal risk management standards.

(b) ensure that senior management has sufficient knowledge and is fully capable of managing foreign exchange risk, including taking the steps necessary to identify, measure, monitor, and control the risk.

(c) periodically review and deliberate reports from senior management to understand and assess the performance of senior management in monitoring and controlling foreign exchange risk in compliance with the institution's policies.

(d) ensure that the institution's foreign exchange risk management is subject to independent, objective, and periodic assessment, which may be conducted by the internal audit function or independent experts, covering the effectiveness of foreign exchange risk policies, controls, and processes.

(e) ensure that information on the level of foreign exchange risk exposure and practices for measuring and controlling foreign exchange risk are disclosed to the public on a regular basis.

(f) Approve methodologies and assumptions used to identify, measure, monitor and control foreign exchange risk, including those covering on and off-balance sheet exposures.

6.3.3. **Foreign exchange risk strategy**

6.3.3.1. A sound and well-informed foreign exchange risk management strategy shall define the level of foreign exchange risk the institution is willing to assume. Upon establishing its foreign exchange risk tolerance, the institution shall develop and implement a strategy that appropriately balances business objectives with approved foreign exchange risk appetite,

while ensuring compliance with regulatory requirements and prudent risk management practices. In setting a foreign exchange risk strategy, an institution shall consider:

(a) prevailing economic and foreign exchange market conditions, and their potential impact on the institution's foreign exchange risk exposures;

(b) the institution's expertise, systems, and capacity to identify, measure, monitor, and control foreign exchange risk arising from foreign currency activities; and

(c) the composition of the institution's portfolio and the potential effects on its financial condition should be considered if higher levels of foreign exchange risk are assumed.

6.3.3.2. The institution's foreign exchange risk strategy shall be subject to periodic review and effectively communicated across relevant levels of the institution. The institution shall establish robust processes to identify, monitor, and promptly address deviations from the approved foreign exchange risk strategy and established foreign exchange risk limits or targets.

6.3.3.3. An institution shall maintain a foreign exchange risk policy that is aligned with its overall strategy and clearly articulates its approach to identifying, measuring, controlling, and managing foreign exchange risk. The policy shall be reviewed at least annually to reflect changes in the institution's risk profile, business activities, and prevailing market conditions. The policy at a minimum shall prescribe;

(a) how foreign exchange risk is identified, measured and monitored;

(b) the institution's foreign exchange risk appetite, including limits and tolerances, and specify management procedures and approval authorities for policy exceptions.

(c) foreign exchange risk management tools and procedures for identifying, measuring, monitoring and controlling foreign exchange risk;

(d) the lines of authority and the responsibilities of the personnel responsible for managing foreign exchange risk;

(e) the content and frequency of management reports submitted to the board and senior management on foreign exchange risk management; and

(f) procedures for approval of any changes and exceptions to these policies.

6.3.3.4. An institution shall establish controls over foreign exchange risk that are commensurate with the nature, scale, and complexity of its activities. An effective control framework shall at a minimum include the following key elements;

(a) Clearly defined organizational and procedural controls to ensure effective segregation of duties between personnel responsible for initiating or executing foreign exchange transactions and those responsible for operational functions, including confirmation, settlement, reconciliation, and accounting of foreign exchange activities;

(b) Procedural controls designed to ensure that all foreign exchange transactions are accurately and completely recorded in the institution's records;

(c) Transactions are settled accurately and in a timely manner, and unauthorized or irregular transactions are promptly identified, escalated, and reported to management;

(d) Monitoring controls to ensure that foreign exchange activities are regularly and frequently measured against approved foreign exchange risk limits, counterparty exposure limits, and other relevant limits, and that any breaches or excesses are promptly reported in accordance with established escalation procedures; and

(e) Compliance controls to ensure that all foreign exchange activities are conducted in accordance with applicable laws, regulations, internal policies, and supervisory requirements.

6.4. Senior Management

6.4.1. Senior Management shall be responsible for the effective implementation of policies, procedures, and controls for managing foreign exchange risk on both a strategic and day-to-day basis. Senior Management shall establish and maintain clear lines of authority, responsibility, and accountability for the identification, measurement, monitoring, and control of foreign exchange risk. Furthermore, Senior Management shall ensure that foreign exchange risk strategies are implemented in a manner that appropriately limits the risks inherent in each strategy and ensures full compliance with applicable laws, regulations, and supervisory requirements. At a minimum, senior management shall:

(a) implement policies and procedures approved by the Board for management of foreign exchange risk.

(b) establish and maintain effective internal controls over the foreign exchange risk management framework, ensuring segregation of duties, independent monitoring, appropriate escalation mechanisms and clear communication of roles and responsibilities to all staff.

(c) ensure that personnel responsible for foreign exchange risk management have adequate expertise, experience, and sufficient staffing resources are allocated to effectively carry out their responsibilities.

(d) monitor foreign exchange risk positions continuously and ensure regular reports are comprehensive and timely submitted to the board for deliberation on the level of foreign exchange risk and effectiveness of controls.

(e) assess the impact of foreign exchange risk exposures on the institution's capital and earnings, considering both existing conditions and potential stress scenarios.

(f) oversee the implementation, maintenance, and effectiveness of Management Information Systems (MIS), models and analytical tools used to identify, measure, monitor, and control foreign exchange risk across the institution.

(g) implement directives and recommendations as well as resolving weaknesses or findings provided by oversight functions, including regulatory authorities, external audit, internal audit and risk management.

(h) implementing procedures and practices that translate the board's goals, objectives, and risk tolerances into operating standards that are well understood by institution personnel and consistent with the board's intent.

6.4.2. **Foreign Exchange Risk Management Structure**

6.4.2.1. The responsibility for managing the overall foreign exchange risk of the institution shall be delegated to a specific function or an identified committee within the institution. This may take the form of an Asset Liability Committee (ALCO) comprised of senior management or the treasury function.

6.4.2.2. Foreign exchange risk management requires specialized expertise and strong governance. Officers responsible for managing foreign exchange exposures must have a comprehensive understanding of the institution's foreign-currency liquidity position, including the nature, scale, and maturity profile of its foreign-exchange risks. They should be capable of assessing the impact of exchange rate movements, currency mismatches, and foreign-currency funding constraints on liquidity, and ensuring that appropriate risk management frameworks, limits, and controls are effectively implemented and monitored.

6.5. Operations Management

6.5.1. Operations Management refers to the business units that own and manage foreign exchange risk on a day-to-day basis. This is the first line of defence responsible for management, monitoring, and oversight of foreign exchange risk within the institution. This

includes ensuring that foreign exchange risk exposures are properly identified, measured, and controlled across all business units.

6.5.2. Operations Management shall ensure that operational controls are robust, and resources are adequate to identify, monitor, and mitigate inherent foreign exchange risks in line with the approved policies. Operations Management supports the implementation of the foreign exchange risk framework by ensuring compliance with internal standards and regulatory requirements, and contributing to the safety, soundness, and resilience of the institution to foreign exchange risk exposure. At a minimum, the business units shall:

(a) identify, measure, and control foreign exchange risk at all levels of business activities across the institution.

(b) ensure that there is adequate internal controls around foreign exchange risk-related activities that includes top level reviews over foreign exchange activities, checking compliance with exposure limits and follow up on non-compliance.

(c) assess the foreign exchange risks inherent in new products and activities and ensure that such risks are subject to adequate review and approval prior to their introduction or undertaking.

(d) monitor foreign exchange risk positions continuously and ensure regular reports are comprehensive and timely submitted to senior management for deliberation on the level of foreign exchange risk and effectiveness of controls.

(e) notify the senior management of the material changes or exceptions from established policies that could have an impact on the implementation of foreign exchange risk framework including the capital allocated to cover losses arising from foreign exchange risk.

(f) implement and maintain a robust, reliable, comprehensive, and secure Management Information System (MIS) for foreign exchange risk monitoring.

(g) ensure that effective mechanisms are in place to detect any deviations from approved policies. All foreign exchange transactions must be conducted in accordance with approved limits and established procedures.

(h) ensure timely and accurate measurement and monitoring of approved foreign exchange risk limits, including net open positions and exposure ratios, and provide reliable data for risk reporting.

(i) ensure that regular reports are comprehensive, accurate, and submitted on a timely basis to Senior Management for review and deliberation.

6.5.3. **Management Information System**

6.5.3.1. A robust management information system shall be in place to support the effective identification, measurement, monitoring, and control of foreign exchange risk exposures. The MIS shall provide timely and reliable information to senior management and the board in support of compliance with approved policies. Risk reporting shall be conducted regularly and shall clearly compare current foreign exchange risk exposures against approved limits. In addition, the institution shall perform periodic back-testing by comparing past forecasts or risk estimates with actual outcomes, to identify model weaknesses, data limitations, or other shortcomings and to take appropriate remedial actions.

6.5.4. **Foreign Exchange Risk Measurement and Monitoring**

6.5.4.1. An institution may employ a range of techniques to measure and control exposure to foreign exchange risk. One commonly used approach is the establishment of limits on net open positions for each foreign currency in which the institution is authorized to operate, as well as on the aggregate net open position across all currencies. Such limits are typically expressed as a percentage of Tier 1 capital or total assets to ensure that foreign exchange exposures remain commensurate with the institution's capital strength. Other approaches can be:

(a) the ratio of foreign currency assets to foreign currency liabilities;

(b) changes in net open position;

(c) size of off-balance sheet business of foreign denominated currency; and

(d) the ratio of income from foreign exchange trading to total income.

6.6. Risk Management

6.6.1. Risk management function serves as the second line of defense within the institution's foreign exchange risk management framework. Its primary role is to provide oversight, guidance, and independent review to the first line of defense, ensuring that foreign exchange risks are properly identified, assessed, and managed across all business activities

6.6.2. The Risk Management function shall be adequately staffed and resourced with the requisite expertise, systems, tools, and authority to effectively oversee the institution's foreign exchange risk management framework. The function shall be responsible for advising on the formulation and review of foreign exchange risk policies, limits, monitoring frameworks, and

reporting mechanisms, as well as independently monitoring exposures and rigorously challenging, validating, and assessing the adequacy and effectiveness of risk controls and risk mitigation measures. At a minimum, the risk management function shall:

(a) define and maintain comprehensive risk management policies related to foreign exchange risk, ensuring they are consistent with the institution's overall risk appetite and strategy.

(b) develop and monitor implementation of the enterprise-wide risk management framework including policies, limits, risk appetite statement and controls standards subject to board review and approval.

(c) ensure that foreign exchange risk management policies, appetite and tolerance levels are clearly communicated and applied across the institution.

(d) monitor compliance with established foreign exchange risk policies, limits, and regulatory requirements.

(e) Identify, measure, and assess foreign exchange risk across all relevant business lines and markets. Provide timely and accurate information on risk exposures to support informed decision making by the board and senior management.

(f) independently validating foreign exchange risk assessments submitted by operations management to ensure accuracy, completeness and consistency across the institution.

(g) ensuring that foreign exchange risk is integrated into the institution's enterprise risk management framework, including risk appetite, capital planning, operational risk assessments and strategic planning.

(h) frequently reporting to senior management and the board on all key foreign exchange risk issues including risk exposures, limit utilizations, stress testing results, and breaches to enabling effective oversight, timely decision making, and appropriate risk mitigation actions.

(i) maintain a reliable Management Information System (MIS) capable of generating accurate and timely reports for foreign exchange risk control, including adherence to internal limits and regulatory requirements. The reports shall include early warning, red flags or triggers to monitor breaches of foreign exchange limits.

(j) conduct regular foreign exchange stress testing exercises using plausible assumptions about future volatility of foreign exchange rates.

6.7. Internal Audit

6.7.1. Internal Audit function serves as the third line of defence in the management of foreign exchange risk and plays a critical role in providing an independent assurance to the board and senior management on the risk management framework. Internal audit evaluates the effectiveness of the foreign exchange risk management framework, verifies that foreign exchange risk is properly identified, assessed, monitored and mitigated and ensures that the first and second lines of defence are operating in accordance with the institution's policies, risk appetite and regulatory requirements.

6.7.2. An institution shall have an Internal Audit Charter that clearly defines the authority, responsibilities, and scope of the internal audit function. The charter shall ensure that the internal audit function operates independently, has direct reporting lines to the board or audit committee, and possesses unrestricted access to records, personnel, and processes necessary to assess the effectiveness of governance, risk management, and internal controls. At a minimum, the internal audit function shall:

(a) provide independent, objective and risk-based assurance to the board and senior management on the adequacy, effectiveness, and integrity of the institution's foreign exchange risk management framework, including governance, risk appetite, strategies, policies, processes, systems, models, data, assumptions, reporting, and internal controls.

(b) ensure the function maintains sufficient authority, professional competence, and resources to assess foreign exchange risk management practices effectively. Audit staff shall possess appropriate expertise in foreign exchange risk, treasury and funding activities, stress testing, financial markets, model risk and relevant regulatory standards.

(c) ensure that an institution's quantification systems are sufficiently robust to guarantee the integrity of inputs, assumptions, processes, and methodologies, and produce foreign exchange risk assessments that accurately reflect the institution's risk profile.

(d) verify if foreign exchange risk limits are properly set, monitored, and adhered to, and that any breaches are appropriately escalated and resolved.

(e) establish and implement a risk based audit plan that covers all material aspects of foreign exchange risk management, ensuring that all significant risk areas are reviewed as planned and emerging or evolving foreign exchange risk arising from market conditions, new products or strategic changes are appropriately assessed. The scope

and frequency of audits shall be commensurate to the institution's risk profile and complexity.

(f) prepare and submit audit reports to the board or audit committee on foreign exchange risk management, highlighting material deficiencies, control weaknesses, governance issues, and regulatory concerns, together with prioritized and actionable recommendations.

(g) track and monitor the implementation of recommendations arising from internal audits, external audits, and regulatory authorities' reviews related to strategic risk. This includes ensuring that business units respond to raised issues promptly, accurately, and adequately, and that regular reports are provided to the Board of Directors or its relevant committees on both pending and resolved matters.

7.0. STRATEGIC RISK MANAGEMENT

7.1. Introduction

7.1.1. Strategic risk is the current or prospective risk to earnings, capital, and long-term viability arising from adverse business decisions, ineffective or improper execution of those decisions, or a failure to respond in a timely and appropriate manner to changes in the internal and external operating environment. It is driven by the degree of alignment between the institution's strategic objectives, the business strategies and resources deployed to achieve them, and the effectiveness with which those strategies are implemented and monitored.

7.1.2. If not properly managed, strategic risk may gradually permeate different units of an institution and become embedded in its organizational culture, making it difficult to detect and address in a timely manner. Over time, this can erode the institution's competitive position in the market.

7.1.3. **Sources of Strategic Risk**

7.1.3.1. Strategic risk can arise from two main sources: external and internal risk factors. External risk factors are difficult for the institution to control or those over which the institution has no control and affect or deter the realization of the goals determined in the strategic plan. Such factors include:

(a) **Competition -** a strategic plan and business plan must be in line with current and anticipated future competition. Competitive factors must be taken into consideration in the institution's pricing practices and when developing new products.

(b) **Change in demographics and consumer profiles -** changes in demographics and consumer profiles may affect the customer base, earnings and capital funding of an institution.

(c) **Technological changes -** an institution may face risks from changing technology because its competitors can develop more efficient systems or services at lower costs. The institution should ensure that the level of technology in use is sufficient to retain its customer base.

(d) **Economic factors -** global, regional, or national economic conditions affect the level of profits of an institution. Thus, continual assessment and monitoring of economic trends and forecasts are needed.

(e) **Regulations –** changes in laws and regulations of the supervisor, tax authorities, local authorities and other authorized agencies may affect the implementation of

strategic and business plans established to meet the institution's goals; and may require adjustments to the plans in order to ensure compliance.

7.1.3.2. Internal risk factors are controllable by the institution but can affect or deter the implementation of the strategic plan. Such factors include:

(a) Organizational structure – An organizational structure that is inconsistent with the institution's strategic plans may give rise to conflicts of interest among directors, management, shareholders, and staff, thereby undermining effective governance and impairing the achievement of the institution's strategic objectives. It is important for an institution to establish an organizational structure that is consistent with the institution's strategic plans for effective implementation of strategic and business plans.

(b) Work processes and procedures – improper design and implementation of work processes and procedures may impede timely and accurate implementation of business plans. The institution shall establish policies that stipulate clear responsibilities, guidelines and procedures for discharging responsibilities while maintaining robust internal controls.

(c) Personnel – Lack of competent and sufficient staff levels can increase risk exposures, impair financial performance and damage the institution's reputation. The success of accomplishing strategic and business plan is dependent on the knowledge, experience, and vision of the Board, management and staff. The staff shall have the necessary expertise and training to perform their assignments in an efficient and effective manner.

(d) Information - Deficiencies in the quality, relevance, accuracy, or timeliness of information undermine management's understanding of the institution and its operating environment, which in turn weakens strategic and business planning and leads to sub-optimal managerial decisions.

(e) Technology – inadequate systems may fail to support complex transactions and customers' needs, potentially undermining competitiveness and hindering the development and support of new business lines.

7.1.3.3. Risk mitigation factors help in the implementation of a strategic plan. Such factors include a qualified Board of Directors, adequate preparation of strategic and business plans, quality personnel and their ongoing training, an effective risk management system, adequate access to information, and timely and efficient introduction of new products or services.

7.1.3.4. Strategic risk, if not adequately managed, may gradually manifest itself in different units of an institution. It has a tendency of attaching itself to the 'institutional culture' and might not easily be recognized. It can further affect an institution's position in the market e.g. through falling share of the target market.

7.2. Management of Strategic Risk

7.2.1. Effective management of strategic risk requires an institution to establish and maintain robust risk mitigation measures that support the successful execution of its strategic plan. These include a competent and independent Board of Directors, well-developed strategic and business plans, suitably qualified personnel supported by continuous training, a sound risk management framework, reliable and timely access to information, and the efficient and well-controlled introduction of new products and services.

7.2.2. An institution shall establish a clear strategic direction through a well defined vision and mission that articulate where it intends to position itself in the medium to long term. This direction shall be documented in a strategic plan that clearly sets out the institution's objectives and goals across all major areas of its business, providing a structured framework to guide decision-making and resource allocation.

7.2.3. A strategic plan is a document reflecting the mission and strategic goals of an institution, generally for a period of at least four years and subject to annual review. A good strategic plan must be clear, consistent with goals, flexible, and adjustable to changes in the environment. A strategic plan shall contain at least the following:

(a) Analysis of the external environment in which the institution operates, including the PEST analysis;

(b) Critical review of the institutional performance including SWOT analysis;

(c) Institution's strategic goals and objectives;

(d) Description of the institution's risk management system;

(e) Mission, goals and operating plans for each of the institution's units; and

(f) Institution's quantitative projection of financial statements for the planning period.

7.2.4. Effective strategic risk management enables an institution to identify, assess, monitor, and mitigate risks arising from its business strategy and external environment. It also reflects the effectiveness of the institution's governance and oversight functions, specifically the Board of Directors, Senior Management, Operations Management, Risk Management, and Internal Audit, in fulfilling their respective responsibilities.

7.3. Board of Directors

7.3.1. The board of directors has a critical role to play in overseeing the strategic risk management functions of an institution. The board shall have ultimate responsibility for approving the institution's strategic plan and significant policies relating to strategic risk management.

7.3.2. The Board shall be knowledgeable about the institution's market, economic and competitive conditions and ensure that the strategic plan is implemented effectively and reviewed at least annually. They shall receive relevant reports that are accurate and timely and can be appropriately used in the decision making process. At a minimum, the board shall:

(a) Set, approve and oversee the implementation of the institution's strategic plan, vision, and mission in line with the institution's purpose, long-term goals, and periodically reviewing the vision and mission to ensure they remain relevant to the evolving business and regulatory environment.

(b) develop, approve, and oversee the implementation of the strategic risk appetite statement, limits, budget, and significant strategic risk policies of an institution.

(c) appoint senior management with appropriate expertise and integrity, oversee their performance in implementing the strategic risk management framework, and take corrective action, including dismissal, where risk management objectives or policies are not met.

(d) approve a policy or plan for management succession. The policy or plan should be reviewed at least annually, be consistent with the organizational structure and job descriptions, and cover the necessary training and minimum qualifications for each position and career path.

(e) ensure that the institution's strategic risk management framework is subject to independent, objective, and periodic assessment, which may be conducted by the Internal Audit function or independent experts, covering the effectiveness of the strategic plan, strategic risk appetite statement, limits, budget, strategic risk policies, controls, and processes.

(f) ensure that new products and activities are carefully evaluated and designed to meet the needs of target markets while aligning with the institution's risk appetite and strategic objectives.

(g) ensure that the Board meets at least quarterly, with strong attendance and active participation, and that its deliberations are supported by timely, accurate, and comprehensive management reports and records to enable informed discussion, effective challenge, and sound decision making on various risks and strategic matters.

(h) ensure that the Board is composed of an adequate number of members with sufficient skills, knowledge, and experience necessary to provide effective oversight of strategic risk.

(i) ensure Board members are exposed to induction programs and ongoing training on risk management and regulatory matters.

(j) approve the institution's corporate training plan, including the allocation of sufficient resources and budget to ensure effective implementation and development of staff capabilities.

(k) approve a staff retention plan to retain capable individuals who have the proper knowledge and understanding of the institution's business and operations.

(l) receive and deliberate on reports from senior management on strategic risk management. At a minimum, these reports shall cover existing and emerging strategic risks, compliance with and breaches of approved limits or tolerances, performance relative to strategic goals, an assessment of outcomes against the approved strategic objectives, internal control failures, legal or regulatory concerns and issues raised by the 'whistleblowing' process.

(m) approve and ensure effective oversight of policies and procedures governing conflicts of interest in relation to strategic risk.

(n) ensure effective oversight of the finance function, approval of annual financial statements, and independent review of critical financial and strategic risk areas.

(o) approve methodologies and assumptions used to identify, measure, monitor and control strategic risk.

(p) approve compensation guidelines and methods for management and employees. The compensation should be appropriate to the financial standing of the institution.

7.3.3. **Strategic Risk Policy**

7.3.3.1. Strategic risk management shall be anchored on a strategic risk management policy that aligns with the institution's overall Risk Management Framework and applicable regulatory guidelines. The Strategic Risk Management Policy shall provide general

guidelines for identifying, assessing, monitoring, and controlling strategic risks across the institution. The policy shall be reviewed at least annually to reflect changes in the institution's risk profile, business activities, and prevailing market conditions. At a minimum, the policy shall include the following:

(a) definition of strategic risk.

(b) Sources of strategic risk (external and internal risk factors).

(c) Risk mitigation factors to strategic risk.

(d) Roles and responsibilities of the personnel responsible for managing strategic risk.

(e) Contents and frequency of management reports submitted to the board and senior management on strategic risk management.

(f) Tools and procedures for identifying, measuring, monitoring, and controlling strategic risk.

7.3.4. **Strategic Risk Measurement Tools**

7.3.4.1. Every institution shall design on-going methods for formal assessment of both the strategic and operational plans in relation to its business scope, complexity, external environment, and internal factors.

7.3.4.2. An institution shall utilize a range of tools to assess its strategic risk. The following are some examples of the techniques:

(a) risk maps: summary charts and diagrams that help the bank to identify, understand and address risks by portraying sources and types of risks and functions involved;

(b) modelling tools: such as scenario analysis and forecasting models to show the range of possibilities and to build scenarios into contingency plans; and

(c) qualitative techniques: such as questionnaires and self-assessment to identify and assess risks.

7.4. Senior Management

7.4.1. Senior Management is responsible for implementing the institution's approved strategic and business plans. Creation of adequate conditions for implementation, including the design and adoption of a strategic risk management policy, procedures, as well as duties and responsibilities of different units, is the most critical step towards effective implementation of the strategic and business plans. Critical to the effective implementation of the strategic plan is a well-designed internal infrastructure, encompassing an efficient organizational structure, skilled personnel, robust budgeting processes, adequate

resources, reliable and timely management information systems, and comprehensive monitoring and control mechanisms that ensure business objectives are achieved effectively and efficiently. Specifically, the senior management shall:

(a) translate strategic objectives into achievable operational targets, prioritized according to their strategic significance, and cascade them into clearly defined, executable actions assigned to the relevant business units across the institution.

(b) implement strategic risk policies and procedures approved by the board to ensure operations are in line with the approved risk appetite.

(c) establish and oversee a Management Information System (MIS) capable of generating comprehensive, timely information that supports the management of strategic risk. The system shall be able to capture strategic risk exposures that approach or exceed established limits, and report exceptions promptly, allowing senior management to take corrective action.

(d) maintain continuous surveillance of market trends, competitor strategies, and technological innovations to support informed strategic decision-making and sustainable product development. Furthermore, management shall undertake thorough evaluations of risks, commercial and operational feasibility, customer demand, and implementation requirements when developing and proposing new products or services.

(e) develop and annually update a policy or plan for management succession in line with the organizational structure, job descriptions, minimum qualifications for each position and career path.

(f) operationalize approved compensation guidelines and ensure fairness, competitiveness, and alignment with institutional goals. Senior management shall also implement staff retention plans to retain capable individuals with the proper knowledge and understanding of the institution’s business and operations.

(g) develop a comprehensive annual training plan and allocate an adequate budget for training.

(h) ensure adequate staffing with appropriate competencies in strategic functions.

(i) advise the Board regarding strategic risk policies, objectives, and plans.

(j) report quarterly to the board or the designated committee on strategic risk management.

(k) implement directives and recommendations as well as resolving weaknesses or findings provided by oversight functions including regulatory authorities, external audit, internal audit, and risk management. Senior management shall ensure that remediation actions are tracked, completed, and validated.

7.5. Operations Management

7.5.1. Operations Management refers to the business units and front-line staff who own and manage strategic risk on a day-to-day basis. This is the first line of defence in strategic risk management by an institution. They are responsible for ensuring that day to day activities align with the organization's goals and risk appetite.

7.5.2. As the function responsible for the execution of day to day business activities, it serves as the initial point where potential risks to strategy can be identified, measured, monitored, and controlled, by aligning operational processes with the organization's strategic objectives and risk appetite. Operations Management helps to ensure that threats are detected early and mitigated before they escalate. Institutions shall have a policy that defines clear roles and responsibilities in relevant business units.

7.5.3. Operations Management shall ensure that operational controls are robust, and resources are adequate to identify, monitor, and mitigate inherent strategic risks in line with the approved policies. Operations Management supports the implementation of the strategic risk framework by ensuring compliance with internal standards and regulatory requirements, and contributing to the safety, soundness, and resilience of the institution's strategic position. At a minimum, the operations management function shall:

(a) identify and monitor emerging and existing strategic risks arising from changes in business models, products, delivery channels, markets, operational constraints, capacity limitations or skill gaps, technology changes, outsourcing arrangements, and process redesigns.

(b) advise senior management on the establishment of appropriate and effective controls to mitigate inherent strategic risks.

(c) implement and maintain information systems covering all strategic activities. These systems must be secure, independently monitored, supported by adequate contingency arrangements, and provide accurate, timely and complete information.

(d) advise whether strategic activities are supported by competent personnel and reporting whether the business units have adequate resources, tools and training for the day-to-day management and oversight of strategic risk.

(e) ensure strategic plans, policies and procedures are effectively communicated to staff for understanding their duties and responsibilities.

(f) implement clearly defined workflows, effective segregation of duties, and robust authorization controls. These measures support strong reconciliation processes, incident management procedures, and well-defined escalation mechanisms, ensuring disciplined and consistent execution of the institution's strategy.

(g) ensure that day-to-day activities remain within the institution's established strategic risk appetite and tolerance limits.

(h) ensure that regular reports are comprehensive, accurate, and submitted on a timely basis to Senior Management for review and deliberation. This includes prompt escalation and reporting of strategic incidents and control breaches to the risk management function, enabling effective assessment and timely corrective action.

7.5.4. **Identification, Measurement and Monitoring of Strategic Risk**

7.5.4.1. An effective measurement and monitoring process is essential for adequately managing strategic risk. Identification and measurement of strategic risk can be determined through strategic planning, the preparatory process of a strategic plan and the reasonableness of a strategic plan. Both the strategic plan and the operational plans and budget should be consistent with the business scope, complexity, external environment, and internal factors of the institution, including its size and resources.

7.5.4.2. Management shall actively and fully participate in the strategic planning process and make informed decisions based on comprehensive and reliable information to ensure that business and strategic plans are feasible, appropriate, and aligned with the institution's objectives. Management shall further ensure effective communication, coordination, and cooperation among all employees and departments involved in the strategic planning process.

7.5.4.3. The goals of the operational plans shall be consistent with the strategic plan and overall objectives of the institution, as well as, allocation of budget. The institution shall set goals, such as the quality of its credit portfolio, that are consistent with its capacity, current market share, and competitive environment.

7.5.4.4. The objectives of the operational plans shall be fully aligned with the institution's strategic plan, overall objectives, and approved budget allocations. The institution shall set measurable and achievable goals, such as targets for the size and quality of the credit portfolio, that are consistent with its capacity, current market position, and the prevailing competitive environment.

7.5.4.5. An institution shall periodically evaluate actual performance against the approved strategic plan to effectively monitor and measure progress. Such evaluations shall be based on clear, measurable indicators and conducted with sufficient frequency to enable a timely identification of deviations and implementation of corrective actions. The evaluation results will enable the institution to adjust its plans appropriately and consistently as changes occur.

7.5.4.6. To ensure the adequacy and appropriateness of strategic risk monitoring frameworks, reporting arrangements, and management information systems, each business unit shall, at a minimum, ensure that:

(a) reports submitted to senior management and the Board contain relevant, complete, and reliable information to support informed decision-making;

(b) reports are prepared and submitted with appropriate frequency and timeliness;

(c) the format and presentation of reports facilitate a clear understanding of key issues; and

(d) reports clearly identify material strategic risks, along with the mitigating strategies, controls, and actions implemented to address them.

7.5.4.7. An institution shall put in place a robust management information system (MIS), for effective monitoring of strategic risk. The MIS supports the implementation of the strategic plan through the following:

(a) Collects, processes and provides data;

(b) Reduces operating cost;

(c) Enhances communication among staff; and

(d) Enables the institution to identify, measure and monitor its strategic risk in a timely manner and generate data and reports for use by the board and senior management.

7.5.4.8. The MIS shall be consistent with the complexity and diversity of the institution’s business operations. For example, a large institution with many complex transactions shall have a reporting system and risk monitoring system that can measure the overall risk level. It shall have the ability to collect, store and retrieve both internal and external data including financial data; economic condition data, competition data, technology and regulatory requirements.

7.6. Risk Management

7.6.1. Risk management function as a second line of defence, has the responsibility of providing independent oversight, guidance, and challenge to business units. The function shall be responsible for systematically identifying and assessing strategic risks, measuring the institution's risk exposure, and assessing the effectiveness of controls.

7.6.2. The risk management function shall be adequately staffed and equipped with the necessary expertise, tools, and resources to effectively oversee the strategic risk management framework. The function must ensure continuous monitoring of the strategic risk profile of an institution. At a minimum, the risk management function shall:

(e) independently oversee, monitor, and challenge strategic risks in business units and enterprise-wide, including identified material strategic risk, design and effectiveness of key controls and risk tolerance.

(f) ensure that the risk policies, appetite, and tolerance levels are clearly communicated and applied across the institution. This includes providing training and instilling risk awareness.

(g) provide timely, accurate and comprehensive reports on key strategic risk issues, emerging risks, control gaps and recommended mitigation actions to Senior management and the Board or the relevant Board committee.

(h) maintain a reliable Management Information System (MIS) capable of generating accurate and timely reports for strategic risk control. The reports shall include early warning, red flags or triggers to monitor breaches of strategic limits.

(i) challenge the relevance and consistency of the business unit's implementation of the strategic risk management tools, measurement activities and reporting systems.

(j) Provide inputs in developing and maintaining strategic risk management policies, procedures, and guidelines.

(k) monitor and report the business units' strategic risk profile and ensure adherence to the established strategic risk appetite and tolerance.

7.7. Internal Audit

7.7.1. Internal audit function serves as the third line of defence in the management of strategic risk and plays a critical role in providing an independent assurance to the board and senior management. Internal audit evaluates the effectiveness of the strategic risk management framework, verifies that strategic risks are properly identified, assessed, monitored and mitigated and ensures that the first and second lines of defence are

operating in accordance with the institution's policies, risk appetite and regulatory requirements.

7.7.2. For the effective implementation of the strategic plan, the Board shall ensure that, where the internal audit function provides independent assurance and advisory input to those charged with strategic risk management, its independence and objectivity are maintained at all times and are not compromised by involvement in the execution or management of strategic risk management activities.

7.7.3. An institution shall have an Internal Audit Charter that clearly defines the authority, responsibilities, and scope of the internal audit function. The charter shall ensure that the internal audit function operates independently, has direct reporting lines to the board or audit committee, and possesses unrestricted access to records, personnel, and processes necessary to assess the effectiveness of governance, risk management, and internal controls. At a minimum, the internal audit function shall:

(a) evaluate the design, implementation, and effectiveness of the institution's strategic risk management framework, including policies, procedures, controls and risk monitoring processes.

(b) report directly to the Board or Audit Committee on strategic risk matters.

(c) provide timely, accurate and comprehensive reports on strategic risk exposures, control effectiveness, emerging risks, and significant issues requiring corrective actions.

(d) review strategic risk management practices related to outsourcing and critical third party services.

(e) track and monitor the implementation of recommendations arising from internal audits, external audits, and regulatory authorities' reviews related to strategic risk. This includes ensuring that business units respond to raised issues promptly, accurately, and adequately, and that regular reports are provided to the Board of Directors or its relevant committees on both pending and resolved matters.

(f) review validation processes to ensure they are independent and implemented in a manner consistent with established institution policies.

(g) ensure that an institution's measurement tools are sufficiently robust to guarantee the integrity of inputs, assumptions, processes, and methodologies, and produce strategic risk assessments that accurately reflect the institution's risk profile.

(h) develop and implement a risk-based audit plan that adequately covers all areas posing significant strategic risk. The audit plan must define an appropriate scope and frequency of reviews, ensuring higher risk areas are assessed more frequently and comprehensively.

8.0. COMPLIANCE RISK MANAGEMENT

8.1. Introduction

8.1.1. Compliance risk is the current or prospective risk to earnings and capital arising from violations or non-compliance with laws, regulations, rules, agreements, prescribed practices, or ethical standards, as well as from the possibility of incorrect interpretation of effective laws or regulations. An institution is exposed to compliance risk due to relations with a great number of stakeholders, such as regulators, customers, counter parties, as well as tax authorities, local authorities and other authorized agencies.

8.1.2. Compliance risk can lead to licenses revocation, fines and penalties, payment of damages, deteriorating position in the market, reduced expansion potential, and lack of contract enforceability. Compliance risk can also lead to reputation risk, arising from an adverse perception of the image of the institution by customers, counter parties, shareholders, or regulators. This affects the institution's ability to establish new relationships, services or products, or service existing relationships. This risk may also expose the institution to administrative, civil and criminal liability, financial loss or a decline in its customer base.

8.1.3. Compliance risk is difficult to measure, but it can be defined, understood, and controlled within the institution's capacity and its readiness to confront non-compliance. Compliance risk can occur whether deliberate or unintentional.

8.1.4. Appropriate actions for the institution to take in mitigating compliance risk would include: reducing exposures of sources of compliance risk, an appropriate compliance risk management process and putting in place an effective compliance function in the institution. Sources of Compliance risk shall include:

(a) violations or non-compliance with laws and regulations and prescribed standards.

(b) non-compliance or inadequate compliance with contractual obligations and other legal documentation.

(c) inadequate identification of rights and responsibilities between the institution and its customers.

(d) complaints by customers and other counterparties.

(e) harming the interests of third parties. and/or

(f) limited knowledge and delayed response to implement legal and reputation risk management.

8.2. Management of Compliance Risk

8.2.1. Effective compliance risk management requires a coordinated governance structure in which all key oversight functions of risk management work together to identify, assess, and control compliance obligations across the institution. A sound governance framework shall emphasize clear accountability, robust oversight, and effective internal controls to ensure that compliance risk is proactively managed and mitigated.

8.2.2. Effective compliance risk management enables an institution to better understand and mitigate its risk profile, and it reflects the effectiveness of oversight functions, specifically the board of directors, senior management, operations management, risk management, and internal audit in fulfilling their responsibilities.

8.3. Board of Directors

8.3.1. The institution's board of directors is responsible for overseeing the management of the financial institution's compliance risk. The board shall approve the institution's compliance policy, including a formal document establishing a permanent and effective compliance function, its corresponding responsibilities, as well as the position of Head of Compliance. At least once a year, the board or a committee of the board shall assess the extent to which the institution is managing its compliance risk effectively. At a minimum, the Board shall:

(a) establish the compliance function and approve its structure, including itsHead of Compliance.

(b) ensure that the compliance function and the Head of Compliance are given appropriate stature, authority, and independence.

(c) review and approve an appropriate framework, policy, and related processes and procedures to identify, analyze, measure, mitigate, manage, and monitor its compliance risk. The policy and framework shall be reviewed at least annually.

(d) receive and deliberate regular reports from senior management on compliance risk management, at least on a quarterly basis.

(e) ensure that compliance issues are resolved effectively and promptly by senior management with the assistance of the compliance function, and that appropriate measures, including, where relevant, disciplinary actions, are taken.

(f) ensure that the compliance function is provided with adequate expertise and budgetary resources to effectively discharge its responsibilities.

8.3.2. Compliance risk should be a standing item on the agenda of board meetings at least on a quarterly basis to deliberate compliance issues and ensure that they are resolved effectively and expeditiously.

8.3.3. The Board shall ensure adequate policies and procedures for managing compliance risk are in place. The compliance risk management policy shall explain the main processes by which compliance risk is to be identified and managed through all levels of the institution. The policy shall also define the compliance function with specific roles and responsibilities of the compliance staff and detail the compliance officer's communication methods with the management and staff in the various business units. At a minimum, the policy shall cover the following:

(a) Definition of compliance risk.

(b) Objectives of compliance risk management.

(c) Procedures and tools for identifying, assessing, monitoring, controlling and managing compliance risk;

(d) Well-defined authorities, responsibilities, and information flows for compliance risk management at all management levels; and a clear statement of the institution's accepted tolerance for compliance risk exposure.

(e) the financial institution's expectations on compliance culture;

(f) structure (including the broad categories of staff), the roles and responsibilities and reporting lines of the compliance function, as well as other staff performing compliance responsibilities.

(g) reporting requirements of the compliance function to senior management and the board, including the minimum contents of the reports and reporting frequency.

(h) procedures for assessing, resolving, escalating, and reporting compliance breaches and other related issues.

(i) Capacity building programs on compliance risk management.

8.3.4. The procedures for managing compliance risk shall contain:

(a) Definition of the required legal documents establishing the collateral on loans for clients. These also include verification, by the institution's legal expert, of the legitimacy of the collateral on the basis of the available documentation;

(b) Definition of standard procedures for foreclosures;

(c) Standardized contracts for similar institutions' products, clients, and other services with third parties. The terms and conditions of a contract shall be confirmed by the institution's legal expert. Special attention shall be paid to the procedures for changing the terms of a signed contract. The institution's legal expert shall also confirm annexes to any contract;

(d) Legal due diligence of the institution's major clients and counterparties, vendors and outsourcing companies;

(e) Documentation standards for all initiated court proceedings against or on behalf of the institution. Permanent and accurate information and documents of the institution's effectiveness in court proceedings and needed. Institution's legal experts shall keep a list of all court proceedings with their opinion on the possible result of the case, as well as, a list of court cases that in the name of the institution are led by outside attorneys. In addition, the institution shall separately retain data describing the types of claims for which the institution has usually initiated litigation and in which cases the institution was sued;

(f) Definition of the major mitigating actions to compliance risk (e.g., through reviewing contract terms by experienced lawyers, restricted dealings to reputable counterparts, placing limits on exposure to legal interpretations, etc.);

(g) Clear documentation standards for the institution's shareholders;

(h) Documentation standards for all decisions made by the Bank of Tanzania in respect of the institution and written communications between the Bank of Tanzania and the institution;

(i) Procedures for safeguarding of original legal documents; and

(j) Regular compliance checks.

8.3.5. An institution shall adopt structured assessment methodologies to enable each business line to understand the severity and likelihood of non-compliance events to adequately assess vulnerability to compliance risk. The following tools shall be applied as part of the measurement process:

(a) Self-Assessment: Business units shall regularly evaluate their processes against compliance checklists and internal regulatory requirements. This internal review helps identify weaknesses, outdated procedures and areas requiring remediation.

(b) Risk Indicators: Risk indicators are statistics or matrices that can provide insight into an institution's risk position. Such indicators may include the volume and/or

frequency of law violations, frequency of complaints, number of initiated litigation procedures, regulatory breaches, operational errors, payments of damages, fines and court expenses, unfavorable court verdicts or number of finalized court cases on a periodical basis, and frequency of actual or suspected fraud or money laundering activities. Business units shall track and report risk indicators, which shall allow management to understand trends and areas of elevated risk exposure. The indicators shall also provide good incentives, tying risk to capital to desirable improvement in the compliance function.

(c) Risk Mapping: Business units shall map their activities against specific types of compliance risks, such as risks related to customer profiling in onboarding, contract enforcement challenges in credit operations, or reporting obligations in payments. This mapping helps determine priorities for operational improvements.

8.3.6. The size of the institution and the complexity of its business activities dictate the scope of the compliance function and staffing requirements (number and competencies) of a compliance function unit. Not all compliance responsibilities are necessarily carried out by a compliance unit. Compliance responsibilities may be exercised by staff in different departments, or all compliance responsibilities may be conducted by the compliance unit.

8.3.7. Regardless of how the compliance function is organized within the institution, it shall be independent, with sufficient resources and clearly specified activities. The compliance staff, especially the head of compliance, shall not be in a position where a conflict of interest may arise between their compliance responsibilities and any other responsibilities they may have.

8.3.8. The head of compliance function may or may not be a member of senior management. If the head of the compliance function is a member of senior management, he or she shall not have direct business line responsibilities. If the head of the compliance function is not a member of senior management, he or she shall have a direct reporting line to a member of senior management who does not have direct business-line responsibilities.

8.4. Senior Management

8.4.1. Senior management shall be responsible for the effective management of the institution's compliance risk. The senior management shall establish and communicate a compliance policy to ensure that it is observed and kept up to date, and to report to the board of directors on the management of the institution's compliance risk. Specifically, the senior management shall:

(a) implementing policies and procedures approved by the Board for management of compliance risk.

(b) assigning adequate staffing with appropriate competencies in the compliance function.

(c) providing sufficient financial and technological resources for compliance operations.

(d) maintaining continuous communication with compliance staff and legal teams for regular monitoring of compliance activities;

(e) report to the board or the designated committee annually on the effectiveness of the institution's management of its compliance risk and governance framework to assist the board in making an informed judgment on whether the institution is managing its compliance risk effectively.

(f) report quarterly to the board or the designated committee on compliance risk management including any significant risk of legal or regulatory sanctions.

(g) ensuring ongoing compliance training that covers compliance requirements for all business lines, particularly when entering new markets or offering new products.

(h) implementing directives and recommendations as well as resolving weaknesses or findings provided by oversight functions, including regulatory authorities, external audit, internal audit, and risk management.

8.4.2. Senior Management shall maintain strong oversight over compliance risk by establishing a structured regulatory change management process to track and implement new requirements, ensuring that digital and data systems adequately support compliance while embedding compliance checks into all product approval and customer onboarding processes.

8.4.3. Senior management shall oversee periodic stress testing or scenario analyses to assess the institution's resilience to emerging compliance risks, particularly those arising from regulatory changes.

8.4.4. Senior management shall put in place an effective whistleblower protection mechanism to encourage safe reporting of misconduct.

8.5. Operations Management

8.5.1. Operations Management serves as the first line of defense in the compliance risk management framework. As owners of day-to-day business activities, business units are directly responsible for identifying, assessing, controlling, and mitigating compliance risks

inherent in their processes. This includes ensuring that activities comply with applicable laws, regulations, internal policies, and ethical standards.

8.5.2. Operations Management plays a critical role in preventing regulatory breaches, operational failures, and reputational damage by embedding compliance controls into operational processes. Proactive risk ownership, effective internal controls, timely issue escalation, and continuous monitoring form the foundation of the first line of defense.

8.5.3. An effective risk measurement and monitoring process is essential for adequately managing compliance risk. To understand its compliance risk profile, an institution shall identify the sources of compliance risk and assess its vulnerability to theme. If a new compliance risk is not identified, the institution's legal experts may never thoroughly review the existing contracts. Thus, the institution shall identify and assess the Compliance risk inherent in all existing or new rules, procedures, internal processes, activities, contracts, and court cases.

8.5.4. An institution shall establish a structured and continuous process for identifying compliance risk inherent in all business activities, products, services, and operational processes. This includes identifying risks originating from laws, regulations, contractual obligations, internal policies, and ethical standards applicable to the institution. The identification process must extend beyond existing activities to include new products, new delivery channels, digital initiatives, outsourcing arrangements, customer onboarding procedures, and third-party relationships. Business units, being closest to day-to-day activities, shall actively flag emerging compliance concerns to Senior Management.

8.5.5. Business units shall monitor compliance risk on a continuous basis through periodic reviews of risk indicators, exception reports, customer complaints, legal cases, and compliance findings. Monitoring must be part of daily operations and not treated as a one-off exercise. Results from monitoring activities shall be compiled into periodic reports submitted to the Compliance Function, Risk Management and Senior Management. These reports shall highlight emerging risks, recurring issues and root causes requiring corrective action.

8.5.6. Business units shall establish processes, procedures, and internal controls to manage and mitigate compliance risk. This includes validation of legal documentation and adherence to proper segregation of duties, proper documentation, and standard operating procedures.

8.5.7. Business units shall conduct regular reviews to determine whether operational activities meet legal and policy requirements. Where gaps are identified, timely corrective actions must be initiated and documented.

8.6. Risk Management

8.6.1. Risk management function serves as the second line of defense within the institution's compliance risk management framework. Its primary role is to provide oversight, guidance, and independent review to the first line of defense, ensuring that compliance risks are properly identified, assessed, and managed across all business activities.

8.6.2. The risk management function is responsible for advising compliance risk policies, monitoring frameworks, and reporting mechanisms, as well as challenging and validating the adequacy of controls implemented by operational units. Key responsibilities of the risk management function in compliance risk management shall include:

(a) developing, maintaining, and periodically updating methodologies for assessing compliance risk, ensuring they reflect regulatory developments, industry best practices and changes in the institution's risk profile. This includes providing tools, templates, and guidance to help business units in conducting compliance risk assessments.

(b) independently validating compliance risk assessments submitted by business units to ensure accuracy, completeness, and consistency across the institution. It shall consolidate institution-wide assessments to determine overall compliance risk exposure and trends.

(c) monitoring compliance risk indicators, emerging regulatory issues, and stress-testing results. Stress testing shall include scenario analyses involving major regulatory changes or enforcement actions.

(d) ensuring that compliance risk is integrated into the institution's enterprise risk management framework, including risk appetite, capital planning, operational risk assessments and strategic planning.

(e) maintaining a robust Management Information System (MIS) capable of capturing, measuring, and reporting compliance risk in a timely and accurate manner. The MIS shall support automated and manual data collection, analysis, and reporting. It shall be aligned with the size, complexity, and technological maturity of the institution. Further, MIS shall be able to generate exception reports and trend analyses to support decision-making at the Senior Management and Board level.

(f) submitting regular reports, at least monthly, to senior management. The reports shall include the following, as applicable:

(i) the institution's compliance with applicable laws, regulations and other compliance obligations based on the monitoring and testing exercise of the compliance function;

(ii) results of the compliance risk assessment made during the reporting period;

(iii) changes in the compliance risk profile, including relevant risk indicators;

(iv) identified breaches, incidents, deficiencies and the impact (financial and non-financial) and the corrective measures taken/ to be taken;

(v) changes in relevant legal, regulatory, and other compliance obligations including measures being taken for timely compliance; and

(vi) observations regarding the compliance culture prevailing across the financial institution.

8.7. Internal Audit

8.7.1. Internal Audit shall evaluate the adequacy and effectiveness of the institution's compliance risk management framework. This includes the independence of the compliance function, robustness of operational controls and adherence to policies and regulatory requirements.

8.7.2. Review of compliance risk shall be incorporated into the Internal Audit annual plan using a risk-based approach. Internal Audit function, within its scope of operations, shall cover the following areas as part of its review of compliance risk management:

(a) verification of implementation of compliance policies and procedures by business units.

(b) assessment of the adequacy of controls to mitigate risks of fraud, regulatory breaches, mis-selling, customer harm and reputational damage.

(c) determination of whether senior management implements corrective actions promptly and effectively when compliance issues are identified.

(d) ensure frequency of audit review and scope reflect the institution's compliance risk exposure.

(e) review of compliance with relevant laws, regulations, circulars, and other directives issued by the Bank.

(f) assessment of business units and risk management monitoring of compliance risk indicators.

(g) review of the quality, timeliness and accuracy of compliance risk reports submitted to senior management and the board of directors.

8.7.3. Internal Audit must remain independent of the Compliance Function to ensure that its evaluation is objective. However, it must keep the Head of Compliance informed of all audit findings related to compliance risk for follow-up.

8.7.4. Audit reports must clearly highlight deficiencies, root causes and recommendations for strengthening compliance risk management. Follow-up audits shall be conducted to confirm closure of identified issues.