RISK MANAGEMENT GUIDELINES

January 2013

TABLE OF CONTENTS

1. 0 OVERVIEW OF RISK MANAGEMENT FRAMEWORK

1.1 Introduction

The Central Bank of Kenya has put forward this document for the purpose of providing guidelines to all institutions on minimum requirements for risk management systems and frameworks. For the purpose of these guidelines, financial risk in a banking organization is the possibility that the outcome of an action or event could bring about adverse impacts on the institution's capital or earnings. Such outcomes could either result in direct loss of earnings/capital or may result in imposition of constraints on bank's ability to meet its business objectives.

Risk Categories

While the types and degree of risks an organization may be exposed to depend upon a number of factors such as its size, complexity, business activities, and volume, these guidelines have identified the following categories of risks as critical risks in financial institutions:-

1. Strategic Risk
2. Credit Risk
3. Liquidity Risk
4. Market Risk
5. Operational Risk
6. Information and Communication Technology Risk
7. Reputational Risk
8. Compliance Risk and
9. Country and Transfer Risk

Risk Management Function

In accordance with the Basel Core Principles for Effective Banking Supervision, 'Risk Management Processes' requires that *banks and banking groups must have comprehensive risk management processes (including Board and senior management oversight) to identify, evaluate, monitor and control or mitigate all material risks and to assess their overall capital adequacy in relation to their risk profile. These processes should be commensurate with the size and complexity of the institution*.

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

behalf of the institution and should report directly to the board or a committee of the board.

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

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

Risk Management Process.

Regardless of the Risk Management Programme design, each programme should include:

Risk Identification: Almost every product and service offered by institutions has a unique risk profile composed of multiple risks. For example, at least four types of risks are usually present in most loans: credit risk, interest rate risk, liquidity risk and operational risk. Risk identification should be a continuing process and risk should be understood at both the transaction and portfolio levels.

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

Risk Control: Once risks have been identified and measured for significance, there are basically three ways to control significant risks, or at least minimize their adverse consequences: avoiding or placing limits on certain activities/risks, mitigating risks and/or offsetting risks. It is a primary management function to balance expected rewards against risks and the expenses associated with controlling risks. Institutions should establish and communicate risk limits through policies, standards and procedures that define responsibility and authority.

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

of changes in interest rate risk is very important. In general, 'monitoring risks' means developing reporting systems that identify adverse changes in the risk profiles of significant products, services and activities and monitoring changes in controls that have been put in place to minimize adverse consequences.

1.2 BASIC ELEMENTS OF A SOUND RISK MANAGEMENT SYSTEM

The risk management program of each institution should at least contain the following elements of a sound risk management system:

1.2.1 Active Board and Senior Management Oversight

Boards have ultimate responsibility for the level of risk taken by their institutions. Accordingly, they should approve the overall business strategies and significant policies of their organizations, including those related to managing and taking risks and should ensure that senior management is fully capable of managing the activities that their institutions conduct. All boards of directors are responsible for understanding the nature of the risks significant to their organizations and for ensuring that the management is taking the steps necessary to identify measure, monitor and control these risks.

The level of technical knowledge required of directors may vary depending on the particular circumstances at the institution. Consequently, what is most important is for directors to have a clear understanding of the types of risks to which their institutions are exposed and to receive regular reports that identify the size and significance of the risks in terms that are meaningful to them. Directors could take steps to develop an appropriate understanding of the risks their institution face, possibly through briefings from auditors and experts. Using this knowledge and information, directors should provide clear guidance regarding the level of exposures acceptable to their institutions and have the responsibility to ensure that senior management implements the procedures and controls necessary to comply with adopted policies.

Senior management is responsible for implementing strategies in a manner that limits risks associated with each strategy. Management should therefore be fully involved in the activities of their institutions and possess sufficient knowledge of all major business lines to ensure that appropriate policies, controls and risk monitoring systems are in place and that accountability and lines of authority are clearly delineated. Senior management is also responsible for establishing and communicating a strong awareness of and need for effective internal controls and high ethical standards. Meeting these responsibilities requires senior managers of institutions to demonstrate a thorough understanding of developments in the financial sector and a knowledge of the activities their institution conducts, including the nature of the internal controls necessary to limit the related risks.

1.2.2 Adequate Policies Procedures and Limits

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

A bank's policies, procedures and limits should:

- Provide for adequate and timely identification, measurement, monitoring, control and mitigation of the risks posed by its lending, investing, trading, securitisation, off balance sheet, fiduciary and other significant activities at the business line and firm-wide levels;

- Ensure that the economic substance of a bank's risk exposures are fully recognised and incorporated into the bank's risk management systems;

- Be consistent with the bank's stated goals and objectives, as well as its overall financial strength;

- Clearly delineate accountability and lines of authority across the bank's various business activities, and ensure there is a clear separation between business lines and the risk function;

- Escalate and address breaches of internal position limits;

- Provide for the review of new businesses and products by bringing together all relevant risk management, control and business lines to ensure that the bank is able to manage and control the activity prior to it being initiated; and

- Include a schedule and process for reviewing the policies, procedures and limits and for updating them as appropriate.

1.2.3 Adequate Risk Monitoring and Management Information Systems (MIS)

Effective risk monitoring requires institutions to identify and measure all material risk exposures. Consequently, risk-monitoring activities must be supported by information systems that provide senior managers and directors with timely reports on the financial condition, operating performance and risk exposure of the institution. The sophistication of risk monitoring and MIS should be consistent with the complexity and diversity of the institution's operations. Every institution shall require a set of management and board

reports to support risk-monitoring activities. These reports may include daily or weekly balance sheets and income statements, a watch list for potentially troubled loans, a report of overdue loans, simple interest rate risk report and other relevant reports.

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

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

1.2.4 **Adequate Internal Controls**

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

When properly structured, a system of internal controls promotes effective operations and reliable financial and regulatory reporting, safeguards assets and helps to ensure compliance with relevant laws, regulations and institutional policies. Internal controls should be tested by an independent and suitably qualified internal auditor who reports directly to the board’s Audit Committee. Given the importance of appropriate internal controls to institutions, the results of audits or reviews, conducted by an internal auditor or other persons, should be adequately documented, as should management’s responses to them. In addition, communication channels should exist that allows negative or sensitive findings to be reported directly to the board’s Audit Committee.

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

- The system of internal controls should be appropriate to the type and level of risks posed by the nature and scope of the institution's activities.

- The institution's organisational structure should establish clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits.

- Reporting lines should provide sufficient independence of the control areas from the business lines and appropriate segregation of duties throughout the institution such as those relating to trading, custodial, and back-office activities.

- Official institutional structures should reflect actual operating practices.

- Financial, operational, and regulatory reports should be reliable, accurate and timely; wherever applicable, exceptions are noted and promptly investigated.

- Adequate procedures for ensuring compliance with applicable laws and regulations should be in place.

- Internal audit or other control review practices should provide for independence and objectivity.

- Internal controls and information systems should be adequately tested and reviewed; the coverage, procedures, findings, and responses to audits and review tests should be adequately documented; identified material weaknesses should be given appropriate and timely high level attention; and management's actions to address material weaknesses should be objectively verified and reviewed.

- The institution's audit committee or board of directors should review the effectiveness of internal audits and other control review activities on a regular basis.

2.0 STRATEGIC RISK MANAGEMENT

2.1 Introduction

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

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

2.2 Board and Senior Management Oversight

2.2.1 Specific responsibilities for the Board

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

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

2.2.2 Specific responsibilities of senior management

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

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

2.3 Policies and Procedures and Limits

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

Procedures for defining and reviewing the institutions' business strategy are intended to ensure that the following aspects are given adequate consideration:

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

Limits are necessary in defining*:*

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

2.3.1 Strategic risk management process

An effective strategic management process should include the following:

2.3.1.1 Strategic Planning

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

A strategic planning process has three basic elements

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

2.3.1.2 Setting of Strategic goals and objectives

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

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

2.3.1.3 Development of strategies

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

The process involves understanding of the general banking, business and economic environment that an institution operates in, assess its strength and weaknesses and analyze its position and possible strategies that can be considered having regards to its stated goals and objectives and risk tolerance.

2.3.1.4 Formulation of strategic plan

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

Strategic decisions agreed upon during the planning process should form the basis of the strategic plan. Apart from describing what strategies the institution will take and how the institution will implement them to meet its strategic goals and objectives, the plan may also provide other information, such as the institution's philosophy towards its business, its growth targets, the extent of its financial risk-taking, and other relevant factors (institutional and environmental) affecting its growth and development. The depth and coverage of the strategic plan should be commensurate with the institution's scale and complexity of business.

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

Institutions which are branches or subsidiaries of a foreign bank should have their own strategic plan for strategic risk management purposes if the group's strategic plan is not adequate to fully reflect their local situation, needs and activities.

2.3.2 Alignment and change management

Before implementing their strategies, institutions should ensure that they have made proper alignment of internal resources and processes and, if necessary, managed all change issues (such as those arising from organisational or cultural changes) to facilitate the achievement of desired outcomes. Interdependencies between processes across departments (e.g. reconciliation of transaction information between front and back offices using a more advanced IT system) should also have been addressed so that they can be properly understood and accounted for during the implementation.

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

- sufficient resources (financial and non-financial) have been allocated to undertake the necessary tasks;
- the right people have been put in the right place; and
- the organisation and risk management structure, systems, infrastructure and technology are in the right shape to support the new initiatives.

2.4 Measuring and monitoring

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

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

Where institutions have identified strategic issues arising from anticipated operational or market changes which may result in a significant adverse impact on their business or financial conditions, such issues should be reported to the Board and senior management in a timely manner, with an assessment of the strategic risk implications and the need for taking remedial actions (such as modifying existing strategies and implementing risk mitigating or contingency measures).

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

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

- Exposure to different sectors, and associated sector risks.

2.4.1 Performance evaluation and feedback

Comparison of actual performance to desired outcomes serves as an important check on the success of implementing approved strategies, and allows management to take timely remedial actions to address significant deviations from set targets. Therefore, institutions are expected to develop a performance evaluation system that tracks progress towards achieving both financial and non-financial targets.

In order to ensure efficient and continuous performance evaluation, at the setting of strategic goals and targets stage, long term goals and targets should be broken down in short term (preferably yearly) measurable goals and targets.

2.4.2 Other Supporting Processes

2.4.2.1 Planning and Management of Capital and Funding needs

Inadequate planning of capital and funding needs is an obstacle to implementing strategic decisions and can have a disruptive effect on an institution operations and its ability to meet strategic goals and objectives. As such, institutions should view such planning as a crucial element of the strategic planning process.

Capital planning should be risk-based and forward-looking, and take into account such factors as an institution's current and future capital needs, anticipated capital expenditures, dividend payment forecasts, desirable capital levels, and external capital sources (e.g. available supply of capital and capital raising options)

2.4.2.2 Management Information System

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

2.4.2.3 Human resources management and development

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

2.4.2.4 Succession Planning

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

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

2.4.3 Stress-Testing and Contingency Strategies

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

Stress-testing does not necessarily mean the use of sophisticated financial modelling tools, but rather focuses on the need for institutions to evaluate in some way the potential impact (both financial and non-financial) different stress scenarios may have on their business. The level of resources devoted to this effort should be commensurate with the nature, scale and complexity of institutions' business activities.

2.5 Internal audit and controls

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

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

The results of such audit reviews, including any issues and weaknesses identified should be reported to the Board and senior management directly. Both the Board, and a delegated committee (e.g. Board Audit Committee), and senior management should be sufficiently engaged in the process to determine whether such reviews and audits are effectively performed (e.g. whether the performing staff are independent and have sufficient authority to perform their duties) and identified issues are addressed.

3.0 CREDIT RISK MANAGEMENT

3.1 Introduction

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

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

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

3.2 Board and Senior Management Oversight

3.2.1 The Board of Directors

The board of directors carries the ultimate responsibility of approving and reviewing the credit risk strategy and credit risk policies of the bank. This role is part of the board's ultimate responsibility of offering overall strategic direction to the bank. The credit risk strategy should clearly set the acceptable risk appetite and tolerance the institution is willing to engage, and the level of profitability the bank expects to achieve for incurring the various credit risks. The credit policies should be adequate and must cover all the activities in which credit exposure is a significant risk. The board should ensure that:

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

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

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

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

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

- The delegation authority and approval levels are clearly defined.

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

3.2.2 Senior Management

The senior management has the responsibility of implementing the credit strategy approved by the board of directors and developing policies and procedures for effective management of the credit risk. The senior management should ensure the following:

- The credit granting activities conform to the laid down strategy.

- Written procedures have been developed, implemented and responsibilities of the various functions are clearly defined.

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

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

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

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

3.3 Policies, Procedures and Limits

3.3.1 Policies relating to limits

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

An effective credit policy should outline the following:-

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

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

- The policy should require that the board approve all loans to related or connected parties. These credits should be based on market terms and should not be more favourable with regard to amount, maturity, rate and collateral than those provided to other customers.

- On exposure limits the policies should include the following:

    - Acceptable exposure to individual borrowers.
    - Maximum exposure to connected groups and insider dealings.
    - The total overall limit on the credit portfolio in relation to capital, assets or liabilities.
    - Limits in relation to geographical location.

- Maximum exposure to individual economic sectors (for example commercial, consumer, real estate, agricultural).
- Acceptable limits on specific products.

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

3.3.2 Segregation of Duties

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

3.3.3 Policies relating to credit products

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

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

3.3.4 Policies relating to credit assessment and granting process

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

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

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

Also lending authority delegated to staff with clearly established limits should be documented. It is important to include the functions and reporting procedures of the various committees and individual lending officers.

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

3.3.5 Credit risk mitigation techniques

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

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

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

The institution should primarily assess the borrower's capacity to repay and should not use collateral to compensate for insufficient information.

3.3.6 Internal Risk Rating Systems

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

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

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

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

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

3.3.7 Policies on Management of problem credits

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

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

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

3.3.8 Policies on Inter-bank transactions

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

- The establishment and observation of counter party credit limits.
- Any inter-bank transaction for which specific provisions should be made.
- The method and accuracy of reconciliation of the nostro and vostro accounts.
- Any inter-bank credit with terms of pricing that is not a market norm.
- The concentration of inter–bank exposure with a detailed listing of banks and amounts outstanding as well as lending limits.

3.3.9 Provisioning policy

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

3.4 Measuring and Monitoring Credit Risk

3.4.1 Measuring Credit risk

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

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

The measurement of the risk should take into account the nature of the credit, maturity, exposure, profile, existence of collateral or guarantees and potential for default. The institution should also undertake an analysis of the whole economy or in particular sectors to ensure contingency plans are developed for higher than expected levels of delinquencies and defaults.

An important tool in monitoring the quality of individual credits, as well as the total portfolio, is the use of an internal risk rating system. A well-structured internal risk rating system is a good means of differentiating the degree of credit risk in the different credit exposures of a bank. This will allow more accurate determination of the overall characteristics of the credit portfolio, concentrations, problem credits, and the adequacy

of loan loss reserves. More detailed and sophisticated internal risk rating systems, used primarily at larger banks, can also be used to determine internal capital allocation, pricing of credits, and profitability of transactions and relationships.

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

3.4.2 Monitoring Credit Risk

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

Financial Position and Business Conditions

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

Conduct of Accounts

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

Loan Covenants

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

Status and Valuation of Collateral

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

External Rating and Market Price

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

Force Majeure Situation

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

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

3.4.3 Credit administration

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

- Credit application.
- Evidence of approval.
- Latest financial information.
- Record and date of all credit reviews.
- Record of all guarantees and securities.
- Record of terms and conditions of facility.
- Evidence of securities validation function that should include legal validity, existence, valuation, registration of charge and safekeeping.
- Internal rating.

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

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

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

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

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

d. Loan Repayment - The obligors should be communicated to ahead of time as and when the principal/markup installment becomes due. Any exceptions such as non-payment or late payment should be tagged and communicated to the management. Proper records and updates should also be made after receipt.

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

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

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

While in small institutions, it may not be cost effective to institute a separate credit administrative set-up, it is important that in such institutions individuals performing sensitive functions such as custody of key documents, wiring out funds, entering limits into system, should report to managers who are independent of business origination and credit approval process.

3.4.4 Credit exposure and risk reporting

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

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

3.5 Stress testing

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

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

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

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

3.6 Internal controls and audit

Institutions should have in place an independent internal system for assessment of the credit risk management process. This function is necessary in order to independently enable the board determine whether the risk management process is working effectively. The results of these audits should be communicated promptly to the directors and senior management. The review should provide sufficient information to the board and management to enable them evaluate accurately performance and condition of the portfolio. The credit review function should report directly to the board of directors or a board audit committee.

A review of the lending process should include analysis of the credit manuals and other written guidelines applied by various departments of a bank, and the capacity and actual performance of all departments involved in the credit function. It should also cover origination, appraisal, approval, disbursement, monitoring, collection and handling procedures for the various credit functions provided by the institution.

The internal audit review team should ensure the following:-

- The credit granting function is carried out effectively.
- The credit exposures are within the prudential and internal limits set by the board.
- Validation of significant change in the risk management process.
- Verification of the consistency, timeliness and reliability of data used for internal risk rating system.
- Compliance with the institution's credit policies and procedures.
- Adherence to internal risk rating system.
- Identification of areas of weaknesses in the credit risk management process.
- Exceptions to the policies, procedures and limits.

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

4.0 LIQUIDITY RISK MANAGEMENT

4.1 Introduction

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

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

Liquidity risk management systems involves not only analyzing banks on and off balance sheet positions to forecast future cash flows but also how the funding requirements could be met. The latter involves identifying the funding market to which the bank has access, understanding the nature of those markets, evaluating the bank's current and future use of the market and monitoring signs of erosion of confidence.

4.2 Board and Senior Management Oversight

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

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

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

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

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

A sound framework for managing liquidity risk has three dimensions:
- maintaining a stock of liquid assets that is appropriate to the institution's cash flow profile and that can be readily converted into cash without incurring undue capital losses;
- measuring, controlling and scenario testing of funding requirements; and
- Managing access to funding sources.

4.3 Policies, Procedures and Limits

4.3.1 Policies

Institutions should formulate a comprehensive and responsive liquidity policy statement that takes into account all on- and off-balance sheet activities and should be recommended by senior management and approved by the board of directors. While specific details vary across institutions according to the nature of their business, the key elements of any liquidity policy should include:
- General liquidity strategy (short- and long term), specific goals and objectives in relation to liquidity risk management, process for strategy formulation and the level of approval within the institution;
- Roles and responsibilities of individuals performing liquidity risk management functions, including structural balance sheet management, pricing, marketing, contingency planning, management reporting, lines of authority and responsibility for liquidity decisions;

- Liquidity risk management structure for monitoring, reporting and reviewing liquidity;
- Liquidity risk management tools for identifying, measuring, monitoring and controlling liquidity risk (including the types of liquidity limits and ratios in place and rationale for establishing limits and ratios);
- Where an institution is actively involved in multiple currencies and/ or where positions in specific foreign currencies are significant to its business, its liquidity policy should address the measurement and management of liquidity in these individual currencies which should include a back-up liquidity strategy for circumstances in which its normal access to funding in individual foreign currencies is disrupted; and
- Contingency plan for handling liquidity crisis.

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

4.3.2 Procedures

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

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

4.3.3 Limits

Limits should be set which should be appropriate to the size, complexity and financial condition of the financial institution. The limits should be periodically reviewed and adjusted when conditions or risk tolerances change. When limiting risk exposure, senior management should consider the nature of the institution's strategies and activities, its past performance, the level of earnings, capital available to absorb potential losses, and the board's tolerance for risk. Institutions may use a variety of ratios to quantify liquidity and create limits for liquidity management.

In addition, balance sheet complexity will determine how much and what types of limits a bank should establish over daily and long-term horizons. While limits will not prevent liquidity crisis, limit exceptions can be early indicators of excessive risk or inadequate liquidity risk management.

4.4. Measuring and Monitoring Liquidity Risk

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

An effective measurement and monitoring system is essential for adequate management of liquidity risk. Consequently, institutions should institute systems that enable them to capture liquidity risk ahead of time, so that appropriate remedial measures could be prompted to avoid any significant losses. An effective liquidity risk measurement and monitoring system not only helps in managing liquidity in times of crisis but also optimize return through efficient utilization of available funds. Key elements of an effective risk management process include an efficient Management Information System (MIS), systems to measure, monitor and control risks.

Every institution's MIS should be integrated to the overall management information systems of the institution, and thus link various units related to treasury activities, i.e. the dealing, the treasury operation and risk management department. A strong management information system that is flexible enough to deal with various contingencies that may arise is central to making sound decisions related to liquidity.

4.4.1 Measurement of liquidity position

The following are the indicators that a bank should utilise at a minimum, to measure its liquidity position. A bank must establish appropriate internal guidelines on the level of the ratio and ensure prompt corrective actions are undertaken to address any liquidity shortfall. It should be noted that the measures outlined in 4.4.1.3 developed by the Basel Committee on Banking Supervision are intended to come into effect in 2015. Institutions are encouraged to refer to the measures in 4.4.1.3 to strengthen their liquidity risk management frameworks.

4.4.1.1 Minimum Liquidity Ratio

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

4.4.1.2 Loan to Deposit Ratio

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

4.4.1.3 Liquidity Coverage Ratio

The LCR is intended to promote resilience to potential liquidity disruptions over a thirty day horizon. The ratio ensures that institutions have sufficient unencumbered, high-quality liquid assets to offset the net cash outflows it could encounter under an acute short-term stress scenario.

LIQUIDITY COVERAGE RATIO =

$$\frac{\text{Stock of High Quality Liquid Assets}}{\text{Total Net Cash outflow Over 30 Day Period}} \geq 100\%$$

High quality liquid assets include 'liquid assets' specified in the Banking Act Section 19 (2) (a) to (e) and any other assets with the following characteristics:-

Low credit risk – Risk of default by the counterparty is low.
Low market risk- The asset should be easily traded in a developed, recognized and active market.

Net cash outflows are defined as cumulative expected cash outflows minus cumulative expected cash inflows arising in the specified stress scenario in the time period under consideration. This is the net cumulative liquidity mismatch position under the stress scenario measured at the test horizon.

Cumulative expected cash outflows are calculated by multiplying outstanding balances of various categories or types of liabilities by assumed percentages that are expected to roll-

off, and by multiplying specified draw-down amounts to various off-balance sheet commitments. Cumulative expected cash inflows are calculated by multiplying amounts receivable by a percentage that reflects expected inflow under the stress scenario.

4.4.1.4 Net Stable Funding Ratio (NSFR)

Stable Funding is funding which is not susceptible to fluctuations and is readily available at affordable cost and for a longer period of time (at least one year). The NSFR requires a minimum amount of stable sources of funding at an institution relative to the liquidity profiles of the assets, as well as the potential for contingent liquidity needs arising from off-balance sheet commitments, over a one-year horizon. The NSFR aims to limit over-reliance on short-term wholesale funding during times of buoyant market liquidity and encourage better assessment of liquidity risk across all on- and off-balance sheet items.

$$\frac{\text{Available amount of Stable Funding}}{\text{Required amount of Stable Funding}} \geq 100\%$$

Available amount of Stable Funding (ASF)

The ASF comprises of the bank's capital, preferred stock and liabilities with maturities greater than or equal to one year, portions of demand and term deposits by retail customers and wholesale funding having residual maturities < 1 year which are not expected to be withdrawn during the stress event. It does not include borrowings from the central bank other than those available through regular open market operations.

Each of these components are slotted into 4 separate ASF categories which are assigned ASF factors representing the amount of that components' carrying value that will be included in the calculation of the numerator of the ratio.

Broadly the available amounts of Stable Funding (ASF) factors are as given below.

- Bank's capital, preferred stock and liabilities with maturities greater than or equal to one year will be assigned a factor of 100%.
- Stable and less stable portions of demand and term deposits by retail customers having residual maturities < 1 year will be assigned ASF factors of 90% and 80% respectively.
- Unsecured wholesale funding having residual maturities < 1 year will have an ASF factor of 50%.
- All other liabilities and equity categories not specified in the ASF categories mentioned will be assigned a factor of 0%.

The available amount of stable funding is calculated as the weighted sum of the carrying values of each ASF component where the weights are ASF factors assigned to each component category.

Required amount of Stable Funding (RSF)

As in the case of the numerator of the NSFR ratio, the RSF is calculated as the weighted sum of the value of assets held and funded by the entity including off-balance sheet exposures where the weights are RSF factors assigned to each RSF asset category. The weights represent the portion of the asset that would not be able to be monetized either by its sales or its use as collateral in an extended firm-specific liquidity stress scenario-assets. In effect that would need to be covered by more stable sources of funds.

Hence more liquid assets will be assigned a lower RSF factor whereas a higher RSF factor will be applied to values of the more illiquid assets. A brief outline of asset categories and RSF factors is given below:

- Cash, unencumbered short-term unsecured actively traded securities, securities with exactly offsetting reverse repo, securities and non-renewable loans with residual maturities $<$ 1 year will have an RSF factor of 0%.
- Unencumbered debt issued or guaranteed by sovereigns, central banks, BIS, IMF, EC and PSEs/ multilateral development banks with risk weights of 0% under the Basel II standardized approach are assigned a RSF factor of 5%.
- Unencumbered non-financial sector corporate and covered bonds having residual maturities $>$ 1 year with rating grade of AA- or higher and debt issued or guaranteed by sovereigns, central banks, PSEs with risk weights of 20% are assigned a RSF factor of 20%.
- Unencumbered listed equity securities or non-financial senior unsecured corporate bonds with residual maturities $>$ 1 year and rating grades A+ to A-, gold and loans to non-financial corporate clients, sovereigns, central banks and PSEs with residual maturities $>$ 1 year will have an RSF factor of 50%.
- Unencumbered residential mortgages of any residual maturity and non-financial entity loans with residual maturities $>$ 1 year having risk weights of 35% will be assigned a RSF factor of 65%.
- Unencumbered retail loans with residual maturities $<$ 1 year will have an RSF factor of 85%.
- All other assets are assigned an RSF factor of 100%.
- Off-balance sheet undrawn committed credit and liquidity lines are assigned RSF factors of 5%.

4.4.1.5 Maturity Profile

Analyzing funding requirements involves the construction of a **maturity profile.** A cash flow projection estimates a bank's inflows and outflows and thus establishes net deficit or surplus **(GAP**) over time horizon. It takes into account the institution's funding requirement arising out of distinct sources on different time frames.

Maturity profiles will depend heavily on assumptions regarding future cash flows associated with assets, liabilities and off-balance sheet items.

Institutions should review the assumptions utilized in managing liquidity frequently to determine that they continue to be valid, since an institution's future liquidity position will be affected by factors that cannot always be forecast with precision given the rapidity of change in financial markets.

4.4.2 Monitoring Liquidity

4.4.2.1 Management Information

An institution should have a reliable management information system designed to provide the board of directors, senior management and other appropriate personnel with timely and forward-looking information on the liquidity position of the bank. The management information system should have the ability to calculate liquidity positions in all of the currencies in which the bank conducts business. To effectively manage and monitor its net funding requirements, an institution should have the ability to calculate liquidity positions on an intraday basis, on a day-to-day basis for the shorter time horizons, and over a series of more distant time periods thereafter. The management information system should be used in day-to-day liquidity risk management to monitor compliance with the bank's established policies, procedures and limits.

4.4.2.2 Key Liquidity Factors

The following key liquidity factors should be monitored closely:

- The maturity profile of cash flows under varying scenarios;
- The stock of liquid assets available to the institution and their market values;
- The ability of an institution to execute assets sales in various markets (notably under adverse conditions) and to borrow in markets;
- Potential sources of volatility in assets and liabilities (and claims and obligations arising from off-balance sheet business);
- The impact of adverse trends in asset quality on future cash flows and market confidence in the bank;
- Credit standing and capacity of providers of standby facilities to meet their

obligations;

- The impact of market disruptions on cash flows and on customers;
- Intra-group cash flows and the accessibility of intra-group funding; and
- The type of new deposits being obtained, as well as its source, maturity, and price.

4.4.2.3 Asset Liability Committee (ALCO)

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

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

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

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

4.4.3 Contingency Planning

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

- Provide specific procedures to ensure timely and uninterrupted information flows to senior management.
- Clear division of responsibility within management in a crisis.

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

4.4.4 Stress Testing

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

Stress testing involves subjecting institution's liquidity position to several scenarios and assessing whether the institution can withstand liquidity shocks. The scenario entails a significant stress, albeit not a worst-case scenario, and assumes the following:

- a significant downgrade of the institution's public credit rating;
- loss of major deposits;
- a significant change in market interest rates;
- a significant increase in demand for loans and other funding;
- increases off-balance sheet exposures, including committed credit and liquidity facilities.

4.5.5. Internal Controls and Audit

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

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

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

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

5.0 MARKET RISK MANAGEMENT

5.1 Introduction

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

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

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

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

- Interest rate risk
- Price Risk
- Foreign Exchange risk

5.1.1 Interest rate risk

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

5.1.2 Price Risk

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

5.1.3 Foreign Exchange risk

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

5.2 Board and Senior Management Oversight

5.2.1 The Board of Directors

The board of directors has the ultimate responsibility for understanding the nature and the level of market risk taken by the institution. The board therefore has the following principal responsibilities:

- To formulate and approve broad business strategies and policies that govern or influence the market risk of the institution. Accordingly, the board of directors is responsible for approving the overall policies with respect to interest rate risk, price risk and foreign exchange and ensuring that management takes the steps necessary to identify, measure, monitor and control these risks.

- It should also review the overall objectives of the institution with respect to market risk and ensure the provision of clear guidance regarding the level of market risk acceptable to the institution.

- To approve policies that identify lines of authority and responsibility for managing market risk exposures. As such it is responsible for ensuring that the institution has adequate policies and procedures for managing market risk on both a long-term and day-to-day basis and that it maintains clear lines of authority and responsibility for managing and controlling this risk.

    - The board of directors should also review and approve the procedures to measure, manage and control price risk within which foreign exchange transactions shall be conducted.

- The board and senior management should therefore identify and have a clear understanding and working knowledge of the price risks inherent in the institution's investment portfolio and make appropriate efforts to remain informed about these risks as financial markets, risk management practices, and the institution's activities evolve.

- The board of directors should also review and approve the procedures to measure, manage and control foreign exchange risk within which foreign exchange transactions shall be conducted.

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

5.2.2 Senior Management

The senior management has the responsibility of implementing all approved policies that govern Market Risk and developing procedures for effective management of the risks.

1. Management should be mandated by the board to be responsible for maintaining:
- Appropriate limits on risk taking;
- Adequate systems and standards for measuring market risk;
- Standards for valuing positions and measuring performance;
- A comprehensive market risk reporting and review process.
- Effective internal controls.

2. Management should be sufficiently competent and able to respond to price risks, interest risks and foreign exchange risks that may arise from changes in the competitive environment or from innovations in markets in which the institution is active.

5.3 Policies, Procedures and Limits

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

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

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

An appropriate limit system should:-

- Enable management to control market risk exposures, initiate discussion about opportunities and risks and monitor actual risk taking against predetermined risk tolerances;
- Ensure that positions that exceed certain predetermined levels receive prompt management attention;
- Be consistent with overall approach to measuring market risk;
- Should be approved by the board of directors and re-evaluated periodically;
- Be appropriate to the size, complexity and capital adequacy of the institution as well as its ability to measure and manage its risk; and
- Be identifiable with individual business unit, portfolios, instrument types or specific instruments.

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

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

- Violation of approved responsibilities by managers when taking interest rate risk exposures. Or investing in un- approved instruments.

- Excesses over approved interest rate limits;
- Any exceptions highlighted by the internal auditor.

5.4 Measurement, Monitoring and Control

5.4.1 Approaches to measuring and limiting Market Risk

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

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

5.4.2 Stress tests

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

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

5.4.3 Assets and Liability Committee

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

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

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

5.4.4 Management Information System

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

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

- Summaries of the institution's aggregate exposures;
- Reports demonstrating the institution's compliance with policies and limits;
- Results of stress tests including those assessing breakdown in key assumptions and parameters;
- Summaries of the findings of reviews of interest rate risk, price risk, and foreign exchange risk;
- Policies, procedures, and the adequacy of the market risk measurement systems, including any findings of internal and external auditors/consultants;
- Maturity distribution by currency of the assets and liabilities for both on and off balance sheet items;
- Outstanding contracts by settlement date and currency;
- Total value of outstanding contracts, spot and forward;
- Gains and losses, totals and comparison to previous day's;

- Market value of off-balance sheet products and aggregate dealing limits;
- Exceptional reports e.g. Limit or line excesses;
- Total value of outstanding investments, and current market values;
- Profit and loss, totals and comparison to previous mark to market and aggregate investment limits
- Limit or sectoral excesses and valuation of option contracts, if any.

5.5 Internal Controls and Audit

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

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

An effective system of internal control for market risk includes:

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

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

6.0 OPERATIONAL RISK MANAGEMENT

6.1 Introduction

Operational risk has been defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk. It seeks to identify why a loss happened and at the broadest level includes the breakdown by four causes: people, processes, systems and external factors.

Institutions should develop, implement and maintain an enterprise-wide Operational Risk Management Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual institution will depend on a range of factors, including its nature, size, complexity and risk profile.

The policies defining the Framework should clearly

- Identify the governance structures used to manage operational risk, including reporting lines and accountabilities;
- Describe the risk assessment tools and how they are used;
- Describe the bank's accepted operational risk profile, permissible thresholds or tolerances for inherent and residual risk, and approved risk mitigation strategies and instruments;
- Describe the bank's approach to establishing and monitoring thresholds or tolerances for inherent and residual risk exposure;
- Establish risk reporting and Management Information System (MIS);
- Provide for appropriate independent review and assessment of operational risk; and
- Require the policies to be revised whenever a material change in the operational risk profile of the bank occurs.

6.2 Board and Senior Management Oversight

The board of directors should take the lead in establishing the "tone at the top" which promotes a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour.

6.2.1 Role of Board of Directors Oversight

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

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

6.2.2 Role of Senior Management

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

Senior Management responsibilities includes:-

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

6.3 Policies and Procedures

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

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

The review and approval process should consider:-

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

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

6.3.1 Policies on Outsourcing

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

Outsourcing policies and risk management activities should encompass:

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

6.4 Measuring, Monitoring and Control

6.4.1 Measuring operational risk

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

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

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

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

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

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

- **Scenario Analysis:** Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome.

On measuring operational risk capital charge, the institution will at a minimum be required to use basic indicator method to compute and quantify its operational risk and allocate capital.

6.4.2 Monitoring

An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss.

An institution should maintain a log of major operational risks events such as:-
- frauds and attempted frauds;
- robberies;
- breaches of the bank's risk appetite and tolerance level;
- details of recent significant internal and external operational risk events and losses;
- Any operational risk events witnessed in the financial industry and the how well the institution is prepared to mitigate such events;
- System downtime.

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

There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk. Management should ensure that information is received by the appropriate people, on a timely basis, in a form and format that will aid in the monitoring and control of the business. The reporting process should include information such as:-

- The critical operational risks facing the institution;
- Risk events and issues together with intended remedial actions;

- The effectiveness of actions taken;
- Details of plans formulated to address any exposures where appropriate;
- Areas of stress where crystallization of operational risks is imminent.

6.4.3 Control and Mitigation

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

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

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

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

Effective use and sound implementation of technology can contribute to the control environment. For example, automated processes are less prone to error than manual processes. However, automated processes introduce risks that must be addressed through sound technology governance and infrastructure risk management programmes.
The use of technology related products, services, delivery channels and processes exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks.

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

6.4.4 Stress Testing

An institution should conduct stress tests on a regular basis for a variety of short-term and protracted institution-specific and operational risks stress scenarios to identify sources of potential operational risks and to ensure that institution is prepared to continue in business after minor and major operational risk events. An institution should use stress test outcomes to adjust its operational risk management strategies, policies, and positions and to develop effective contingency plans

6.5 Internal controls and audit

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

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

7.0 INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) RISK

7.1 Introduction

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

7.2 Board and Senior Management Oversight

7.2.1 Specific Responsibilities for the Board of Directors

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

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

7.2.2 Specific Responsibilities for the Senior Management

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

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

7.2.3 Head of Information and Communication Technology

The following are the responsibilities of the Head of ICT:

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

7.2.4 Staffing of the Information and Communication Technology Unit:

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

- Verification of personal information including confirmation of personal identification issued by government, academic credentials, prior work experience, professional qualifications, certificates of good conduct by the Police;

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

7.2.5 Intellectual Proprietary Rights

Institutions should put in place policies and procedures to:

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

7.3 ICT Risk Management Framework

7.3.1 Information and Communication Technology Strategy

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

7.3.2 ICT Risk Management Policy

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

- Information security classification policy,
- System development, testing and maintenance policy,
- ICT operation and maintenance policy,
- Access control policy,
- Physical security policy,
- Change controls policy,
- Personnel security policy, and

- Business Continuity Planning and Crisis and Emergency Management procedure.

7.3.3 ICT Risk Identification

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

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

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

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

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

7.3.4 Identifying Vulnerabilities

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

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

- Vulnerability Scanners – software that can examine an operating system, network application or code for known flaws by comparing the system (or system responses to known stimuli) to a database of flaw signatures.
- Penetration Testing – an attempt by human security analysts to exercise threats against the system. This includes operational vulnerabilities, such as social engineering.

- Operational and Management Controls – A review of operational and management controls by comparing the current documentation to best practices (such as ISO 17799) and by comparing actual practices against current documented processes.

7.4 Risk Assessment, Measurement and Monitoring

7.4.1 Risk Assessment

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

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

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

7.4.2 Risk Measurement

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

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

- Assessment of the risk profile on IT outsourcing projects periodically.

7.4.3 ICT Risk Mitigation

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

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

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

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

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

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

  i) Top level reviews;
  ii) Controls over physical and logical access to data and system;

iii) Access granted on “need to know” and “minimum authorization” basis;
iv) A system of approvals and authorizations; and
v) A system of verification and reconciliation.

7.5 Information Security

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

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

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

The Information security policy should include the following areas:

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

7.5.1 Information Confidentiality

The Information and Communication Technology function of institutions should oversee the establishment of an information classification and protection scheme. All employees of the institution should be made aware of the importance of ensuring information confidentiality and provided with the necessary training to fully understand the information protection procedures within their responsibilities.

7.5.2 Authentication and Access Control

Institutions should have an effective process to manage user authentication and access control. Access to data and system should be strictly limited to authorized individuals whose identity is clearly established, and their activities in the information systems should be limited to the minimum required for their legitimate business use. An appropriate user authentication mechanism commensurate with the classification of information to be accessed should be adopted.

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

7.5.2.1 Physical Security Zones

Institutions should ensure all physical security zones, such as computer centres or data centres, network closets, areas containing confidential information or critical ICT equipment, and respective accountabilities are clearly defined, and appropriate preventive, detective, and curative control measures are put in place.

7.5.2.2 Logical Security Domains

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

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

7.6 Operating System and System Software

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

- Developing baseline security requirement for each operating system and ensuring all systems meet the baseline security requirement;
- Clearly defining a set of access privileges for different groups of users, namely, end-users, system development staff, computer operators, and system administrators and user administrators;
- Setting up a system of approval, verification, and monitoring procedures for using the highest privileged system accounts;
- Requiring technical staff to review available security patches, and report exceptions in the patch status to Head of ICT periodically; and
- Requiring technical staff to include important items such as unsuccessful logins, access to critical system files, and changes made to user accounts in system logs monitor the systems for any abnormal event manually or automatically, and report the monitoring periodically.

7.7 Application Software

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

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

7.8 Audit Trail

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

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

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

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

7.9 Encryption Technologies

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

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

7.10 Computing Equipment

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

7.11 Handling Consumer Information

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

7.12 Training

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

7.13 System Acquisition, Development, Testing and Maintenance

7.13.1 System Development

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

7.13.2 Project Risks

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

7.13.3 System Development Methodology

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

7.13.4 Reliability, Integrity, and Relevance

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

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

7.13.5 Data Integrity, Confidentiality, and Availability

Institutions should have in place a set of policies, standards, and procedures to ensure data integrity, confidentiality, and availability. These policies should be in accordance with the latest international data integrity and information security standards e.g. ISO 27001.

7.13.6 System upgrade

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

7.14 ICT Operations

7.14.1 Physical and Environmental Controls

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

7.14.2 Access by Third-party Personnel

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

7.14.3 Segregation of Duties

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

7.14.4 Documentation of operational instructions

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

7.14.5 Problem management

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

7.14.6 System monitoring

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

7.14.7 Capacity plan

Institutions should develop a capacity plan to cater for business growth and transaction

increases due to changes of economic conditions. The capacity plan should be extended to cover back-up systems and related facilities in addition to the production environment.

7.14.8 Record keeping

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

7.14.9 Change management

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

7.15 Business Continuity Management

7.15.1 BCP plans

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

7.15.2 Documentation

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

7.16 Outsourcing

7.16.1 Supervisory Duties

Institutions should not contract out their obligations to regulatory authorities and should take reasonable care to supervise the discharge of outsourced ICT functions. (See details in the Outsourcing Guideline CBK/PG/16)

7.16.2 Critical ICT Functions

Institutions should take particular care to manage material outsourcing arrangement (such

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

7.16.3 Risk Analysis

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

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

7.16.4 Data Security

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

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

7.16.5 Contingency Plan

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

service provider, and unexpected termination of the outsourcing agreement.

7.17 Internal Control and Audit

7.17.1 Systems Audit

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

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

7.17.2 Role of Internal Audit

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

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

7.17.3 Frequency of IT Internal Audit

Based on the nature, scale and complexity of its business, deployment of information and communication technology and ICT risk assessment, institutions should determine the scope and frequency of ICT internal audit. However, a comprehensive ICT internal audit shall be performed at a minimum once every 2 years.

7.17.4 Implementing System Development

Institutions should engage their Internal Audit and Risk Management functions when implementing system development of significant size and scale to ensure it meets the ICT Risk standards of the institution.

7.18 ICT External Audit

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

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

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

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

8.0 REPUTATIONAL RISK MANAGEMENT

8.1 Introduction

Reputational risk is the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions. This risk may result from an institution's failure to effectively manage any or all of the other risk types.

Managing reputational risk begins with recognizing that reputation is a matter of perception. An institution's overall reputation is a function of its reputation among its various stakeholders (investors, customers, suppliers, employees, regulators, politicians, non-governmental organizations, the communities in which the firm operates) in specific categories (product quality, corporate governance, employee relations, customer service, intellectual capital, financial performance, handling of environmental and social issues). A strong positive reputation among stakeholders across multiple categories will result in a strong positive reputation for the financial institution.

8.2 Board and Management Oversight

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

Management should fully understand all aspects of reputational risk and exhibit a clear commitment to compliance. The commitment should be communicated throughout the institution. Responsibility for corporate reputation is typically vested with the Chief Executive or the corporate communications department. Reputation risk falls between the two, cutting across many aspects of the business. It requires a small, cross-functional team to create and implement a protection strategy. This would typically comprise a representative from corporate communications, customer relations, the health and safety department, investor relations, the legal department, operations, public affairs, and risk management, with input from the chief executive or chairman.

The board should approve a reputational risk strategy and establish a management structure capable of implementing that strategy. The board should review the strategy regularly to ensure that the institution is managing the reputational risks. This review process should also aim to incorporate industry innovations (such as the internet) in reputational risk management into the institution's systems and processes.

8.3 Policies, Procedures and Limits

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

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

- **Management Integrity** – The personal ethics and behavior of directors and senior management (e.g. the Chief Executive and key managers) are important determinants of stakeholder confidence, the probity and conduct of such persons will always be under close scrutiny by its stakeholders.

- **Staff competence / support** - Staff competence and support is essential for business success. Given that human capital is an important asset, an institution's ability to harness it to meet their business objectives will enhance reputation. Deficiencies in employment and staff management practices could lead to various problems, including high staff turnover, insufficient staffing, poor service quality, staff incompetence / misconduct, customer complaints and employee disputes. Some of these problems may result in adverse publicity.

- **Corporate culture** - If the corporate culture is seen to inadequately support the achievement of its business objectives and effective risk management, it may arouse stakeholder concerns and result in a loss of confidence. It is therefore crucial to promote a corporate culture where:
    - the adoption of ethical and responsible behaviour that can protect and enhance their reputation is encouraged;
    - compliance issues or lax control standards are not tolerated; and
    - there is an established mechanism for employees to voice concerns if they are aware of any potential threats to reputation (e.g. business malpractices, suspicion of fraud, etc).

8.4 Risk Measurement, Monitoring and Management Information System

8.4.1 Reputational Risk Identification and Measurement

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

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

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

1. **Financial soundness / business viability** – An institution's reputation is likely to suffer if its financial soundness or business viability is called into question. For example, substantial losses resulting from unsuccessful investments or business operations may spark immediate concerns from stakeholders (in particular, shareholders, investors, or analysts) about whether the institution is still a safe investment or of long term business value. Such concerns may spread quickly to other aspects of reputation (e.g. management competence) as well.

2. **Business practices –**Institutions are required to run their businesses in a responsible, honest and prudent manner. Business practices which deviate from this basic standard could erode stakeholder confidence and irreparably damage their reputation, and any resultant breach of laws and regulations (e.g. adopting improper selling practices, engaging in unauthorized activities, etc.) may lead to investigations, disciplinary actions and criminal charges. In dealing with customers and other counterparties, they should be guided by, and closely adhere to, all relevant ethical standards, consumer protection provisions and codes of conduct.

3. **Fraudulent Activities** – Fraudulent activities perpetrated through a bank whether externally or internally schemed can damage the reputation of an institution. To mitigate this risk, sound internal controls should be put in place to guard against this risk.

4. **Litigations** – Litigations, for or against the bank, if not properly handled, could have a negative impact on the image of the bank. When dealing with litigations, institutions should take cognisance of the reputational risk and take appropriate measures to manage the risk.

5. **Customer satisfaction -** The ability to satisfy customer needs and expectations on a continuing basis is of paramount importance in sustaining their business in a highly competitive banking environment. Failure to do so, as illustrated by the following examples, may result in loss of customer confidence, falling business, adverse publicity or, in some cases, legal sanctions:

   - Unfair treatment of customers – customers may have been overcharged or inaccurately billed, or have suffered losses due to errors or omissions (e.g. customer instructions not being properly executed) without obtaining fair compensation; Mishandling of customer information – customers' confidential information may have been inadvertently destroyed, lost or exposed to third parties, thereby breaching confidentiality obligations and privacy rules relating to personal data;

   - Unreliable / inefficient banking services – frequent system outages, significant operational errors and oversight, inefficient processing systems and inefficient customer services will weaken customer confidence and lack of capacity to deliver quality services. Lack of new / innovative products and services to suit changing customer needs may also arouse discontent;

   - Mis-handling of customer complaints – customers expect banks to be responsive to their concerns. A poor complaint-handling system runs the risk of damaging customer goodwill and overlooking early indicators of potential threats to reputation; and

   - Business malpractices – customer confidence will be greatly impaired if institutions are found to have engaged in improper or illegal business practices.

6. **Anti-Money Laundering (AML) Concerns –**Institutions are required to be vigilant to ensure they are not used as conduits for Money Laundering as this will expose the institution to Reputation Risk. To mitigate the risk, the institution should strictly adhere to KYC procedures, limit transactions with non-account holders, require supporting documents for some transactions (say for over USD 10,000) and should be able to identify the high risk accounts e.g. Politically Exposed Persons Accounts, Non-Resident Accounts and Forex Bureaus.

7. **Contagion risk / rumours -** Institutions operating as part of a group (comprising banking or non-banking entities) will be susceptible to reputation events affecting their parent bank, non-bank holding company, or other members of the group (e.g. sister companies, subsidiaries and affiliates). For example, the reputation may be damaged by regulatory sanctions against its parent bank for, say, breach of anti-money laundering regulations or by publicised concerns about the parent bank's safety and soundness (e.g. due to substantial trading losses). Such contagion effects may also result from other problematic relationships, such as any close association (whether knowingly or unknowingly) with major customers, counterparties or service providers that are revealed to be engaged in unethical, unlawful or corrupt activities.

8. **Transparency/accountability -** The ability to be responsive to and satisfy stakeholders' information needs (e.g. by disclosing information in respect of material issues of interest to stakeholders in a transparent, honest and prompt manner) has itself become a key determinant of business competence. Such information will help stakeholders in understanding values, strategies, and performance and future prospects.

8.4.2 Risk Monitoring and Management Information System

Examining reputational risk for its likelihood and impact is only one side of the coin. The other side requires an assessment of the organization's ability to avoid the risk or respond to it if it occurs.

Having mapped important risks, the organization should establish procedures to monitor early warning signs of them occurring or increasing. One of the important listening posts in an institution is the customer services department. This department will often be able to establish early warning signals of a trend occurring before the issue spills over to the public domain. The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. The results of these monitoring activities should be included in management and board reports.

A system should exist to ensure that deficiencies identified are promptly managed and meaningful corrective action implemented. Training programs should be effective, and the necessary resources provided to ensure compliance.

Using the internet proactively enables a company to provide regular updates to all its important stakeholders. This need not only apply to external audiences but can apply internally through the corporate intranet. "Crisis centres" might make information available in real time, assisting those attempting to manage the situation. It can ensure that a single, current position statement is used by representatives in every market in

which the company operates, reducing inaccuracy and inconsistency. It can also provide low-cost training and a central facility to capture the lessons learned from past crises.

Some factors to consider in monitoring Reputational Risk include:-

- **Staff awareness** - The business managers should recognise and assess the reputational implications of each business activity in the regular risk assessment.
- **Evaluating initiatives before launch** - The departments introducing major new services or policies should undertake a viability assessment to be monitored by internal audit.
- **Using data on complaints or dissatisfaction** - Maintaining and regularly analysing a log of complaints and other events with reputational implications can provide the early warning signs of serious problems, and the data can help guide efforts to mitigate the risks and improve performance. In addition, banks can conduct discreet public opinion surveys on a regular basis to track the public's awareness of their products and services, as well as the public's satisfaction with and support for their policies and services.
- **Implementing codes of conduct -** A code of conduct reflects the core values of an organisation and the expectations of stakeholders and the community at large. But simply having the code does not suffice – regular staff training and occasional updating of the code are also needed.

8.5 Internal Controls and Audit

The banking institution's audit and risk management committees should be responsible for reviewing adequacy and effectiveness of internal control systems relating to reputation risk and means through which exposures related to reputation risk are managed.

Appropriate members of senior management (responsible for the institution's public relations) should comply to the laid down principles and procedures in managing the communication of information to the market so that it minimizes the impact of adverse reputation risk events. It should also be responsible for monitoring a banking institution's reputation within the market place.

9.0 COMPLIANCE RISK MANAGEMENT

9.1 Introduction

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

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

9.1.1 Impact of Compliance Risk

Non-compliance with the legal and regulatory framework exposes an institution to payment of fines, penalties, damages, and the violation of contracts. It can also lead to diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential and an inability to enforce contracts. Furthermore, public knowledge of legal and regulatory violations can cause substantial harm to a bank's reputation contributing to a loss of public confidence.

9.1.2 Organisation of Compliance Function

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

Institutions should organise their compliance function and set priorities for the management of its compliance risk in a way that is consistent with its own risk management strategy and structures. Some institutions may wish to organise their compliance function within their operational risk management function, as there is a close relationship between compliance risk and certain aspects of operational risk. Others may prefer to have separate compliance and operational risk functions, but establish mechanisms requiring close cooperation between the two functions on compliance matters.

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

9.2 Board and Senior Management Oversight

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

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

- defining the compliance risk management system and ensuring that the system is aligned with overall business activities;
- approving compliance risk management policy that provides the senior management with clear guidelines and procedures for managing compliance risk;
- establishing a management structure capable of implementing the institution's compliance risk management process; and
- periodically reviewing the institution's compliance risk management policy to ensure proper guidance is provided for effectively managing the institution’s compliance risk.

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

9.3 Policies and Procedures

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

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

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

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

9.4 Measuring, Monitoring and Control of Compliance Risk

The compliance function should monitor the institution's compliance status periodically and report to the board or a committee of the board. The compliance function should also report to the Central Bank the compliance status as required from time to time through the compliance return (**Appendix I**).

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

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

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

9.4.1 Management Information System

Technology can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems (e.g. an increasing number of customer complaints, irregular trading or payments activity, etc). The institution's management information systems should therefore be sound to be able to

capture aspects of non-compliance. This is possible when the institutions have a strong control culture. Compliance considerations should be incorporated into product and system development and modification processes, including changes made by outside service providers or vendors.

9.5 Internal Audit

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

10. COUNTRY AND TRANSFER RISK MANAGEMENT

10.1 Introduction

10.1.1 Definitions

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

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

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

Other types of country and transfer risk

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

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

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

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

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

10.1.2 Background

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

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

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

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

10.1.3 Board and Senior Management Oversight

The board and senior management are responsible for defining the level of country and transfer risk the institution can undertake and to ensure that the institution has an effective risk management framework consistent with the level of the institution's cross-border exposure. Towards this end, the board should ensure that there are well-defined policies, procedures and processes to identify measure, evaluate, monitor, report and control or mitigate country and transfer risk.

10.2 Policies and Procedures

Institutions (having significant cross-border exposure) should have adequate policies and procedures for identifying, monitoring and controlling country risk and transfer risk in their international lending and investment activities and for maintaining appropriate reserves against such risks. The details to be included in the policy, and any procedures

drawn up in respect of them, depend on the nature and scope of an institution's cross-border activities.

Generally, an institution should set out the business strategy in overseas countries, the parameters under which such business is carried out, its risk appetite and risk tolerances in the light of available financial resources, staff skills and systems for country risk identification, measurement, monitoring, reporting and provisioning. Such policies/ procedures should encompass the following aspects:

(1) Clear lines of authority (including approval of cross-border lending and exceptions), responsibility and accountability for country risk management;
(2) Types of country risk which may be incurred by the institution and the policies and procedures for managing them (in particular whether the institution's country risk management process is centralized or decentralized and integrated with the overall credit risk management);
(3) The overall limits and sub-limits for cross-border exposures;
(4) The standards and criteria which the institution will use to analyze the risk of particular countries;
(5) The internal country rating system, if any, or how the country risk elements are factored into the institution's existing loan classification system;
(6) The method to be used in measuring country risk exposures;
(7) The country risk provisioning policy and methodology;
(8) Types of and criteria for acceptable collateral and guarantees, financial instruments and hedging strategies (e.g. credit derivatives or netting arrangements) which are allowed to be used for the mitigation of country risk and the requirements for perfection of collateral;
(9) The minimum standard terms and conditions to be incorporated in loan documentation in accordance with the legal requirements of each country;
(10) The requirement for registration, if applicable, of credit granted and guarantees accepted, noncompliance with which may render the exposure or guarantee not legally enforceable by the institution;
(11) Lists of designated lawyers for evaluating the legitimacy of documentation and perfection of collateral;
(12) Procedures for dealing with deteriorating situations in a country, with clear contingency plans and exit strategies; and
(13) Types of management reports on country and transfer risk.

The policy should be reviewed at least annually to determine if it is still appropriate for the institution's business and compatible with changing market conditions. Senior management is responsible for monitoring implementation of the policy and developing detailed procedures where necessary to supplement the policy.

10.3 Measurement and Monitoring of Country Risk

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

10.3.1 Measurement System

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

a) Makes Allowance for Risk Allocation

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

b) Ensures Consolidation

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

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

Country exposure consists of all assets including loans, acceptances, placements, securities, etc., which represent claims on residents of another country. A breakdown of residual maturity of claims will assist in providing a comprehensive maturity profile of indebtedness. Additional breakdowns, for example, distinguishing between claims on sovereign borrowers, banks and others, will also assist the institution's management to assess the its country exposure.

Deposits from a country should not ordinarily be offset against credits to that country unless the institution has established a legal right of set-off vis-à-vis the same customer. Some potential claims that may involve risk include letters of credit and

legally binding commitments to lend to foreign clients. Fiduciary operations should also be considered where the institution acts as an agent, which may give rise to country exposure.

Institutions with considerable foreign exposure and considerable country risk have to periodically review the influence of potential credit deterioration, or payment problems of specific countries or groups of countries, on their statement of financial position and statement of comprehensive income. The findings must be brought to the attention of the senior management officers responsible.

10.3.2 Risk tolerance limits

Banks with foreign exposure must have an adequate limit system in place for country risk. The limits must be regularly reviewed and authorized by the senior management function designated for that purpose. For effective oversight, institutions are required to:

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

10.3.3 Internal Control System

The institutions are obliged to have adequate information systems to monitor compliance with country risk limits. It must be possible to detect a limit violation in good time and this should result in a report to the senior management and the board. The employees who are entrusted with controlling country risk limits must have the required knowledge and must be sufficiently independent from the staff whose work they are assigned to monitor.

10.3.4 Lending principles

The following principles should be taken into consideration:-

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

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

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

iv. Institutions should not lend on the basis of inadequate information. While it may be difficult for borrowers in some countries to provide comprehensive financial data and audited accounts compiled in accordance with international accounting standards, institutions should not let that difficulty become an excuse not to ask for the information they need to assess a credit proposal.

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

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

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

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

10.3.5 Country Risk Ratings

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

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

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

10.3.6 Country Risk Limits

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

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

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

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

Limits should be periodically reviewed to incorporate changing scenarios. Finally, once the limits are set, they should not be breached without going through a procedure for approval from a designated approving authority as identified by the board or policy-making group, which actually approved the policy and the said limits. The institutions should establish a mechanism of monitoring compliance with these limits. Any breach of limits should be reported to the senior management who should take appropriate corrective action.

10.3.7 Management Information System

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

10.4 Internal Control and Audit

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

10.5 Reporting and Disclosure

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

APPENDIX I

CBK/RMG/ 7-1				
	MONTHLY COMPLIANCE RETURN			
	Institution:			
	Financial Year:		Version 1.1.7.2	
	Start Date:			
	End Date:			
	Legal and Regulatory Requirements	**Actual Position**	**Compliance Yes/No**	**Comments**
1	Core Capital (Minimum for Banks and Mortgage Finance companies - Shs. 700m (2012); Shs. 1,000m (from 31.12.2012). NBFIs - Shs. 200m. **B.A. Section 7(1).**			
2	Total Capital/Total Risk Weighted Assets Ratio (Min. 12%). **B.A. Section 18**			
3	Core Capital to Total Risk Weighted Assets Ratio is 8%. **B.A. Section 18**			
4	Core Capital to Total Deposits ratio is 8%. **B.A. Section 17**			
5	Liquidity Ratio - Minimum is 20 %. **B.A. Section 19(1)**			
6	Single Borrower limit - 25 % of Core Capital. **B.A. Section 10(1)**			
7	The Institution must not Grant any Advance or Credit Facility Against the Security of Its Own Shares. **B.A. Section 11(1)(a)**			
8	The Institution must not Grant any Facility to a Company in which it has Equity Interest Directly or Indirectly of 25% or more of the Share Capital of that Company. **B.A. Section 11(1)(b)**			
9	All Insider Borrowing must be Secured. **B.A. Section 11(1)(c) & (d)**			
10	All Loans to Directors and Management should be at Arm's Length and Approved by the Full Board and should be reported to CBK within Seven Days. **B.A. Section 11(1)(e)**			
11	Single Insider Borrower Limit - 20% of Core capital. **B.A. Section 11(1)(f)**			

12	Total Insider Borrowing Limit - 100% of Core Capital. **B.A. Section 11(1)(g)**			
13	The institution must not Grant any Credit Facility, Give Guarantee, or Incur any Liability in a Fraudulent or Reckless Manner. **B.A. Section 11(1)(h)**			
CBK/RMG/ 7-1				
MONTHLY COMPLIANCE RETURN				
14	Investment in Land & Buildings **purchased after 10.06.1999** limited to not more than 20% of Core Capital. **B.A. Section 12(c) and (CBK/PG/07 - Prohibited Business)**			
15	Restriction on Ownership of Share Capital to 25%. **B.A. Section 13(1)**			
16	Transfer of 5% Shareholding of an Institution must be Approved by CBK. **B.A. Section 13(4)**			
17	Advances for Real Estate is Limited to 25 % of Total Deposits, except for MFCs. **B.A. Section 14(1)**			
18	Loans and Advances to be Classified in Accordance with Risk Classification of Assets and Provisioning. **(CBK/PG/04)**			
19	All Capitalised Expenditure Including Preliminary Expenses must be Written off before Paying Dividends. **B.A. Section 20(1)**			
20	The Institution must make Adequate Provisions for bad and Doubtful Debts. **B.A. Section 20(2)(b) and (CBK/PG/04)**			
21	Institutions must Display in a Conspicuous Position in Every Office and Branch a Copy of the Latest Audited Balance Sheet and Profit & Loss Account. **B.A. Section 22**			
22	Institutions must Furnish Information at such Time and Manner as Required by the Central Bank. **B.A. Section 28**			
23	Officers of an Institution must take Reasonable Steps to Secure Accuracy of Information Submitted to CBK. **B.A. Section 50(1)(b)**			

24	Every Institution must Submit to CBK within Three Months of the End of its Financial Year the following; **B.A. Section 23(1) (Reported once after 1st Quarter)**			
	(a) An Audited Balance Sheet			
	(b) An Audited Profit & Loss			
	(c) A copy of the Auditor's Report in the Prescribed Form relating to its activities			
25	An Institution Incorporated Outside Kenya or a Kenyan Incorporated Institution with Branches Outside Kenya must Submit to CBK;			
	(a) An Audited Balance Sheet for the Global Operations			
	(b) An audited Profit and Loss Account for the Global Operations (Report once after audit)			
26	Foreign Exchange exposure limit- 10 % of Core Capital. (**CBK/PG/06 - Foreign Exchange Exposure Limits)**			
27	Aggregate large exposures restricted to not more than 5 times of Core Capital. **(CBK/PG/07 - Prohibited Business)**			
28	All Suspicious transactions should be reported (**CBK/PG/08** - **Proceeds of Crime and Money Laundering Prevention)**			
29	No Institution shall Increase its Rate of Banking or Other Charges Except with Prior Approval of the CBK (**B.A. Section 44)**			
30	An Institution Shall be Limited in what It May Recover from a Debtor with Respect to a Non-performing Loan to the Maximum Amount Under Section 44A (2). **B.A. Section 44A(1)**			
32	No Institution shall Impose Any Form of Charges on a Savings, Seven day Call or Fixed Deposits Account. **B.A. Section 16A(1)**			
33	The Institution Must Appoint an external Auditor Qualified Under Section 161 of the Companies Action and Seek CBK Approval (Reported once a year). (**CBK/PG/09 - Appointment, Duties & Responsibilities of External Auditors)**			

34	If the Institution has Changed or Removed Its Auditors, was Written Approval Obtained from CBK? **B.A. Section 25(1) and (CBK/PG/09 - Appointment, Duties & Responsibilities of External Auditors)**			
35	The Institution must make its Annual Contribution to the Deposit Protection Fund Board (to be reported once a year). **B.A. Section 38**			
36	All Officers of an Institution must be Qualified to Hold Office and shall Cease to hold Office and shall not thereafter be Eligible to hold Office in any Institution if any of them is as stated below; **B.A. Section 48**			
	(a) Bankrupt			
	(b) Convicted of an Offence Involving Dishonesty or Fraud			
	(c) Disqualified from Holding Office Under B.A. Section 32A			
	(d) Removed from Office Under the Provisions Of B.A. Section 34			
37	Does the Institution Comply with the following **(CBK/PG/02 - Corporate Governance) requirements:-**			
	(a) Chief Finance Officer(Head of Finance) and Head of Internal Audit should be Members of ICPAK.			
	(b) Company Secretary should be a Member of ICPSK.			
	(c) Every Board Member must Attend at Least 75% OF THE Board Meetings Annually.			
	(d) No Chief Executive Officer, Executive Director or Member of Management should Own more than 5% of the Institution's Shareholding.			
38	Has the institution established a Compliance Function which includes an AML section (Corporate Governance, Proceeds of Crime and Money Laundering (Prevention) Prudential Guidelines and Compliance Risk Management)			

39	Compliance with Consumer Protection provisions as stipulated in the Consumer Protection Guideline			

NB

1. This Compliance return should be submitted monthly to the Central Bank of Kenya, Bank Supervision Department
2. Misreporting and late submission will be subject to penalties
3. Officers compiling, checking and authorizing this return shall be held accountable for the accuracy/inaccuracy of this return.

AUTHORIZATION:

We have taken necessary measures to ensure that this return is accurate

AUTHORIZATION:

We declare that this return, to the best of our knowledge and belief is correct.

Name of Compiling Officer: **Sign: .....**

…… **Date:**

Name of authorizing officer (1): **Sign: .....** **.....**

…… **Date:**

Name of authorizing officer (2): **Sign: .....** **.....**

……

APPENDIX 11

CBK/PR30		COUNTRY AND TRANSFER RISK	
	Institution :		
	Financial Year:		
	Start Date:		
	End Date:	-	
		ASSETS	
	1.0	**NOSTRO ACCOUNT BALANCES**	
	1.1	*Demand Deposits*	
	1.1.1	Central Banks	
	1.1.2	Commercial Banks	
	1.2	*Term Deposits*	
	1.2.1	Central Banks	
	1.2.2	Commercial Banks	
	2.0	**FOREIGN SECURITIES PURCHASED**	
	2.1	Central Governments	
	2.1.1	i) Treasury Bills	
	2.1.2	ii) Treasury Bonds	
	2.1.3	iii) Stocks	
	2.2	Local Governments	
	2.3	Non-Financial Public Entities	
	2.4	Commercial banks	
	2.5	Non-bank Financial Institutions.	
	2.6	Private Entities	
	2.7	Others n.e.s	
	3.0	**LOANS ADVANCED**	
	3.1	Central Governments	
	3.2	Central Govt - Autonomous Agencies	
	3.3	Local Governments	
	3.4	Non-Financial Public Entities	
	3.5	Commercial Banks	
	3.6	Non-bank Financial Institutions	
	3.7	Private Entities	
	3.8	Individuals	
	3.9	Others n.e.s	
	4.0	**FINANCIAL DERIVATIVES**	
	4.1	Central Governments	

	4.2	Central Govt - Autonomous Agencies	
	4.3	Local Governments	
	4.4	Non-Financial Public Entities	
	4.5	Commercial Banks	
	4.6	Non-bank Financial Institutions	
	4.7	Other Private Entities	
	4.8	Individuals	
	4.9	Others n.e.s	
	5.0	**INVESTMENT IN SHARES AND EQUITIES**	
	5.1	Commercial Banks	
	5.2	Non-Bank Financial Institutions	
	5.3	Private Entities	
	5.4	Other Ivestments n.e.s	
		TOTAL ASSETS	
	AUTHORIZATION:		
	We declare that this return, to the best of our knowledge and belief is correct.		
	Name of Compiling Officer: **.....**		
	Name of authorizing officer (1): **.....**		
	Name of authorizing officer (2): **.....**		

Note: The Table to provide the regional/geographical breakdown will be provided separately with the returns compilation software.