RESERVE BANK OF MALAWI



RISK MANAGEMENT GUIDELINES FOR BANKING INSTITUTIONS

SUPERVISION OF FINANCIAL INSTITUTIONS
2007

RISK MANAGEMENT GUIDELINES

FOR

BANKING INSTITUTIONS

2007

TABLE OF CONTENTS

1 INTRODUCTION 5
1.1 Risk Management Process 5
1.2 Active Board and Senior Management Oversight 6
1.3 Adequate Policies, Procedures, and Limits 7
1.4 Adequate Risk Monitoring and Management Information Systems 8
1.5 Adequate Internal Controls 9
1.6 The Risk Management Function 10
2 STRATEGIC RISK MANAGEMENT GUIDELINES 12
2.1 Introduction 12
2.2 Board and Senior Management Oversight 13
2.2.1 Board Oversight 13
2.2.2 Senior Management Oversight 14
2.3 Policies, Procedures & Limits 14
2.4 Risk Monitoring and Management Information System 15
2.5 Internal Controls and Audit 16
3 CREDIT RISK MANAGEMENT GUIDELINES 17
3.1 Introduction 17
3.2 Board and Senior Management's Oversight 18
3.2.1 Board Oversight 18
3.2.2 Delegation of Authority 19
3.2.3 Senior Management Oversight 19
3.3 Credit Strategy, Policies, Procedures and Limits 20
3.3.1 Credit Strategy 20
3.3.2 Policies 21
3.3.3 Limits 22
2.3.4 Credit Origination 22
3.3.4 Approving New Credits and Extension of Existing Credits 24
3.3.5 Credit Administration 25
3.4 Internal Risk Rating Systems 26
3.5 Managing Problem Credits 27
3.6 Management Information System 28
3.7 Internal Controls 29
3.7.1 Risk review 29
4 LIQUIDITY RISK MANAGEMENT GUIDELINES 29
4.1 Introduction 30
4.2 Board and Senior Management Oversight 31
4.2.1 Board Oversight 31
4.2.2 Senior Management Oversight 31
4.2.3 Liquidity Risk Strategy 32
4.3 Policies, Procedures and Limits 33
4.3.1 Liquidity Policies 33
4.3.2 Procedures and Limits 34
4.4 Risk Measurement, Monitoring and Management Information System 34
4.4.1 Measurement and Monitoring of Liquidity Risk 35
4.4.2 Foreign Currency Liquidity Management 39

4.4.3 Managing Market Access 39
4.4.4 Review of Assumptions Utilized in Managing Liquidity 39
4.4.5 Stress Testing 39
4.5 Management Information System 40
4.6 Internal Controls 41
5 INTEREST RATE RISK MANAGEMENT GUIDELINES 43
5.1 Introduction 43
5.1.1 Sources of Interest Rate Risk 43
5.2 Board and Senior Management Oversight 44
5.2.1 Board Oversight 44
5.2.2 Senior Management Oversight 45
5.3 Policies, Procedures and Limits 45
5.3.1 Policies and procedures 45
5.3.2 Limits 46
5.4 Risk Measurement, Monitoring and Management Information System 47
5.4.1 Interest Rate Risk Measurement and Monitoring 48
5.4.2 Stress testing 50
5.4.3 Management Information Systems 51
5.5 Internal Controls 51
5.6 Lines of responsibility and authority 52
6 FOREIGN EXCHANGE RATE RISK MANAGEMENT GUIDELINES 53
6.1 Introduction 53
6.2 Board and Senior Management Oversight 53
6.3 Policies and Procedures 54
6.4 Risk Identification, Measurement, Monitoring and Control 55
6.4.1 Risk identification 55
6.4.2 Risk Measurement 55
6.4.3 Risk Limits 55
6.4.4 Stress Tests 56
6.4.5 Risk Monitoring and Control 56
6.4.6 Risk Reporting 56
6.5 Internal Controls and Independent Audits 56
7 PRICE RISK MANAGEMENT GUIDELINES 57
7.1 Introduction 57
7.2 Board and Senior Management Oversight 57
7.3 Policies, Procedures and Limits 58
7.4 Measuring and Monitoring Price Risk 58
7.5 Management Information System 59
7.6 Internal Control and Audit 59
8 OPERATIONAL RISK MANAGEMENT GUIDELINES 60
8.1 Introduction 60
8.2 Board and Senior Management Oversight 62
8.2.1 Board Oversight 62
8.2.2 Senior Management Oversight 63
8.3 Policies, Procedures and Limits 64

8.4 Risk Identification, Assessment, Monitoring, Control and Management Information System 65
8.4.1 Risk Identification and Assessment 65
8.4.2 Risk Monitoring and MIS 66
8.4.3 Risk Control/Mitigation 67
8.5 Internal Control 69
9 COMPLIANCE RISK MANAGEMENT GUIDELINES 70
9.1 Introduction 70
9.1.1 Compliance Risk Management 71
9.2 Board and Senior Management Oversight 71
9.2.1 Board Oversight 71
9.2.2 Senior Management Oversight 71
9.3 Policies and Procedures 72
9.3.1 Compliance Risk Analysis 73
9.3.2 Self Assessment 73
9.3.3 Risk Maps and Process Flows 73
9.3.4 Key Indicators 73
9.3.5 Escalation Triggers 74
9.3.6 Breach Logs and Near Miss Logs 74
9.3.7 Internal Audit Reports 74
9.3.8 Front-line Prevention Controls 74
9.4 Compliance Monitoring and Reporting 75
9.4.1 Tools to Manage the Compliance Process 75
9.5 Legal Risk 76
9.5.1 Policies and Procedures 77
10 REPUTATION RISK MANAGEMENT GUIDELINES 78
10.1 Introduction 78
10.2 Policies and Procedures 79
10.3 Reputation Risk Management and Monitoring 80
10.4 Risk Methodology Components 80
10.5 Reputation Risk Analysis Methodology and Process 80
10.6 Roles and responsibilities 81

1 INTRODUCTION

Risk-taking is an inherent element of banking and, indeed, profits are in part the reward for successful risk taking in business. On the other hand, excessive and poorly managed risk can lead to losses and thus endanger the safety of a bank's depositors. Accordingly, the Reserve Bank of Malawi places significant emphasis on the adequacy of an institution's management of risk. The Reserve Bank of Malawi puts forward this document for the purpose of providing guidelines to all banking institutions on risk management systems that are expected to be in place. The document sets out minimum standards that shall be expected of a risk management framework at any banking institution. For the purpose of these guidelines, risk in a banking organization refers to the possibility that the outcome of an action or event could bring adverse impacts on the institution's capital, earnings or its viability. Such outcomes could either result in direct loss of earnings and erosion of capital or may result in imposition of constraints on a bank's ability to meet its business objectives. These constraints could hinder a bank's capability to conduct its business or to take advantage of opportunities that would enhance its business. As such, managers of banking institutions are expected to ensure that the risks an institution is taking are warranted.

Risks are considered warranted when they are understandable, measurable, controllable and within a banking institution's capacity to readily withstand adverse results. Sound risk management systems enable managers of banking institutions to take risks knowingly, reduce risks where appropriate and strive to prepare for a future, which by its nature cannot be predicted with absolute certainty. Risk Management is a discipline at the core of every banking institution and encompasses all activities that affect its risk profile. Managers of banking institutions should attach considerable importance to improve the ability to identify, measure, monitor and control the overall risks assumed.

The guidelines are in line with internationally accepted risk management principles and best practices. They are also aligned with the revised version of Core Principles for Effective Banking Supervision which the Basel Committee published in October 2006. Core Principle 7 on '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.* Other relevant Core Principles (CP) touch on credit risk (CP8), market risk (CP13) liquidity risk (CP14), operational risk (CP15) and interest rate risk (CP16). Whilst 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, volume etc, these guidelines cover the most common risks in banking institutions in Malawi, namely: Strategic Risk, Credit Risk, Liquidity Risk, Interest Rate Risk, Foreign Exchange Rate Risk, Price Risk, Operational Risk, Compliance Risk and Reputation Risk.

1.1 Risk Management Process

Because of the vast diversity in risk that banking institutions take, there is no single

prescribed risk management system that works for all. Each banking institution should tailor its risk management program to its needs and circumstances. Regardless of the risk management program design, each program should cover:

Risk identification

In order to properly manage risks, an institution must recognize and understand risks that may arise from both existing and new business initiatives; for example, risks inherent in lending activity include credit, liquidity, interest rate and operational risks. Risk identification should be a continuing process, and should be understood at both the transaction and portfolio levels.

Risk Measurement

Once risks have been identified, they should be measured in order to determine their impact on the banking institution's profitability and capital. This can be done using various techniques ranging from simple to sophisticated models. Accurate and timely measurement of risk is essential to effective risk management systems. An institution that does not have a risk measurement system has limited ability to control or monitor risk levels. Banking institutions should periodically test their risk measurement tools to make sure they are accurate. Good risk measurement systems assess the risks of both individual transactions and portfolios.

Risk Monitoring

Institutions should put in place an effective management information system (MIS) to monitor risk levels and facilitate timely review of risk positions and exceptions. Monitoring reports should be frequent, timely, accurate, and informative and should be distributed to appropriate individuals to ensure action, when needed.

Risk Control

After measuring risk, an institution should establish and communicate risk limits through policies, standards, and procedures that define responsibility and authority. These limits should serve as a means to control exposure to various risks associated with the banking institution's activities. Institutions may also apply various mitigating tools in minimizing exposure to various risks. Institutions should have a process to authorize and document exceptions or changes to risk limits when warranted.

A sound risk management system should have the following elements:

- active board and senior management oversight; (BMO)
- adequate policies, procedures and limits; (PPL)
- adequate risk measurement, monitoring and management information system (MIS); and
- comprehensive internal controls. (ICs)

1.2 Active Board and Senior Management Oversight

Boards of directors 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 institutions, including those related to managing and taking risks, and should also ensure that senior management is fully capable of managing the activities that their institutions undertake. While all boards of directors are responsible for understanding the nature of the risks significant to their institutions and for ensuring that 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.

Directors should have a clear understanding of the types of risks to which their institutions are exposed and should receive reports that identify the size and significance of the risks in terms that are meaningful to them. In fulfilling this responsibility, directors should take steps to develop an appropriate understanding of the risks their institutions face, possibly through briefings from auditors and experts external to the institution. 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 and that ensures compliance with laws and regulations on both a long-term and day-to-day basis. Accordingly, management should 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 an institution to have a thorough understanding of banking and financial market activities and detailed knowledge of the activities their institution conducts, including the nature of internal controls necessary to limit the related risks.

1.3 Adequate Policies[1], Procedures[2], and Limits

An institution's 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 its more fully articulated procedures should provide detailed guidance for the day-to-day implementation of broad business strategies, and generally include limits designed to shield the institution from excessive and imprudent risks. While all institutions should have policies and procedures that address their significant activities and risks,

[1] Policies are written statements of the institution's commitment to pursue certain objectives and results. Policies often set standards (e.g. of risk tolerance) and recommend courses of action. They also express an institution's underlying mission, values and principles.
[2] Procedures are step by step processes, programs and practices that impose order on the institution's pursuit of its objectives, defining how daily activities are to be carried out. They are consistent with the underlying policies.

management is expected to ensure that they are modified when necessary to respond to significant changes in the banking institution's activities or business conditions.

To ensure that, an institution's policies, procedures, and limits are adequate, the same should at minimum address the following:

- policies, procedures, and limits should provide for adequate identification, measurement, monitoring, and control of the risks posed by its significant activities.

- policies, procedures, and limits should be consistent with management's experience level, the institution's stated goals and objectives, and the overall financial strength of the institution.

- policies should clearly delineate accountability and lines of authority across the institution's activities.

- policies should provide for the review of activities new to the banking institution to ensure that the infrastructures necessary to identify, monitor, and control risks associated with an activity are in place before the activity is initiated.

1.4 Adequate Risk Monitoring and Management Information Systems

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, as well as with regular and sufficiently detailed reports for line managers engaged in the day-to-day management of the institution's activities.

Institutions should have risk monitoring and management information systems in place that provide directors and senior management with a clear understanding of the banking institution's positions and risk exposures.

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

- the institution's risk monitoring practices and reports should address all of its material risks.

- key assumptions, data sources, and procedures used in measuring and monitoring risk should be appropriate and adequately documented and tested for reliability on an on-going basis.

- reports and other forms of communication should be 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.

- reports to management or to the institution's directors should be 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.

1.5 Adequate Internal Controls[3]

An institution's internal control structure is critical to the safe and sound functioning of the institution generally and to its risk management system, in particular. Establishing and maintaining an effective system of controls, including the enforcement of official lines of authority and the appropriate separation of duties such as trading, custodial, and back-office is one of management's more important responsibilities.

Indeed, appropriately segregating duties is a fundamental and essential element of a sound risk management and internal control system. Failure to implement and maintain an adequate separation of duties can constitute an unsafe and unsound practice and possibly lead to serious losses or otherwise compromise the financial integrity of the institution. Serious lapses or deficiencies in internal controls, including inadequate segregation of duties, may warrant supervisory action, including formal enforcement action.

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. Ideally, internal controls are tested by an independent internal auditor who reports directly either to the institution's board of directors or its audit committee. Given the importance of appropriate internal controls, the results of audits or reviews, whether conducted by an internal auditor or by other personnel, should be adequately documented, as should management's responses to them.

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.

[3] Any action taken by management, the board and other parties to manage risk and increase the likelihood that objectives and goals will be achieved.

- Reporting lines should provide sufficient independence of the control areas from the business lines and adequate separation 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.

1.6 The Risk Management Function

Banking institutions should institute a setup that supervises overall risk management at the bank. Such a setup could be in form of a risk manager, committee or department depending on the size and complexity of the institution. Ideally, overall risk management function should be independent from those who take or accept risk on behalf of the institution. Where individuals responsible for overall risk management function are involved in day to day operations, then sufficient checks and balances should be established to ensure that risk management is not compromised. Overall risk management function provides an oversight of the management of risks inherent in the institution’s activities. The function is tasked to:

- identify current and emerging risks;
- develop risk assessment and measurement systems;
- establish policies, practices and other control mechanisms to manage risks;
- develop risk tolerance limits for Senior Management and Board approval;
- monitor positions against approved risk tolerance limits; and
- report results of risk monitoring to Senior Management and the Board.

However, it must not be construed that risk management is only restricted to individual(s) responsible for overall risk management function. Business lines are equally responsible for the risks they are taking. Because line personnel, more than anyone else, understand

the risks of their activities, any a lack of accountability on their part can run counter to sound and effective risk management.

2 STRATEGIC RISK MANAGEMENT GUIDELINES

2.1 Introduction

Strategic risk arises from an institution's inability to implement appropriate business plans, strategies, decision making, resource allocation and its inability to adapt to changes in its business environment. This risk is therefore a function of:

- a banking institution's strategic goals
- the business strategies developed to achieve the goals
- the resources deployed in pursuit of these goals, and the quality of implementation; and
- the resources needed to carry out business strategies both tangible and intangible.

They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities. In strategic management, the organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

Common Sources of Strategic Risk

Strategic risk can arise through many ways. However, the common sources of the risk within banking institutions are the following:

a) competition – through emerging industry rivals;
b) technology – shift in technology;
c) customer - customer priority shift and over-reliance on a few customers;
d) economic factors;
e) regulations;
f) work processes and procedures; and
g) adequacy of information for decision-making.

Strategic planning process

Every institution should put in place a strategic plan which should be supported by a realistic budget. A strategic plan clarifies an institution's overall purpose, defines goals and priorities and determines practical approaches for achieving targeted priorities.

If the strategic planning process is not appropriate or if the assumptions are not realistic, the strategic plan will be flawed thereby exposing the banking institution to strategic risk.

In this regard, every institution should have an appropriate strategic planning process encompassing the following:

- support or participation of the board, delegated committees, and senior management;
- participation of staff from various departments;

- adequacy of information in developing assumptions in relation to economic factors, position of the banking institution compared to competitors, current competitive position, future market trends and customer needs, among others;
- consistency of the operational plans with the overall objective of a banking institution, and
- assessment of actual performance against strategic plans.

Risk Mitigation Factors

Banking institutions should adopt and implement robust strategic risk mitigation measures and techniques to enhance the achievement of strategic objectives. These include engaging qualified board and senior management, formulation of strategic and operational plans, high quality of personnel and proper training, comprehensive risk management systems and adequate access to information.

2.2 Board and Senior Management Oversight

Board of Directors and Senior Management oversight is an integral part of an effective strategic risk management program. The Board of Directors retains the overall responsibility for strategic risk management of the institution. It is chiefly responsible for setting corporate strategy and reviewing management performance in implementing the banking institution's strategic plan. In turn, Senior management have a duty to ensure that there is an effective strategic risk management process by transforming the strategic direction given by the Board through policy. To do this, senior management should have an understanding of the nature and level of the various risks associated with the banking institution's strategic plan and how such risks fit within the overall business strategies.

2.2.1 Board Oversight

The responsibilities of the Board of Directors with regard to strategic risk management are to:

a) ensure that risk management practices are an intrinsic part of strategic planning;

b) establish corporate objectives and values, strategic goals, and a mission statement describing the purpose of the banking institution; and ensure that these are effectively communicated and consistently applied throughout the banking institution;

c) ensure that the banking institution's overall strategic risk exposure is maintained at prudent levels, and is compatible with developed business strategies;

d) assess whether the institution's strategic/business plans make sense given the current economic and competitive environment, consist of reasonable and measurable targets, and; review the associated Strategic Risk Management framework periodically to determine that it remains adequate and appropriate under the prevailing business environment;

e) assess management's success in implementing the banking institution's strategic plan and achieving targets and results;

f) ensure that strategic direction and initiatives are well conceived and supported by appropriate management information system, operating systems, and service delivery networks. The Board must also ensure that initiatives are supported by capital for the foreseeable future and pose only nominal possible effects on earnings volatility; and

g) ascertain that strategic initiatives are supported by sound due diligence and strong risk management systems. Also ascertain that decisions can be reversed with little difficulty and manageable costs.

2.2.2 Senior Management Oversight

The responsibilities of senior management with regard to strategic risk management are to:

a) ensure that a comprehensive Strategic Risk Management process that is commensurate with the strategic goals of the banking institution is in place;

b) ensure that business continuity plans have been prepared and tested so that important changes in the business/risk environment are assessed and catered for;

c) ensure that management of succession planning is an active ongoing process, integrated with the institution's strategic plans; and

d) ensure that Strategic Risk Management framework is implemented throughout the institution and that all levels of staff understand their responsibilities with respect to Strategic Risk Management.

2.3 Policies, Procedures & Limits

Effective management of strategic risk requires that the banking institution establishes prudent policies, procedures and limits approved by the Board to ensure its objective evaluation and responsiveness to the banking institution'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.

Policies and procedures should cover all material risks associated with the banking institution's business segments defined in the strategic plan. Accountability should be spelt out clearly and lines of authority for all the banking institution's business segments should be clearly defined.

To be effective, policies and procedures should be reviewed on regular basis, to take into account internal and external changes to the operating environment. The policies should establish clear guidelines on frequency and procedures for review of its business strategies.

Policies should be consistent with the organisation's broader business strategies, capital adequacy, technical expertise and risk tolerance. It should take into account the size, nature and complexities of the banking institution's business plans and consider past experiences and performances.

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

- the institution's inherent strengths;
- its identified weaknesses;
- opportunities external to the institution; and
- external factors that pose threats to the institution.

Where appropriate, strategic risk management policies and procedures should cover the use of risk mitigation techniques

A set of Board approved limits should be put in place to control a banking institution's exposure to various quantifiable risks associated with its strategic plan. Risk limits should be clearly communicated to the business units and understood by the relevant staff.

The Board or its designated committee should ensure that limits are subject to regular review and are assessed in light of changes in market conditions or business strategy. The bank's limits should at least define the following:

- exposure to different sectors of the economy;
- growth of business and staff strength; and
- network expansion programmes.

2.4 Risk Monitoring and Management Information System

In order to ensure an effective strategic risk management process, every institution should deploy a management information system that enables management to identify and measure the risks associated with the banking institution's strategic plan.

The level of sophistication of the system should depend on the nature, scale and complexity of the business segments within the business plan of the banking institution. In general the MIS should 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
- mechanisms that are in place to detect exceptions to limits and guidelines

Reporting should be frequent enough to provide timely and adequate information to judge the changing nature of the banking institution's strategic risk profile and evaluate compliance with stated policy objectives and constraints.

To remain effective, the banking institution should review its MIS regularly, and subject it to regular upgrades and modifications.

2.5 Internal Controls and Audit

A banking institution's internal control structure is critical to the safe and sound functioning of the organization generally and the management of the banking institution's strategic direction in particular. Banking 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's structure establishes clear lines of authority;

- the institution's systems and structures provide for business continuity planning; and

- the process of setting up and reviewing strategic and business plans are comprehensive and carefully adhered to.

Internal and external audits are integral to the implementation of a risk management process to control risk associated with a banking institution's business strategy. To carry out their function effectively, internal auditors should have appropriate independence and status within the banking institution to ensure that senior management reacts to and acts upon their recommendations.

A banking institution's internal audit function should among other things, perform periodic checking on whether the strategic risk management system is properly implemented and the established policies and control procedures in respect of risk management are complied with.

The risk management process and the related internal controls should be examined and tested periodically. The scope and frequency of audit may vary but should be increased if there are significant weaknesses or major changes or new products are introduced.

3 CREDIT RISK MANAGEMENT GUIDELINES

3.1 Introduction

Credit risk is the likelihood that a debtor or financial instrument issuer is unwilling or unable to pay interest or repay the principal according to the terms specified in a credit agreement resulting in economic loss to the banking institution.

In a banking institution's portfolio, losses also stem from reduction in portfolio value due to actual or perceived deterioration in credit quality. Credit risk emanates from a banking institution's dealing with individuals, corporates, other banking institutions or a sovereign. For most banking institutions, loans are the largest and most obvious source of credit risk; however, credit risk could stem from activities both on and off balance sheet.

Credit risk means that payments may be delayed or ultimately not paid at all, which can in turn cause cash flow problems and affect its liquidity. Credit risk is still the major single cause of bank failures.

Common sources of credit problems are:

- Credit concentrations: these are viewed as any exposure where the potential losses are large relative to the banking institution's capital, its total assets or, where adequate measures exist, the bank's overall risk level. This may be in the form of single borrowers or counterparties, a group of connected counterparties, and sectors or industries, such as trade, agriculture, etc or in the form of common or correlated factors. The Asian crisis demonstrated how close linkages among emerging markets under stress situations and correlation between market and credit risks as well as between those risks and liquidity risk, can produce widespread losses.

- Credit process issues: Many credit problems reveal basic weaknesses in the credit granting and monitoring processes. While shortcomings in underwriting and management of credit exposures represent important sources of losses at banking institutions, many credit problems would have been avoided or mitigated by a strong internal credit process.

3.2 Board and Senior Management's Oversight

3.2.1 Board Oversight

The Board of directors has a critical role to play in overseeing the credit-granting and credit risk management functions of a banking institution. It is the overall responsibility of a banking institution's Board to approve credit risk strategy and significant policies relating to credit risk and its management which should be based on the overall business strategy. To keep it current, the overall strategy as well as significant policies have to be reviewed by the Board, preferably annually. The responsibilities of the Board with regard to credit risk management shall, interalia, include to**:**

a) Delineate banking institution's overall risk tolerance in relation to credit risk;

b) Ensure that banking institution's significant credit risk exposure is maintained at prudent levels and consistent with the available capital;

c) Ensure that top management as well as individuals responsible for credit risk management possess sound expertise and knowledge to accomplish the risk management function;

d) Ensure that the banking institution implements sound fundamental policies that facilitate the identification, measurement, monitoring and control of credit risk;

e) Ensure that appropriate plans and procedures for credit risk management are in place;

f) Ensure that internal audit reviews the credit operations to assess whether or not the Institution's policies and procedures are adequate and being adhered to;

g) Review exposures to insiders and their related parties, including policies related thereto;

h) Ratify exposures exceeding the level of the management authority delegated to management and be aware of exposures that, while worthy of consideration, are not within the ambits of existing credit policies of the institution;

i) Review trends in portfolio quality and the adequacy of institution's provision for credit losses; and

j) Outline the content and frequency of management report to the Board on credit risk management.

3.2.2 Delegation of Authority

Institutions are required to establish responsibility for credit sanctions and delegate authority to approve credits or changes in credit terms. It is the responsibility of institution's Board to approve the overall lending authority structure, and explicitly delegate credit sanctioning authority to senior management and the credit committee. Lending authority assigned to officers should be commensurate with the experience, ability and personal character. It would be better if institutions develop risk-based authority structure where lending power is tied to the risk ratings of the borrower. Large institutions may adopt multiple credit approvers for sanctioning such as credit ratings, risk approvals etc to institute a more effective system of check and balance. The credit policy should spell out the escalation process to ensure appropriate reporting and approval of credit extension beyond prescribed limits. The policy should also spell out authorities for unsecured credit (while remaining within Reserve Bank of Malawi limits), approvals of disbursements of excess over limits, and other exceptions to credit policy.

In cases where lending authority is assigned to the loan originating function, there should be compensating processes and measures to ensure adherence to lending standards. There should also be periodic review of lending authority assigned to officers.

3.2.3 Senior Management Oversight

Senior Management is responsible for implementing the institution's credit risk management strategies and policies and ensuring that procedures are put in place to manage and control credit risk and the quality of credit portfolio in accordance with these policies. The responsibilities of Senior Management with regard to credit risk management shall include:

a) developing and establishing credit policies and credit administration procedures as a part of overall credit risk management framework for approval by the Board;

b) implementing credit risk management policies;

c) ensuring the development and implementation of appropriate reporting system with respect to the content, format, and frequency of information concerning the credit portfolio and the credit risk to permit effective analysis and sound and prudent management and control of existing and potential credit risk exposure;

d) monitoring and controlling the nature and composition of the institution's portfolio;

e) monitoring the quality of credit portfolio and ensuring that the portfolio is soundly and conservatively valued, uncollectible exposure is written off and probable losses are adequately provided for;

f) establishing internal controls including putting in place clear lines of accountability and authority to ensure effective credit risk management process; and

g) developing lines of communication to ensure timely dissemination of credit risk management policies, procedures and other credit risk management information to all individuals involved in the process.

3.3 Credit Strategy, Policies, Procedures and Limits

3.3.1 Credit Strategy

The primary purpose of banking institution's credit strategy is to determine the risk appetite. Once it is determined, the banking institution could develop a plan to optimize return while keeping credit risk within predetermined limits. The credit risk strategy thus should spell out:

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

b) Target market within each lending segment and level of diversification/concentration;

c) Pricing strategy.

It is essential that institutions give due consideration to their target market while devising credit risk strategy. The credit procedures should aim to obtain an in depth understanding of the banking institution's clients, their credentials and their businesses in order to fully know their customers.

The strategy should provide continuity in approach and take into account cyclic aspect of country's economy and the resulting shifts in composition and quality of overall credit portfolio. While the strategy would be reviewed periodically and amended, as deemed necessary, it should be viable in long term and through various economic cycles.

3.3.2 Policies

Credit policies establish framework for making investment and lending decisions and reflect an institution's tolerance for credit risk. To be effective, policies should be communicated in a timely fashion, and should be implemented through all levels of the institution by appropriate procedures. Any significant deviation/exception to these policies must be communicated to the Senior Management/Board and corrective measures should be taken. At a minimum, credit policies should include:

a) General areas of credit in which the institution is prepared to engage or is restricted from engaging such as type of credit facilities, type of collateral security, types of borrowers, or geographic sectors on which the institution may focus;

b) Detailed and formalized credit evaluation/ appraisal process, administration and documentation;

c) Credit approval authority at various hierarchy levels including authority for approving exceptions;

d) Clear guidelines for each of the various types of credits, such as loans, overdrafts, mortgages, leases, etc[4].

e) Concentration limits on single counterparties and groups of connected counterparties, particular industries or economic sectors, geographic regions and specific products. Banking institutions should ensure that their own internal exposure limits comply with any prudential limits or restrictions set by the Reserve Bank of Malawi;

f) Authority for approval of allowance for probable losses and write-offs;

g) Credit pricing;

h) Roles and responsibilities of units/staff involved in origination and management of credit;

i) Guidelines on management of problem loans; and

[4] Refer to RBM Directive on Asset Classification on guidelines for granting overdraft facilities and monitoring their performance.

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

In order to be effective, credit policies must be communicated throughout the institution, implemented through appropriate procedures, and periodically revised to take into account changing internal and external circumstances.

3.3.3 Limits

An important element of credit risk management is to establish exposure limits covering on-balance sheet and off-balance sheet credit exposures for single counterparties and group of connected counterparties. The objective being to prevent institutions from relying excessively on a large borrower or group of borrowers. Institutions are expected to develop their own limit structure while remaining within the exposure limits set by the Reserve Bank of Malawi. The size of the limits should be based on the credit strength of the counterparty, genuine requirement of credit, economic conditions and the institution's risk appetite. Limits should also be set for respective products, activities, specific industry, economic sectors and/or geographic regions to avoid concentration risk.

Credit limits should be reviewed regularly at least annually or more frequently if counterparty's credit quality deteriorates. All requests of increase in credit limits should be substantiated.

2.3.4 Credit Origination

Establishing sound, well-defined credit-granting criteria is essential to approving credit in a safe and sound manner. The criteria should set out who is eligible for credit and for how much, what types of credit are available, and under what terms and conditions the credits should be granted.

Banking institutions 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;
- a forward-looking analysis of the capacity to repay based on various scenarios and factors both quantitative and qualitative;
- 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.

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

Banks need to understand to whom they are granting credit. Therefore, prior to entering into any new credit relationship, a bank must become familiar with the borrower or counterparty and be confident that they are dealing with an individual or organization of sound repute and creditworthiness. In particular, strict policies must be in place to avoid association with individuals involved in fraudulent activities and other crimes. This can be achieved through a number of ways, including asking for references from known parties, accessing credit reference bureau, and becoming familiar with individuals responsible for managing a company and checking their personal references and financial condition. However, a banking institution should not grant credit simply because the borrower or counterparty is familiar to the banking institution or is perceived to be highly reputable.

Banking institutions should have procedures to identify situations where, in considering credits, it is appropriate to classify a group of borrowers as connected counterparties and, thus, as a single borrower (please refer to RBM Directive on Asset Classification). This would include aggregating exposures to groups of accounts, corporate or non-corporate, under common ownership or control or with strong connecting links (for example, common management, familial ties, etc.).

For overdraft facilities, banking institutions should ensure that these facilities remain lending of a temporary and fluctuating nature which are expected to be cleared by receipt of anticipated funds. Any build up of hardcore (non-fluctuating) component should be converted into term loans and classified accodingly.

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

Banking institutions should assess the risk/return relationship in any credit as well as the overall profitability of the account relationship. Credits should be priced in such a way as to cover all of the imbedded costs and compensate the banking institution for the risks incurred. In evaluating whether, and on what terms, to grant credit, banking institutions need to assess the risks against expected return, factoring in, to the greatest extent possible, price and non-price (e.g. collateral, restrictive covenants, etc.) terms. In evaluating risk, banking institutions should also assess likely downside scenarios and their possible impact on borrowers or counterparties. A common problem among banking institutions is the tendency not

to price a credit or overall relationship properly and therefore not receive adequate compensation for the risks incurred.

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

Banking institutions can utilize collateral and guarantees to help mitigate risks inherent in individual credits but transactions should be entered into primarily on the strength of the borrower's repayment capacity. Collateral cannot be a substitute for a comprehensive assessment of the borrower or counterparty, nor can it compensate for insufficient information. It should be recognized that any credit enforcement actions (e.g. foreclosure proceedings) typically eliminate the profit margin on the transaction. In addition, banking institutions need to be mindful that the value of collateral may well be impaired by the same factors that have led to the diminished recoverability of the credit. Banking institutions should have policies covering the acceptability of various forms of collateral, procedures for the ongoing valuation of such collateral, and a process to ensure that collateral is, and continues to be, enforceable and realisable. With regard to guarantees, banking institutions should evaluate the level of coverage being provided in relation to the credit-quality and legal capacity of the guarantor. Banking institutions should only factor explicit guarantees into the credit decision and not those that might be considered implicit such as anticipated support from the government.

3.3.4 Approving New Credits and Extension of Existing Credits

In order to maintain a sound credit portfolio, a banking institution must have an established formal evaluation and approval process for the granting of credits. Approvals should be made in accordance with written guidelines and granted by the appropriate level of management. There should be a clear audit trail documenting that the approval process was complied with and identifying the individual(s) and/or committee(s) providing input as well as making the credit decision.

Each credit proposal should be subject to careful analysis by a credit analyst with expertise commensurate with the size and complexity of the transaction. An effective evaluation process establishes minimum requirements for the information on which the analysis is to be based. There should be policies in place regarding the information and documentation needed to approve new credits, renew existing credits and/or change the terms and conditions of previously approved credits. The information received will be the basis for any internal evaluation or rating assigned to the credit and its accuracy and adequacy is critical to management making appropriate judgements about the acceptability of the credit.

A banking institution's credit-granting approval process should establish accountability for decisions taken and designate who has the authority to approve credits or changes in credit terms.

A potential area of abuse arises from granting credit to connected and related parties, whether companies or individuals. Related parties typically include a banking institution's parent, major shareholders, subsidiaries, affiliate companies, directors, and executive officers. The relationship includes the ability to exert control over or influence a banking institution's policies and decision-making, especially concerning credit decisions (please refer to RBM Directive on Transactions with Related Persons). A banking institution's ability to systematically identify and track extensions of credit to insiders is crucial. The issue is whether credit decisions are made on a rational basis and according to approved policies and procedures. An additional concern is whether credit is based on market terms or is granted on terms that are more favourable with regard to amount, maturity, rate, and collateral, than those provided to the general public.

Transactions with related parties should be subject to the approval of the board of directors (excluding board members with conflicts of interest).

3.3.5 Credit Administration

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

In developing their credit administration areas, banking institutions should ensure:

- the efficiency and effectiveness of credit administration operations, including monitoring documentation, contractual requirements, legal covenants, collateral, etc.;
- the accuracy and timeliness of information provided to management information systems;
- the adequacy of controls over all "back office" procedures; and
- compliance with prescribed management policies and procedures as well as applicable laws and regulations.

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

The credit files should include all of the information necessary to ascertain the current financial condition of the borrower or counterparty as well as sufficient information to track the decisions made and the history of the credit.

Banking institutions need to develop and implement comprehensive procedures and information systems to monitor the condition of individual credits and single borrowers across the banking institution's various portfolios. These procedures need to define criteria for identifying and reporting potential problem credits and other transactions to ensure that they are subject to more frequent monitoring as well as possible corrective action, classification and/or provisioning.

An effective credit monitoring system will include measures to:

(i) ensure that the banking institution understands the current financial condition of the borrower or counterparty;
(ii) ensure that all credits are in compliance with existing covenants;
(iii) follow the use customers make of approved credit lines;
(iv) ensure that projected cash flows on major credits meet debt servicing requirements;
(v) ensure that, where applicable, collateral provides adequate coverage relative to the obligor's current condition; and
(vi) identify and classify potential problem credits on a timely basis.

Institutions need to enunciate a system that enables them to monitor quality of the credit portfolio on day-to-day basis and take remedial measures as and when any deterioration occurs. Such a system would enable an institution to ascertain whether loans are being serviced as per facility terms, the adequacy of provisions, the overall risk profile is within limits established by management and compliance of regulatory limits. Establishing an efficient and effective credit monitoring system would help senior management to monitor the overall quality of the total credit portfolio and its trends. Consequently, the management could fine tune or reassess its credit strategy /policy accordingly before encountering any major setback. The institutions credit policy should explicitly provide procedural guideline relating to credit risk monitoring. At the minimum it should lay down procedure relating to:

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

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

c) The frequency of monitoring;

d) The periodic examination of collaterals and loan covenants;

e) The frequency of site visits;

f) The identification of any deterioration in any loan.

3.4 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, banking institutions should ensure that the Reserve Bank of Malawi 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 gradations for credits considered satisfactory in order to truly differentiate the relative credit risk they pose. In developing their systems, banking institutions 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, banking institution's internal risk rating system should be responsive to indicators of potential or actual deterioration in credit risk eg. financial position and business condition of the borrower, conduct of the borrower's accounts, adherence to loan covenants, value of collateral, etc. 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.

3.5 Managing Problem Credits

The institution should establish a system that helps identify problem loan ahead of time when there may be more options available for remedial measures. Once the loan is identified as problem, it should be managed under a dedicated remedial process.

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

A problem loan management process encompass the following basic elements.

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

(ii) **Workout remedial strategies.** Sometimes appropriate remedial strategies such as restructuring of loan facility, enhancement in credit limits or reduction in interest rates help improve obligor's repayment capacity. However it depends upon business condition, the nature of problems being faced and most importantly borrower's commitment and willingness to repay the loan. If timely action is not taken to address problem loans, opportunities to strengthen or collect on these poor-quality assets may be missed and losses may accumulate to a point where they threaten a banking institution's solvency. An assessment of work-out procedures should consider the organization of this function, including departments and responsible staff, and assess what the performance of the work-out units has been by reviewing attempted and successful recoveries (in terms of both number and volume) and the average time for recovery. The work out methods utilized and the involvement of senior management should also be evaluated.

(iii) **Review of collateral and security document.** Institutions have to ascertain the loan recoverable amount by updating the values of available collateral with formal valuation. Security documents should also be reviewed to ensure the completeness and enforceability of contracts and collateral/guarantee.

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

3.6 Management Information System

The effectiveness of a banking institution's credit risk measurement process is highly dependent on the quality of management information systems. The information generated from such systems enables the board and all levels of management to fulfill their respective oversight roles, including determining the adequate level of capital that the banking institution should be holding. Therefore, the quality, detail and timeliness of information are critical. In particular, information on the composition and quality of the various portfolios, including on a consolidated basis, should permit management to assess quickly and accurately the level of credit risk that the banking institution has incurred through its various activities and determine whether its performance is meeting the credit risk strategy.

It is also important that banking institutions have a management information system in place to ensure that exposures approaching risk limits are brought to the attention of senior management. All exposures should be included in a risk limit measurement system. The information system should be able to aggregate credit exposures to individual borrowers and counterparties and report on exceptions to credit risk limits on a meaningful and timely basis.

Banking institutions should have information systems in place that enable management to identify any concentrations of risk within the credit portfolio. The adequacy of scope of information should be reviewed on a periodic basis by business line managers, senior management and the board of directors to ensure that it is sufficient to the complexity of the business.

3.7 Internal Controls

3.7.1 Risk review

The institutions must establish a mechanism of independent, ongoing assessment of credit risk management process. All facilities should be subjected to individual risk review at least quarterly. The results of such review should be properly documented and reported directly to Board, or its sub committee. The purpose of such reviews is to assess the credit administration process, the accuracy of credit rating including adequacy of provisions for losses, and overall quality of credit portfolio.

Institutions should conduct credit review with updated information on the counterparty's financial and business conditions, as well as conduct of account. Exceptions noted in the credit monitoring process should also be evaluated for impact on the counterparty's creditworthiness. Credit review should also be conducted on a consolidated group basis to factor in the business connections among entities in a borrowing group.

As stated earlier, credit review should be performed on quarterly basis; however, more frequent review should be conducted for new accounts where institutions may not be familiar with the counterparty, and for classified or adverse rated accounts that have higher probability of default.

4 LIQUIDITY RISK MANAGEMENT GUIDELINES

4.1 Introduction

Liquidity risk is the potential for loss to an institution arising from either its inability to meet obligations as they fall due or to fund increases in assets without incurring unacceptable cost or losses (funding liquidity risk). Sometimes, inadequate market depth where an institution cannot easily unwind or offset specific exposures without significantly lowering market prices causes what is termed as 'market liquidity risk'.

Liquidity is the ability of an institution to transform its assets into cash or its equivalent in a timely manner at a reasonable price to meet its commitments as they fall due.

Liquidity risk is considered a major risk for institutions. It arises when the cushion provided by the liquid assets are not sufficient enough to meet its obligation. In such a situation, institutions often meet their liquidity requirements from the market. However, conditions of funding through market depend upon liquidity in the market and borrowing institution's liquidity. Accordingly, an institution short of liquidity may have to undertake transactions at heavy cost resulting in loss of earnings or in worst case scenario, the liquidity risk could result in bankruptcy of the institution if it is unable to undertake transactions even at current market prices.

Institutions with large off-balance sheet exposures or institutions which rely heavily on large corporate deposits have relatively high level of liquidity risk. Further, institutions experiencing a rapid growth in assets should have major concern for liquidity.

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

An embryonic liquidity problem may initially reveal in the banking institution's financial monitoring system as a downward trend with potential long-term consequences for earnings, capital or going concern. Given below are some early warning indicators that may not necessarily always lead to liquidity problems for an institution; but can ignite such a problem. Consequently, management should carefully watch such indicators and take further analysis wherever it deems appropriate. Examples of such internal indicators are:

a) a negative trend or significantly increased risk in any area or product line;
b) concentrations in either assets or liabilities;
c) deterioration in quality of credit portfolio;
d) decline in earnings performance or projections;
e) rapid asset growth funded by volatile large deposit;
f) large size of off-balance sheet exposure;
g) deteriorating third party evaluation about the banking institution;

h) negative publicity*; and*
i) unwarranted competitive pricing that potentially stresses the banking institution.

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

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

In managing liquidity risk, banking institutions should make close reference to the RBM Policy Statement on Prudential Aspects of Bank Liquidity.

4.2 Board and Senior Management Oversight

4.2.1 Board Oversight

The prerequisite of an effective liquidity risk management includes a well informed Board, capable management and staff having relevant expertise, and efficient systems and procedures. Primarily, it is the duty of the Board of directors to understand the liquidity risk profile of the banking institution and the tools used to manage liquidity risk. The Board has to ensure that the banking institution has necessary liquidity risk management framework and is capable of confronting uneven liquidity scenarios. The Board should approve the strategy and significant policies related to overall management of liquidity. Generally, in this respect the responsibilities of the Board include:

a) Providing guidance on the level of tolerance for liquidity risk;
b) Establishing an appropriate structure for the management of liquidity risk and identifying lines of authority and responsibility for managing liquidity risk exposure;
c) Appointing senior managers who have the ability to manage liquidity risk and delegate to them the required authority to accomplish the job;
d) Continuously monitoring the banking institution's performance and overall liquidity risk profile through reviewing various reports;
e) Ensuring that senior management takes necessary steps to identify, measure, monitor and control liquidity risk; and
f) Reviewing adequacy of the contingency plans of the banking institutions.

4.2.2 Senior Management Oversight

Senior management is responsible for the implementation of sound policies and procedures keeping in view the strategic direction and risk appetite specified by

Board. To effectively oversee the daily and long-term management of liquidity risk, senior managers should:

a) develop and implement procedures and practices that translate the Board's goals, objectives, and risk tolerances into operating standards that are well understood by bank personnel and consistent with the banking institution's intent and strategies;

b) adhere to the lines of authority and responsibility that the Board has established for managing liquidity risk;

c) oversee the implementation and maintenance of management information and other systems that identify, measure, monitor, and control the banking institution's liquidity risk; and

d) establish effective internal controls over the liquidity risk management process and ensure that the same is communicated to all staff.

The responsibility for managing the overall liquidity of the banking institution should be delegated to a specific, identified group within the banking institution. This might be in the form of an Asset Liability Committee (ALCO) comprised of senior management or the treasury function.

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

To underline the importance of synergy, information and attaining benefits of division of responsibility, it is critical that there be close links between those individuals responsible for liquidity and those monitoring market conditions, as well as other individuals with access to critical information. This is particularly important in developing and analysing stress scenarios.

At a minimum, the effective management of assets and liabilities should incorporate the following activities:

- assessing current balance sheet position;
- projecting exogenous factors like the economy, performance of counterparties, competition, etc;
- developing assets and liability strategy;
- simulating strategies;
- determining the most appropriate strategy;
- setting targets;
- communicating targets to appropriate managers and staff; and
- monitoring and reviewing performance.

4.2.3 Liquidity Risk Strategy

Each institution should have an appropriate liquidity strategy for the day-to-day management of liquidity. The strategy should set out the general approach the

institution will have to liquidity, including various quantitative and qualitative targets. This strategy should address the institution's goal of protecting financial strength and the ability to withstand stressful events in the marketplace.

The liquidity risk strategy defined by Board should enunciate specific policies on particular aspects of liquidity risk management, such as:

- **Composition of Assets and Liabilities**. The strategy should outline the mix of assets and liabilities to maintain liquidity. Liquidity risk management and asset/liability management should be integrated to avoid steep costs associated with having to rapidly reconfigure the asset liability profile from maximum profitability due to increased liquidity.

- **Diversification and Stability of Liabilities**. A funding concentration exists when a single decision or a single factor has the potential to result in a significant and sudden withdrawal of funds. Since such a situation could lead to an increased risk, the Board of Directors and senior management should specify guidance relating to funding sources and ensure that the banking institution has a diversified sources of funding day-to-day liquidity requirements. An institution would be more resilient to tight market liquidity conditions if its liabilities were derived from more stable sources. To comprehensively analyze the stability of liabilities/funding sources, the banking institution needs to identify:
  - liabilities that would stay with the institution under any circumstances;
  - liabilities that run-off gradually if problems arise; and
  - liabilities that run-off immediately at the first sign of problems.

- **Managing Liquidity in different currencies:** The institution should have a strategy on how to manage liquidity in different currencies.

- **Dealing with liquidity disruptions:** The institution should put in place strategies to deal with the potential for both temporary and long-term liquidity disruptions. The strategy should take into account the fact that in crisis situations, access to inter bank market could be both difficult and costly.

The liquidity strategy must be documented in a liquidity policy, and communicated throughout the institution. The strategy should be evaluated periodically to ensure that it remains valid.

4.3 Policies, Procedures and Limits

4.3.1 Liquidity Policies

Board of Directors should ensure that there are adequate policies to govern liquidity risk management process. While specific details vary across institutions according to the nature of their business, key elements of any liquidity policy 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 it is approved 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 identifying, monitoring, reporting and reviewing the liquidity position;
- 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); and
- Contingency plan for handling liquidity crises.

To be effective, the liquidity policy must be communicated down the line throughout the institution. It is important that the board and senior management ensure that policies are reviewed at least annually and when there are any material changes in the institution's current and prospective liquidity risk profile. Such changes could stem from internal circumstances (e.g. changes in business focus) or external circumstances (e.g. changes in economic conditions).

Reviews provide the opportunity to fine tune the institution's liquidity policies in light of the institution's liquidity management experience and development of its business. Any significant or frequent exception to the policy is an important barometer to gauge its effectiveness and any potential impact on institutions liquidity risk profile.

4.3.2 Procedures and Limits

Institutions should establish appropriate procedures, processes and limits to implement their liquidity policies. The procedural manual should explicitly narrate the necessary operational steps and processes to execute the relevant liquidity risk controls. The manual should be periodically reviewed and updated to take into account new activities, changes in risk management approaches and systems.

In addition to the statutory limits of Liquidity Reserve Requirement (LRR) the Board and senior management should establish limits on the nature and amount of liquidity risk the institution can assume. 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 banking institution's strategies and activities, it's past performance, the level of earnings, capital available to absorb potential losses, and the Board's tolerance for risk. Balance sheet complexity will determine how much and what types of limits an institution should establish over daily and long-term horizons. While limits will not prevent a liquidity crisis, limit exceptions can be early indicators of excessive risk, inadequate liquidity risk management or trigger the need to revise targets or limits.

4.4 Risk Measurement, Monitoring and Management Information System

Besides the institutional structure discussed earlier, an effective liquidity risk management include systems to identify, measure, monitor and control its liquidity exposures. Management should be able to accurately identify and quantify the primary sources of an institution's liquidity risk timeously. To properly identify the sources, management should understand both existing as well as future risk that the institution can be exposed to. Management should always be alert for new sources of liquidity risk at both transaction and portfolio levels.

Key elements of an effective risk management process include an efficient MIS to identify, measure, monitor and control existing as well as future liquidity risks and reporting them to senior management and the board of directors for proactive remedial action.

As far as information system is concerned, various units related to treasury activities, dealing, treasury operation and risk management function should be integrated. Furthermore, management should ensure proper and timely flow of information among front office, back office and middle office in an integrated manner; however, their reporting lines should be kept separate to ensure independence of these functions.

Periodic reviews should be conducted to determine whether the institution complies with its liquidity risk policies and procedures. Positions that exceed established limits should receive prompt attention of appropriate management and should be resolved according to the process described in approved policies. Periodic reviews of the liquidity management process should also address any significant changes in the nature of instruments acquired, limits, and internal controls that have occurred since the last review.

4.4.1 Measurement and Monitoring of Liquidity Risk

An effective measurement and monitoring process is essential for adequately managing liquidity risk. At a very basic level, liquidity measurement involves assessing all of an institution’s cash inflows against its outflows to identify the potential for any net shortfalls going forward. This includes funding requirements for off-balance sheet commitments. A number of techniques can be used for measuring liquidity risk, ranging from simple calculations and static simulations based on current holdings to highly sophisticated modeling techniques. As all institutions are affected by changes in the economic climate and market conditions, the monitoring of economic and market trends is key to liquidity risk management.

An important aspect of managing liquidity is making assumptions about future funding needs. While certain cash inflows and outflows can be easily calculated or predicted, institutions must also make assumptions about future liquidity needs, both in the very short-term and for longer time periods. One important factor to consider is the critical role an institution’s reputation plays in its ability to access funds readily and at reasonable terms. For that reason, staff responsible for managing overall liquidity should be aware of any information public or otherwise, that could have an impact on market and public perceptions about the soundness of the institution.

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. Discussed below are some (but not all) commonly used liquidity measurement and monitoring techniques that may be adopted by institutions.

i) Contingency Funding Plans (CFP)

In order to develop a comprehensive liquidity risk management framework, institutions should have way out plans for stress scenarios. Such a plan commonly known as CFP is a set of policies and procedures that serves as a blue print for an institution to meet its funding needs in a timely manner and at a reasonable cost. *A CFP is a projection of future cash flows and funding sources of an institution under market scenarios including aggressive asset growth or rapid liability erosion.* To be effective, it is important that a CFP should represent management's best estimate of balance sheet changes that may result from a liquidity or credit event. A CFP can provide a useful framework for managing liquidity risk both short term and in the long term. Furthermore, it helps ensure that a banking institution can prudently and efficiently manage routine and extraordinary fluctuations in liquidity. The scope of the CFP is discussed in more detail below.

- **Use of CFP for Routine Liquidity Management**

For day-to-day liquidity risk management integration, liquidity scenarios will ensure that the banking institution is best prepared to respond to an unexpected problem. In this sense, a CFP is an extension of ongoing liquidity management and formalizes the objectives of liquidity management by ensuring:

a) a reasonable amount of liquid assets are maintained;
b) measurement and projection of funding requirements during various scenarios; and
c) management of access to funding sources.

- **Use of CFP for Emergency and Distress Environments**

It is not always that liquidity crisis shows up gradually. In case of a sudden liquidity stress, it is important for an institution to be seen as organized, candid, and efficient to meet its obligations to the stakeholders. Since such a situation requires a spontaneous action, institutions that already have plans to deal with such situation could address the liquidity problem more efficiently and effectively. A CFP can help ensure that management and key staff are ready to respond to such situations. Bank liquidity is very sensitive to negative trends in credit, capital, or reputation. Deterioration in the company's financial condition (reflected in items such as asset quality indicators, earnings, or capital), management composition, or other relevant issues may result in reduced access to funding.

- **Scope of CFP**

The sophistication of a CFP depends upon the size, nature, complexity of business, risk exposure, and institutional structure. The CFP should anticipate all of the banking institution's funding and liquidity needs by:

a) analyzing and making quantitative projections of all significant on and off balance-sheet funds flows and their related effects;
b) matching potential cash flow sources and uses of funds; and
c) establishing indicators that alert management to a predetermined level of potential risks.

The CFP should project the banking institution's funding position during both temporary and long-term liquidity changes, including those caused by liability erosion. The CFP should explicitly identify, quantify, and rank all sources of funding by preference, such as:

a) reducing assets;
b) modification or increasing liability structure; and
c) using other alternatives for controlling balance sheet changes.

The CFP should include asset side as well as liability side strategies to deal with liquidity crises. The asset side strategy may include; whether to liquidate surplus money market assets, when to sell liquid or longer-term assets, etc. While liability side strategies specify policies such as pricing policy for funding, the dealer who could assist at the time of liquidity crisis, policy for early redemption request by retail customers, use of RBM discount window etc. A CFP should also indicate roles and responsibilities of various individuals at the time of liquidity crises and the management information system between management, ALCO, traders, RBM and the general public.

This outline of the scope of a good CFP is by no means exhaustive. Institutions should devote significant time and consideration to scenarios that are most likely given their activities.

(ii) Maturity Ladder

A maturity ladder is a useful device to compare cash inflows and outflows both on a day-to-day basis and over a series of specified time periods. The number of time frames in such maturity ladder is of significant importance and to some extent depends upon nature of banking institution’s liability or sources of funds. Institutions, which rely on short term funding, will concentrate primarily on managing liquidity on very short term whereas, other institutions might actively manage their net funding requirement over a slightly longer period. In the short term, institution’s flow of funds could be estimated more accurately and also such estimates are of more importance as these provide an indication of actions to be taken immediately. Further, such an analysis for distant periods will maximize the opportunity for the institution to manage the funding gap well in advance before it crystallizes. Consequently institutions should use short time frames to measure near term exposures and longer time frames thereafter. It is suggested that institutions calculate daily gap for next one or two weeks, monthly gap for next six month or a year and quarterly thereafter. While making an estimate of cash flows, the following aspects need attention:

a. the funding requirement arising out of off- balance sheet commitments also need to be accounted for;
b. many cash flows associated with various products are influenced by interest rates or customer behavior. Institutions need to take into account behavioral aspects (anticipated maturity) instead of contractual maturity. In this respect past experiences could give important guidance to make any assumption;
c. some cash flows may be seasonal or cyclical; and
d. management should also consider increases or decreases in liquidity that typically occur during various phases of an economic cycle.

While the institutions should have liquidity sufficient enough to meet fluctuations in loans and deposits, as a safety measure institutions should maintain a margin of excess liquidity. To ensure that this level of liquidity is maintained, management should estimate liquidity needs in a variety of scenarios.

(iii) Liquidity Ratios and Limits

Institutions may use a variety of ratios to quantify liquidity. These ratios can also be used to create limits for liquidity management. However, such ratios would be meaningless unless used regularly and interpreted taking into account qualitative factors. Ratios should always be used in conjunction with more qualitative information such as borrowing capacity, the likelihood of increased requests for early withdrawals, decreases in credit lines, decreases in transaction size, or shortening of term funds available to the banking institution. To the extent that any asset-liability management decisions are based on financial ratios, an institution's asset-liability function should understand how a ratio is constructed, the range of alternative information that can be placed in the numerator or denominator, and the scope of conclusions that can be drawn from ratios. A fuller appreciation of ratios should recognize uniqueness of individual institutions where comparative data is available and seasonal or time differences of a single institution.

- **Cash Flow Ratios and Limits.** One of the most serious sources of liquidity risk emanates from an institution's failure to "roll over" a maturing liability. Cash flow ratios and limits attempt to measure and quantify the effect of the volume of liabilities maturing during a specified period of time.

- **Liability Concentration Ratios and Limits.** Liability concentration ratios and limits help to prevent an institution from relying on too few providers or funding sources. Limits are usually expressed as either a percentage of liquid assets or an absolute amount. Sometimes they are more indirectly expressed as a percentage of deposits, purchased funds, or total liabilities.

- **Other Balance Sheet Ratios.** Total loans/total deposits, liquid assets/demand liabilities, total loans/total equity capital, borrowed funds/total assets etc are examples of common ratios used by banking institutions to monitor current and potential funding levels.

4.4.2 Foreign Currency Liquidity Management

Each institution should have a measurement, monitoring and control system for its liquidity positions in the major currencies in which it is active. In addition to assessing its aggregate foreign currency liquidity needs and the acceptable mismatch in combination with its domestic currency commitments, an institution should also undertake separate analysis of its strategy for each currency. Merely meeting the RBM Foreign Currency Exposure limits is not enough to manage the institution's exposure to foreign currency risk.

4.4.3 Managing Market Access

Each institution should periodically review its efforts to establish and maintain relationships with liability holders, to maintain the diversification of liabilities, and aim to ensure its capacity to sell assets without undue delay.

4.4.4 Review of Assumptions Utilized in Managing Liquidity

Since an institution's future liquidity position will be affected by factors that cannot always be forecast with precision, assumptions need to be reviewed frequently to determine their continuing validity, especially given the rapidity of change in the markets.

4.4.5 Stress Testing

Banking institution should conduct regular stress tests by applying various scenarios on their liquidity positions to ensure that they have adequate liquidity to withstand stressed conditions.

The board of directors and senior management should examine stress-testing results and formulate appropriate strategies to address the cash-flow needs revealed by the scenario analysis. For example, there may be a need to reduce liquidity risk by obtaining more long-term funding or restructuring the composition of assets.

It is important for banking institutions to construct reasonable adverse scenarios when stress testing liquidity, and to examine the resultant cash-flow needs. While banking institutions are encouraged to cover stress events of different types and levels of adversity, they should include the following scenarios in their stress testing exercise:
i. institution-specific crisis scenario; and
ii. general market crisis scenario.

Institution-specific crisis scenarios cover situations where there are some real or perceived problems at an institution, for example, operational problems, solvency concerns or adverse credit rating changes. A general market crisis scenario is one where liquidity at a large number of institutions in one or more markets, is affected.

An institution should detail the assumptions underlying the behaviour of the cashflows of its assets, liabilities and off-balance sheet items under plausible crisis scenarios. The timing and size of the cashflows are important factors to consider.

The assumptions may differ quite sharply from scenario to scenario as cashflow timing and size can behave differently in different situations. Bank institutions should factor in the settlement period or the expected time needed for liquidating assets.

Key assumptions underlying an institution-specific crisis scenario should be that many of the institution's liabilities cannot be rolled-over or replaced, resulting in required repayment at maturity such that the institution would have to wind down its books to some degree.The minimum criteria for using various assumptions when stress testing liquidity risk are as follows:

- the assumptions have to be consistent and reasonable for each scenario;
- the assumptions should be verified and supported by sufficient evidence,experience and performance rather than arbitrarily selected;
- banking institutions should document the behavioural assumptions in their liquidity management policy statement. The type of analysis performed under each assumption should also be documented to facilitate periodic review;
- senior management should ensure that key assumptions are evaluated at least annually for reasonableness.

Under a **general market crisis scenario,** it is assumed that a banking institution may have less control over the level and timing of future cash flows. Characteristics of this scenario may include a liquidity squeeze, counterparty defaults and substantial discounts needed to sell assets and wide differences in funding access among banking institutions due to the occurrence of a severe tiering of their perceived credit quality (i.e. flight to quality).

When performing scenario analysis, institutions may factor in the possibility of intra-group or head office support. This support would be of particular value in a crisis affecting only local operations (because of territorial or jurisdictional limitations) but could prove to be ineffective if the crisis impinged upon the group as a whole. In addition banking institutions should document:

- cash-flow assumptions for the institution specific and general market crisis scenarios; and
- their own estimate of the minimum number of days needed to arrange emergency funding support from other sources.

4.5 Management Information System

An effective management information system (MIS) is essential for sound liquidity management decisions. Information should be readily available for day-to-day liquidity management and risk control, as well as during times of stress. Data should be appropriately consolidated, comprehensive yet concise, focused and available in a timely manner. Ideally, the regular reports an institution generates will enable it to monitor liquidity during a crisis; managers would simply have to prepare the reports more frequently. Managers should keep crisis monitoring in mind when developing liquidity MIS. There is usually a trade -off between accuracy and timeliness as liquidity problems can arise very quickly, and effective liquidity management may require daily internal reporting. Since bank liquidity is

primarily affected by large, aggregate principal cash flows, detailed information on every transaction may not improve the analysis.

The management information system should be used to check compliance with the institution's established policies, procedures and limits and with RBM's prudential requirements on Liquidity. Reporting of risk measures should be done on a timely basis and compare current liquidity exposures with any set limits. The information system should also enable management to evaluate the level of trends in the institution's aggregate liquidity exposure.

Management should develop systems that can capture significant information. The content and format of reports depend on an institution's liquidity management practices, risks, and other characteristics. Routine reports may include a list of large funds providers, a cash flow or funding gap report, a funding maturity schedule, and a limit monitoring and exception report. Day-to-day management may require more detailed information, depending on the complexity of the banking institution and the risks it undertakes. Management should regularly consider how best to summarize complex or detailed issues for senior management or the Board. Besides, other types of information important for managing day-to-day activities and for understanding the banking institution's inherent liquidity risk profile include:

a) asset quality and its trends;
b) earnings projections;
c) the bank's general reputation in the market and the condition of the market itself;
d) the type and composition of the overall balance sheet structure; and
e) the type of new deposits being obtained, as well as its source, maturity and price.

4.6 Internal Controls

Institutions should have adequate internal controls to ensure the integrity of their liquidity risk management process. These should be an integral part of the institution's overall system of internal control aimed at promoting effective and efficient operations, reliable financial and regulatory reporting, and compliance with relevant laws, regulations and institutional policies. An effective system of internal control for liquidity risk includes:

a) a strong control environment;
b) an adequate process for identifying and evaluating liquidity risk;
c) the establishment of control activities such as policies and procedures;
d) adequate management information systems; and,
e) continuous review of adherence to established policies and procedures.

With regard to control policies and procedures, attention should be given to appropriate approval processes, limits, reviews and other mechanisms designed to provide a reasonable assurance that the institution's liquidity risk management objectives are achieved. Many attributes of a sound risk management process, including risk measurement, monitoring and control functions, are key aspects of an effective system of internal control. Institutions should ensure that all aspects of the internal control system

are effective, including those aspects that are not directly part of the risk management process.

In addition, an important element of an institution's internal control system over its liquidity risk management process is regular evaluation and review. This includes ensuring that personnel are following established policies and procedures, as well as ensuring that the procedures that were established actually accomplish the intended objectives. Such reviews and evaluations should also address any significant change that may impact on the effectiveness of controls. The board should ensure that all such reviews and evaluations are conducted regularly by individuals who are independent of the function being reviewed. When revisions or enhancements to internal controls are warranted, there should be a mechanism in place to ensure that these are implemented timeously.

Limit breaches should receive prompt attention of appropriate management and should be resolved according to the processes described in approved policies. Periodically, the internal audit function should review the liquidity management process in order to identify any weaknesses or problems which in turn should be addressed by management.

5 INTEREST RATE RISK MANAGEMENT GUIDELINES

5.1 Introduction

Interest rate risk is the exposure of an institution's financial condition to adverse movements in interest rates. Accepting this risk is a normal part of banking and can be an important source of profitability and shareholder value. However, excessive interest rate risk taking can pose a significant threat to a banking institution's earnings and capital base. Changes in interest rates affect a banking institution's earnings by changing its net interest income and the level of other interest-sensitive income and operating expenses. Changes in interest rates also affect the underlying value of the banking institution's assets, liabilities and off-balance sheet instruments because the present value of future cash flows (and in some cases, the cash flows themselves) change when interest rates change. Accordingly, an effective risk management process that maintains interest rate risk within prudent levels is essential to the safety and soundness of banking institutions.

The primary forms of interest rate risk to which banking institutions are typically exposed include repricing risk, yield curve risk, basis risk and optionality, each of which is discussed in greater detail below. These sections also describe the two most common perspectives for assessing a banking institution's interest rate risk exposure: the earnings perspective and the economic value perspective. As the names suggest, the earnings perspective focuses on the impact of interest rate changes on a banking institution's near-term earnings, while the economic value perspective focuses on the value of a banking institution's net cash flows.

5.1.1 Sources of Interest Rate Risk

Repricing risk: Institutions encounter interest rate risk in several ways. The primary and most often discussed form of interest rate risk arises from timing differences in the maturity (for fixed rate) and repricing (for floating rate) of assets, liabilities and off-balance-sheet (OBS) positions. While such repricing mismatches are fundamental to the business of banking, they can expose a banking institution's income and underlying economic value to unanticipated fluctuations as interest rates vary. For instance, a banking institution that funded a long-term fixed rate loan with a short-term deposit could face a decline in both the future income arising from the position and its underlying value if interest rates increase. These declines arise because the cash flows on the loan are fixed over its lifetime, while the interest paid on the funding is variable, and increases after the short-term deposit matures.

Yield curve risk: Repricing mismatches can also expose a banking institution to changes in the slope and shape of the yield curve. Yield curve risk arises when unanticipated shifts of the yield curve have adverse effects on a banking institution's income or underlying economic value. For instance, the underlying economic value of a long position in 10-year government bonds hedged by a short position in 5-year government notes could decline sharply if the yield curve steepens, even if the position is hedged against parallel movements in the yield curve.

Basis risk: Another important source of interest rate risk (commonly referred to as basis risk) arises from imperfect correlation in the adjustment of the rates earned and paid on different instruments with otherwise similar repricing characteristics. When interest rates change, these differences can give rise to unexpected changes in the cash flows and earnings spread between assets, liabilities and OBS instruments of similar maturities or repricing frequencies. For example, a strategy of funding a one year loan that reprices monthly based on prime rate[5], with a one-year deposit that reprices monthly based on one month treasury bill rate, exposes the institution to the risk that the spread between the two index rates may change unexpectedly.

Optionality: An additional and increasingly important source of interest rate risk arises from the options embedded in many banking institution assets, liabilities and OBS portfolios. Formally, an option provides the holder with the right, but not the obligation, to buy, sell, or in some manner alter the cash flow of an instrument or financial contract. Options may be stand alone instruments or they may be embedded within otherwise standard instruments. While banking institutions use options in both trading and non-trading accounts, instruments with embedded options are generally most important in non-trading activities. They include various types of bonds and notes with call or put provisions, loans which give borrowers the right to prepay balances, and various types of non-maturity deposit instruments which give depositors the right to withdraw funds at any time, often without any penalties. If not adequately managed, the asymmetrical payoff characteristics of instruments with optionality features can pose significant risk particularly to those who sell them, since the options held, both explicit and embedded, are generally exercised to the advantage of the holder and the disadvantage of the seller. Moreover, an increasing array of options can involve significant leverage which can magnify the influences (both negative and positive) of option positions on the financial condition of the firm.

5.2 Board and Senior Management Oversight

Effective oversight by the board of directors and senior management is critical to a sound interest rate risk management process. It is essential that these individuals are aware of their responsibilities with regard to interest rate risk management and that they adequately perform their roles in overseeing and managing interest rate risk.

5.2.1 Board Oversight

The board of directors has the ultimate responsibility for understanding the nature and the level of interest rate risk taken by the banking institution. As such, the board should:

- approve broad business strategies and policies that govern or influence the interest rate risk of the banking institution;
- review the overall objectives of the banking institution with respect to interest rate risk;
- provide clear guidance regarding the level of interest rate risk acceptable to the banking institution;

[5] The prime interest rate is the rate charged by institutions for short-term loans to corporations or individuals whose credit standing is high enough that little risk to the lender is involved in making the loan. This rate fluctuates based on economic conditions and may be different among institutions. The prime rate serves as a basis for the interest rates charged for other higher-risk loans.

- approve policies that identify lines of authority and responsibility for managing interest rate risk exposures;
- ensure that senior management possesses sufficient knowledge and is fully capable of conducting interest rate related activities including taking the steps necessary to identify, measure, monitor, and control these risks;
- ensure that the board or a specific committee of the board periodically reviews 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 board-approved policies. Such reviews should be conducted regularly, being carried out more frequently where the banking institution holds significant positions in complex instruments; and
- ensure that the board or one of its committees periodically re-evaluates interest rate risk management policies as well as overall business strategies that affect the interest rate risk exposure of the banking institution.

5.2.2 Senior Management Oversight

Senior management is responsible for:

- developing and establishing policies and procedures for managing interest rate risk on both a long-term and day-to-day basis;
- maintaining clear lines of authority and responsibility for managing and controlling this risk;
- implementing strategies in a manner that limits risks associated with each strategy and that ensures compliance with laws and regulations;
- maintaining appropriate limits on risk taking;
- maintaining adequate systems and standards for measuring risk;
- maintaining standards for valuing positions and measuring performance;
- maintaining a comprehensive interest rate risk reporting and interest rate risk management review process;
- maintaining effective internal controls and ethical standards;
- ensuring that interest rate risk reports to senior management provide aggregate information as well as sufficient supporting detail to enable management assess the sensitivity of the institution to changes in market conditions and other important risk factors;
- periodically reviewing the institution’s interest rate risk management policies and procedures to ensure that they remain appropriate and sound at all times;
- ensuring that analysis and risk management activities related to interest rate risk are conducted by competent staff with technical knowledge and experience consistent with the nature and scope of the banking institution's activities and
- ensuring that there is sufficient depth in staff resources to manage these activities and to accommodate the temporary absence of key personnel.

5.3 Policies, Procedures and Limits

5.3.1 Policies and procedures

It is essential that banking institution’s interest rate risk policies and procedures are clearly defined and consistent with the nature and complexity of their activities.

Banking institutions should have clearly defined policies and procedures for limiting and controlling interest rate risk. Such policies and procedures should delineate lines of responsibility and accountability over interest rate risk management decisions and should clearly define authorised instruments, hedging strategies and position taking opportunities. Interest rate risk policies should also identify quantitative parameters that define the level of interest rate risk acceptable for the banking institution. Where appropriate, such limits should be further specified for certain types of instruments, portfolios, and activities. All interest rate risk policies should be reviewed periodically and revised as needed. Management should define the specific procedures and approvals necessary for exceptions to policies, limits and authorisations.

Policies should clearly identify:

- the types of instruments and activities that an institution may employ or conduct, as a means of communicating the institution's risk tolerance;
- permissible instruments, either specifically or by their characteristics, and should also describe the purposes or objectives for which they may be used; and
- a delineated set of institutional procedures for acquiring specific instruments, managing portfolios, and controlling the banking institution's aggregate interest rate risk exposure.

Products and activities that are new to the banking institution should undergo a careful pre-acquisition review to ensure that the banking institution understands their interest rate risk characteristics and can incorporate them into its risk management process. When analysing whether or not a product or activity introduces a new element of interest rate risk exposure, the banking institution should be aware that changes to an instrument's maturity, repricing or repayment terms can materially affect the product's interest rate risk characteristics.

Prior to introducing a new product, hedging, or position-taking strategy, management should ensure that adequate policies and procedures are in place. The board should also approve major hedging or risk management initiatives in advance of their implementation. Proposals to undertake new instruments or new strategies should contain these features:

- a description of the relevant product or strategy;
- an identification of the resources required to establish sound and effective interest rate risk management of the product or activity;
- an analysis of the reasonableness of the proposed activities in relation to the banking institution's overall financial condition and capital levels; and
- the policies and procedures to be used to measure, monitor and control the risks of the proposed product or activity.

5.3.2 Limits

Institutions should put in place risk taking guidelines in order to maintain a banking institution's interest rate risk exposure within self-imposed parameters over a range of possible changes in interest rates. Such guidelines should set limits for the level of interest rate risk for the banking institution and those limits could be applied on individual portfolios, activities or business units. An appropriate limit system should enable management to control interest rate risk exposures, initiate discussion about

opportunities and risks, and monitor actual risk taking against predetermined risk tolerances.

Limit systems should also ensure that positions that exceed certain predetermined levels receive prompt management attention.

Interest rate risk limits clearly articulating the amount of interest rate risk acceptable to the banking institution should be approved by the board of directors and re-evaluated periodically. Such limits should be appropriate to the size, complexity and capital adequacy of the banking institution as well as its ability to measure and manage its risk.

Limit exceptions should be made known to appropriate senior management without delay. There should be a clear policy as to how senior management will be informed and what action should be taken by management in such cases. Particularly important is whether limits are absolute in the sense that they should never be exceeded or whether, under specific circumstances, which should be clearly described, breaches of limits can be tolerated for a short period of time. In that context, the relative conservatism of the chosen limits may be an important factor.

5.4 Risk Measurement, Monitoring and Management Information System

As indicated above, changes in interest rates can have adverse effects both on a banking institution's earnings and its economic value. This has given rise to two separate, but complementary, perspectives for assessing interest rate risk exposure.

Earnings perspective: In the earnings perspective, the focus of analysis is the impact of changes in interest rates on accrual or reported earnings. This is the traditional approach to interest rate risk assessment taken by many banking institutions. Variation in earnings is an important focal point for interest rate risk analysis because reduced earnings or outright losses can threaten the financial stability of an institution by undermining its capital adequacy and by reducing market confidence.

In this regard, the component of earnings that has traditionally received the most attention is net interest income (i.e. the difference between total interest income and total interest expense). This focus reflects both the importance of net interest income in banking institutions' overall earnings and its direct and easily understood link to changes in interest rates. However, as banking institutions have expanded increasingly into activities that generate fee-based and other non-interest income, a broader focus on overall net income - incorporating both interest and non-interest income and expenses - has become more common. Even traditional sources of non-interest income such as transaction processing fees are becoming more interest rate sensitive. This increased sensitivity should lead management to take a broader view of the potential effects of changes in market interest rates on earnings and to factor these broader effects into their estimated earnings under different interest rate environments.

Economic value perspective: Variation in market interest rates can also affect the economic value of a banking institution's assets, liabilities and OBS positions. Thus, the sensitivity of a banking institution's economic value to fluctuations in interest rates should be given consideration by board and management of institutions. The economic

value of an instrument represents an assessment of the present value of its expected net cash flows, discounted to reflect market rates. By extension, the economic value of a banking institution can be viewed as the present value of expected net cash flows, defined as the expected cash flows on assets minus the expected cash flows on liabilities plus the expected net cash flows on OBS positions. In this sense, the economic value perspective reflects one view of the sensitivity of the net worth of the banking institution to fluctuations in interest rates.

Since the economic value perspective considers the potential impact of interest rate changes on the present value of all future cash flows, it provides a more comprehensive view of the potential long-term effects of changes in interest rates than is offered by the earnings perspective. This comprehensive view is important since changes in near-term earnings – the typical focus of the earnings perspective - may not provide an accurate indication of the impact of interest rate movements on the banking institution's overall positions.

***Embedded losses**:* The earnings and economic value perspectives discussed thus far focus on how future changes in interest rates may affect a banking institution's financial performance. When evaluating the level of interest rate risk it is willing and able to assume, a banking institution should also consider the impact that past interest rates may have on future performance. In particular, instruments that are not marked to market may already contain embedded gains or losses due to past rate movements. These gains or losses may be reflected over time in the banking institution's earnings. For example, a long term fixed rate loan entered into when interest rates were low and refunded more recently with liabilities bearing a higher rate of interest will, over its remaining life, represent a drain on the banking institution's resources.

5.4.1 Interest Rate Risk Measurement and Monitoring

In general, but depending on the complexity and range of activities, banking institutions should have interest rate risk measurement systems that assess the effects of rate changes on both earnings and economic value. These systems should provide meaningful measures of a banking institution's current levels of interest rate risk exposure, and should be capable of identifying any excessive exposures that might arise.

Measurement systems should:

- assess all material interest rate risk associated with a banking institution's assets, liabilities, and OBS positions;
- utilise generally accepted financial concepts and risk measurement techniques; and
- have well documented assumptions and parameters.

As a general rule, it is desirable for any measurement system to incorporate interest rate risk exposures arising from the full scope of a banking institution's activities, including both trading and non-trading sources. This does not preclude different measurement systems and risk management approaches being used for different activities; however, management should have an integrated view of interest rate risk across products and business lines.

A banking institution's interest rate risk measurement system should address all material sources of interest rate risk including repricing, yield curve, basis and option risk exposures. In many cases, the interest rate characteristics of a banking institution's largest holdings will dominate its aggregate risk profile. While all of a banking institution's holdings should receive appropriate treatment, measurement systems should evaluate such concentrations with particular rigour. Interest rate risk measurement systems should also provide rigorous treatment of those instruments which might significantly affect an aggregate position, even if they do not represent a major concentration. Instruments with significant embedded or explicit option characteristics should receive special attention.

A number of techniques are available for measuring the interest rate risk exposure of both earnings and economic value. Their complexity ranges from simple calculations to static simulations using current holdings to highly sophisticated dynamic modeling techniques that reflect potential future business and business decisions.

Gap Analysis: The simplest techniques for measuring interest rate risk exposure begin with a maturity/repricing schedule that distributes interest-sensitive assets, liabilities and OBS positions into "time bands" according to their maturity (if fixed rate) or time remaining to their next repricing (if floating rate). These schedules can be used to generate simple indicators of the interest rate risk sensitivity of both earnings and economic value to changing interest rates. When this approach is used to assess the interest rate risk of current earnings, it is typically referred to as *gap analysis*. The size of the gap for a given time band - that is, assets minus liabilities plus OBS exposures that reprice or mature within that time band - gives an indication of the banking institution's repricing risk exposure.

Duration: Duration is a measure of the percent change in the economic value of a position that will occur given a small change in the level of interest rates. A maturity/repricing schedule can be used to evaluate the effects of changing interest rates on a banking institution's economic value by applying sensitivity weights to each time band. Typically, such weights are based on estimates of the *duration* of the assets and liabilities that fall into each time-band. Duration-based weights can be used in combination with a maturity/repricing schedule to provide a rough approximation of the change in a banking institution's economic value that would occur given a particular set of changes in market interest rates.

Simulation Techniques: More sophisticated interest rate risk measurement systems include Simulation Techniques. *Simulation techniques* typically involve detailed assessments of the potential effects of changes in interest rates on earnings and economic value by simulating the future path of interest rates and their impact on cash flows.

In *static simulations*, the cash flows arising solely from the banking institution's current on- and off-balance sheet positions are assessed. For assessing the exposure of earnings, simulations estimating the cash flows and resulting earnings streams over a specific period should be conducted based on one or more assumed interest rate scenarios. These simulations should entail straight forward shifts or tilts of the yield
curve or changes of spreads between different interest rates. When the resulting cash flows are simulated over the entire expected lives of the banking institution’s holdings

and discounted back to their present values, an estimate of the change in the banking institution's economic value should be calculated.

In a *dynamic simulation* approach, the simulation builds in more detailed assumptions about the future course of interest rates and expected changes in a banking institution's business activity over that time. These more sophisticated techniques allow for dynamic interaction of payments streams and interest rates, and better capture the effect of embedded or explicit options.

Regardless of the measurement system, the usefulness of each technique depends on the validity of the underlying assumptions and the accuracy of the basic methodologies used to model interest rate risk exposure. In designing interest rate risk measurement systems, banking institutions should ensure that the degree of detail about the nature of their interest-sensitive positions is commensurate with the complexity and risk inherent in those positions. For instance, using gap analysis, the precision of interest rate risk measurement depends in part on the number of time bands into which positions are aggregated. Clearly, aggregation of positions/cash flows into broad time bands implies some loss of precision. In practice, the banking institution must assess the significance of the potential loss of precision in determining the extent of aggregation and simplification to be built into the measurement approach.

Estimates of interest rate risk exposure, whether linked to earnings or economic value, utilise, in some form, forecasts of the potential course of future interest rates. For risk management purposes, banking institutions should incorporate a change in interest rates that is sufficiently large to encompass the risks attendant to their holdings. Banking institutions should consider the use of multiple scenarios, including potential effects in changes in the relationships among interest rates (i.e. yield curve risk and basis risk) as well as changes in the general level of interest rates. For determining probable changes in interest rates, simulation techniques could, for example, be used. Statistical analysis can also play an important role in evaluating correlation assumptions with respect to basis or yield curve risk.

In assessing the results of interest rate risk measurement systems, it is important that:

- the assumptions underlying the system are clearly understood by risk managers and senior management;
- techniques using sophisticated simulations should be used carefully so that they do not become "black boxes", producing numbers that have the appearance of precision, but that in fact are not very accurate when their specific assumptions and parameters are revealed;
- key assumptions should be recognised by senior management and risk managers and should be re-evaluated at least annually;
- key assumptions are clearly documented and their significance understood; and
- assumptions used in assessing the interest rate sensitivity of complex instruments and instruments with uncertain maturities should be subject to particularly rigorous documentation and review.

5.4.2 Stress testing

The risk measurement system should also support a meaningful evaluation of the effect of stressful market conditions on the banking institution. Stress testing should be designed to provide information on the kinds of conditions under which strategies or positions would be most vulnerable, and thus may be tailored to the risk characteristics of the banking institution. Possible stress scenarios might include:

- abrupt changes in the general level of interest rates;
- changes in the relationships among key market rates (i.e. basis risk);
- changes in the slope and the shape of the yield curve (i.e. yield curve risk);
- changes in the liquidity of key financial markets or changes in the volatility of market rates; or
- conditions under which key business assumptions and parameters break down.

The stress testing of assumptions used for illiquid instruments and instruments with uncertain contractual maturities is particularly critical to achieving an understanding of the banking institution's risk profile. In conducting stress tests, special consideration should be given to instruments or markets where concentrations exist as such positions may be more difficult to liquidate or offset in stressful situations. Banking institutions should consider "worst case" scenarios in addition to more probable events. Management and the board of directors should periodically review both the design and the results of such stress tests, and ensure that appropriate contingency plans are in place.

5.4.3 Management Information Systems

An accurate, informative, and timely management information system is essential for managing interest rate 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 modelling shortcomings.

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

- summaries of the banking institution's aggregate interest rate exposures;
- reports demonstrating compliance with policies and limits;
- key assumptions, for example, non-maturity deposit behaviour and prepayment information;
- results of stress tests including those assessing breakdowns in key assumptions and parameters; and
- summaries of the findings of reviews of interest rate risk policies, procedures, and the adequacy of the interest rate risk measurement systems, including any findings of internal and external auditors or any other independent reviewer.

5.5 Internal Controls

Banking institutions should have adequate internal controls to ensure the integrity of their interest rate 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 relevant laws, regulations and institutional policies.

An effective system of internal control for interest rate risk should ensure that:

- there is a strong control environment;
- an adequate process for identifying and evaluating risk is in place;
- there are adequate control activities such as policies, procedures and methodologies; and
- there is an effective management information system.

Banking institutions should have their measurement, monitoring and control functions reviewed on a regular basis by an independent party (such as an internal or external auditor). It is essential that any independent reviewer ensures that the risk measurement system is sufficient to capture all material elements of interest rate risk, whether arising from on- or off-balance sheet activities. Such a reviewer should consider the following factors in making the risk assessment:

- the quantity of interest rate risk, e.g.
  - the volume and price sensitivity of various products;
  - the vulnerability of earnings and capital under differing rate changes including, yield curve twists; and
  - the exposure of earnings and economic value to various other forms of interest rate risk, including basis and optionality risk.
- the quality of interest rate risk management, e.g.
  - whether the banking institutions's internal measurement system is appropriate to the nature, scope, and complexities of the entity and its activities;
  - whether the banking institution has an independent risk control unit responsible for the design and administration of the risk measurement, monitoring and control functions;
  - whether the board of directors and senior management are actively involved in the risk control process;
  - whether internal policies, controls and procedures concerning interest rate risk are well documented and complied with;
  - whether the assumptions of the risk measurement system are well documented, data accurately processed, and data aggregation is proper and reliable; and
  - whether the institution has adequate staffing to conduct a sound risk management process.

In those instances where the independent review is conducted by internal auditors, banking institutions are encouraged to have the risk measurement, monitoring and control functions periodically reviewed by external auditors.

5.6 Lines of responsibility and authority

Care should be taken to ensure that there is adequate separation of duties in key elements of the risk management process to avoid potential conflicts of interest. Management

should ensure that sufficient safeguards exist to minimise the potential that individuals initiating risk-taking positions may inappropriately influence key control functions of the risk management process such as the development and enforcement of policies and procedures, the reporting of risks to senior management, and the conduct of back-office functions. The nature and scope of such safeguards should be in accordance with the size and structure of the banking institution. They should also be commensurate with the volume and complexity of interest rate risk incurred by the banks and the complexity of its transactions and commitments.

6 FOREIGN EXCHANGE RATE RISK MANAGEMENT GUIDELINES

6.1 Introduction

Foreign exchange rate risk is the potential impact of adverse currency rate movements on earnings and economic value. This involves settlement risk which arises when a banking institution incurs financial loss due to foreign exchange positions taken in both the trading and banking books.

The foreign exchange positions arise from the following activities:

- trading in foreign currencies through spot, forward and option transactions as a market maker or position taker, including the unhedged positions arising from customer-driven foreign exchange transactions;
- holding foreign currency positions in the banking book (e.g. in the form of loans, bonds, deposits or cross-border investments); or
- engaging in derivative transactions (e.g. structured notes, synthetic investments and structured deposits) that are denominated in foreign currency for trading or hedging purposes.

6.2 Board and Senior Management Oversight

The board of directors and senior management have ultimate responsibility for understanding the nature and level of foreign exchange risk taken by the banking institution and the management thereof.

Board oversight may be delegated to an appropriate subcommittee such as the Asset and Liability Committee (ALCO) or Risk Management Committee.

The board and senior management's responsibilities include:

- setting the foreign exchange risk management strategy and tolerance levels;
- ensuring that effective risk management systems and internal controls are in place;
- monitoring significant foreign exchange exposures;
- ensuring that foreign exchange operations within the banking institution are in compliance with foreign exchange control regulations;
- ensuring that foreign exchange operations are supported by adequate management information systems which complement the risk management strategy; and
- reviewing policies, procedures and currency limits regularly in line with changes in the economic environment.

6.3 Policies and Procedures

Banking institutions should have written policies and procedures for identifying, measuring and controlling foreign exchange rate risk. The policies and procedures should be consistent with the institution's strategies, financial condition, and risk tolerance levels.

The policies and procedures should be supplemented with ethics and observation of set standards by employees engaged in foreign exchange trading.

Policies and procedures should identify the foreign exchange rate risks inherent in services and activities to ensure that their risk characteristics are understood and can be incorporated into the risk management process.

These policies and procedures should:

- define lines of responsibility and identify individuals or committees responsible for developing foreign exchange risk management strategies, making foreign exchange risk management decisions, and conducting oversight;
- identify authorized types of financial instruments and hedging strategies;
- describe a set of strategies for controlling the institution's aggregate foreign exchange rate risk exposure;
- define quantitative limits on the acceptable level of foreign exchange risk for the institution. The limits include individual currency limits, individual counterparty limits, dealer limits, concentration limits, and stop loss limits; and
- define procedures and conditions for dealing with exceptions to policies, limits, and authorizations.

6.4 Risk Identification, Measurement, Monitoring and Control

6.4.1 Risk identification

Foreign exchange rate risk exposures fall into the following structural and trading categories: *translation exposure:* which arises from accounting based changes in consolidated financial statements caused by changes in exchange rates;

- *transaction exposure:* which occurs when exchange rates change between the time that an obligation is incurred and the time it is settled, thus affecting actual cash flows; and
- *economic exposure:* which reflects the change in the present value of the firm's expected future cash flows as a result of an unexpected change in exchange rates.

6.4.2 Risk Measurement

Banking institutions should have measurement systems that take into account all the sources of foreign exchange risk. The systems should evaluate the effect of foreign exchange rate changes on profitability and economic value of the institution. The measurement systems should:

- evaluate all foreign exchange risks by maturity, on both gross and net bases, arising from the full range of a banking institution's assets, liabilities and off-balance sheet positions;
- employ accepted financial models or methods for measuring risk of foreign exchange options;
- be able to calculate comprehensive risk factor sensitivities for the purpose of capturing the non-linearity nature of price risk of foreign exchange positions;
- have accurate and timely data;
- incorporate daily mark-to-market of trading positions; and
- enable banking institutions to monitor their foreign exchange settlement risk in real-time in order to ensure that settlement limits will not be exceeded.

6.4.3 Risk Limits

In addition to adhering to Foreign Currency Exposure Limits Directive (Directive NO. DO1-97-FX) issued by the Reserve Bank of Malawi, banking institutions should have a comprehensive framework of limits to control foreign exchange risk exposures for different levels of reporting. At a minimum, banking institutions should have the following limits for foreign exchange operations:

- open position limits for individual currencies to which banking institutions have material exposures, both during the day and overnight. Where limits are assigned to a group of currencies, the risk measures should be aggregated on a gross basis;
- open position limits on the aggregate of all currencies, both during the day and overnight;
- open position limits by each centre where the banking institution operates;
- stop loss and/or management-action-trigger limits; and
- limits for settlement risk of all counterparties.
  The limits should be reviewed at least annually or more frequently in line with changes in the operating environment.

6.4.4 Stress Tests

Banking institutions should conduct stress tests on their foreign currency positions. The stress tests for exchange rate risk assess the impact of changes in exchange rates on the profitability and economic value of a banking institution's equity. The effects of significant exchange rate movements, including sharp reductions in liquidity, of individual currencies should be considered when setting stress scenarios.

Stress testing results should be incorporated in the review of business strategies, policies and limits on foreign exchange risk. The assumptions used in the stress testing model should be clearly documented and reviewed from time to time to reflect changes in the operating environment.

6.4.5 Risk Monitoring and Control

Foreign exchange risk monitoring processes should be established to evaluate the performance of a banking institution's risk strategies/policies and procedures in achieving its overall goals. The monitoring function should be independent of units taking risk and should report directly to senior management/board.

The middle office should perform the risk review function in relation to day-to-day activities. Being a highly specialized function, it should be staffed with people who have relevant expertise and knowledge. The unit should also prepare reports for the information of senior management as well as the ALCO. Further, the middle office should reconcile regularly positions of traders to ensure that these are within assigned limits. Internal reports comparing actual positions against internal limits should be routinely prepared for management.

Banking institutions should have management information systems that provide accurate and timely information. Periodic and frequent revaluations at current market rates should permit the monitoring of the banking institution's profits or losses on its foreign exchange book.

6.4.6 Risk Reporting

Types of reports vary depending upon overall foreign exchange risk profile of the banking institution. At a minimum the reports should contain:

- individual and aggregate foreign exchange risk exposures;
- information on adherence to policies and limits; and
- findings of risk reviews on foreign exchange risk policies and procedures including any findings of internal/external auditors.

6.5 Internal Controls and Independent Audits

Banking institutions should conduct periodic reviews of their internal control and risk management process for foreign exchange risk to ensure its integrity,

accuracy and reasonableness. Such reviews should be conducted by parties independent to the function being reviewed.

The reviews should, among others, ensure:

- accuracy and completeness of recording of all transactions;
- effective segregation of duties between trading, settlement and accounting functions; and
- effectiveness and accuracy of reporting of excesses of limits and other exceptions.

Particular attention should be drawn to irregularities in profit and loss, abnormal trading patterns or trends (e.g. unusually large gross positions) and frequent excesses of limits. Internal auditors should ensure that such incidents are properly followed through. Any issues concerning controls in the trading area should be appropriately and timely escalated to senior management.

Banking institutions should promptly respond to findings regarding any violations of established procedures and ensure that there are adequate procedures for addressing weaknesses or irregularities noted by risk control functions, internal or external auditors and supervisory authorities. Internal audit and other risk control functions should be adequately staffed and have sufficient expertise and authority for reviewing the trading business.

7 PRICE RISK MANAGEMENT GUIDELINES

7.1 Introduction

Price risk is the risk that a banking istitution 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 banking institutions to fluctuations in the price or value of on- and off- balance sheet marketable financial instruments. Changes in the prices of equity instruments, commodities and other instruments creates a price risk and the potential for loss arising from the process of revaluing equity or investment positions in Malawi Kwacha terms.

7.2 Board and Senior Management Oversight

The Board of Directors and senior management of banking institutions are ultimately responsible for the institution's exposure to price risk and the level of risk assumed. The Board should, among other things, do the following:

- Put in place well-articulated policies, setting forth the objectives of the banking institution's risk management strategy on commodity dealing/financing with respect to price risk. The parameters and limits within which this strategy is to be controlled should be clearly spelt out.
- Review and approve the price risk management policies and procedures based on recommendations by senior management of the institution;
- Review and approve the procedures for measuring, monitoring and controlling price risk (specifying limits within which foreign exchange transactions shall be conducted).
- Periodically review and approve price risk limits to conform to any changes in the institution's strategies, address new products, and react to changes in market conditions;
- Together with Senior Management, identify and put in place 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;
- Ensure that Management is sufficiently competent and able to respond to price risks that may arise from changes in the competitive environment or from innovations in markets in which the institution is active.

7.3 Policies, Procedures and Limits

Banking institutions should have written policies governing activities in equities trading and other investments, including off- balance sheet items, that communicate the expectations of the board of directors to the management and staff. At a minimum, policies and procedures must set out the following:

- The tolerance level of the board and senior management for the various risks arising from investment and trading activities;
- Limits governing price risk exposure that should include company limit, sectoral exposure and loss limits. Limits for more volatile and less liquid equities and other investments can be lower than those for stable and liquid investments;
- Clearly defined mechanisms by which positions are established by the investment manager/committee.
- The frequency with which positions are revalued and reported to both management and the board.

Overall, the board and senior management should ensure that the policies and guidelines clearly identify procedures to be followed, type of services offered, definition of jobs and responsibilities for all those entrusted with the responsibility of making investment decisions.

7.4 Measuring and Monitoring Price Risk

Measuring risk is critical to understanding the potential loss an institution may be exposed to. The most common approaches to measuring and limiting price risk are:

- Limiting the size and concentration of investments that are price sensitive, based on percentage of either total investment or total assets of the institution;
- Adherence to prudential regulations and the limits on investments imposed by the Banking Act and other relevant laws, regulations and directives; and
- Determining the size of the loss that would be incurred should the prices of shares and other investments move against the position the banking institution has taken.

The principal goal should be to provide strong assurance that losses resulting in price changes involving both on- and off- balance sheet items, will not substantively diminish the capital of the banking institution.

7.5 Management Information System

Accurate and timely information systems are critical to the management of price risk, and for ensuring compliance with relevant risk limits. Banking institutions therefore need to:

- Commit adequate resources to generating information on compliance with relevant risk limits; and
- Design standardised reports to communicate the information regarding risk concentration, current position, country/sectoral exposures etc.

At a minimum, such reports should include:

- total value of outstanding investments, and current market values;
- profit and loss, totals and comparison to previous mark to market;
- aggregate investment limits;
- limit or sectoral excesses; and
- valuation of option contracts, if any.

7.6 Internal Control and Audit

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

The Audit Committee should, among other duties, review periodically the entire price risk management process. The Committee can greatly enhance the quality of reports and the reasonableness of management information supplied to the board, management and the supervisory authority.

8 OPERATIONAL RISK MANAGEMENT GUIDELINES

8.1 Introduction

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.[6]

Globalization, together with increased financial innovation, are making the activities of banking institutions and thus their risk profiles (i.e. the level of risk across an institution's activities and/or risk categories) more complex. Due to these developments, operational risk is becoming more pronounced. Examples of these developments include:

- The greater use of more highly automated technology which has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems;

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

- Acquisitions, mergers, and consolidations test the viability of new or newly integrated systems;

- The emergence of banking institutions acting as large-volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems;

[6] Basle Committee on Banking Supervision, 2003.

- Engagement in risk mitigation techniques (e.g., collateral, netting arrangements, asset securitisation and derivatives) by institutions to optimise their exposure to interest rate risk, foreign exchange risk, price risk and credit risk, but which in turn may produce other forms of risk (e.g. legal risk); and

- Growing use of outsourcing arrangements and the participation in clearing and settlement systems which can mitigate some risks but can also present significant other risks to banking institutions.

The RBM recognises that operational risk is a term that has a variety of meanings within the banking sector and whole financial services industry, and therefore, banking institutions may choose to adopt their own definitions of operational risk. Whatever the exact definition, a clear understanding by banking institutions of what is meant by operational risk is critical to the effective management and control of this risk category. It is also important that the definition considers the full range of material operational risks facing a banking institution and captures the most significant causes of severe operational losses.

Operational risk event types having the potential to result in substantial losses include:

- Internal fraud. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.

- External fraud. For example, robbery, forgery, cheque kiting, and damage from computer hacking.

- Employment practices and workplace safety. For example, workers compensation claims, violation of employee health and safety rules, organized labour activities, discrimination claims, and general liability.

- Clients, products and business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the banking institution's account, money laundering, and sale of unauthorized products.

- Damage to physical assets. For example, terrorism, vandalism, earthquakes, fires and floods.

- Business disruption and system failures. For example, hardware and software failures, telecommunication problems, and utility outages.

- Execution, delivery and process management. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes.

It is clear that operational risk differs from other banking risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and that this affects the risk management process. At the same

time, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to significant losses.

8.2 Board and Senior Management Oversight

Failure to understand and manage operational risk, which is present in virtually all bank transactions and activities, may greatly increase the likelihood that some risks will go unrecognised and uncontrolled. Both the board and senior management are responsible for creating an organisational culture that places high priority on effective operational risk management and adherence to sound operating controls. Operational risk management is most effective where a banking institution's culture emphasises high standards of ethical behaviour at all levels of the entity. The board and senior management should promote an organisational culture which establishes through both actions and words the expectations of integrity for all employees in conducting business.

8.2.1 Board Oversight

The Board of Directors should be aware of the major aspects of the banking institution's operational risks as a distinct category that should be managed, and it should approve and periodically review the banking institution's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

Boards of directors have ultimate responsibility for the level of operational risk taken by their institutions. The board of directors should approve the implementation of an institution-wide framework to explicitly manage operational risk as a distinct risk to the banking institution's safety and soundness. The board should provide senior management with clear guidance and direction regarding the principles underlying the framework and approve the corresponding policies developed by senior management.

An operational risk framework should be based on an appropriate definition of operational risk which clearly articulates what constitutes operational risk in that banking institution. The framework should cover the banking institution's appetite and tolerance for operational risk, as specified through the policies for managing this risk and prioritisation of operational risk management activities, including the extent of, and manner in which, operational risk is transferred outside the banking institution. It should also include policies outlining the banking institution's approach to identifying, assessing, monitoring and controlling/mitigating the risk. The degree of formality and sophistication of the banking institution's operational risk management framework should be commensurate with the overall risk profile.

The board is responsible for establishing a management structure capable of implementing the institution's operational risk management framework. Since a significant aspect of managing operational risk relates to the establishment of strong internal controls, it is particularly important that the board establishes clear lines of management responsibility, accountability and reporting. In addition, there should be separation of responsibilities and reporting lines between operational risk control

functions, business lines and support functions in order to avoid conflicts of interest. The framework should also articulate the key processes the institution needs to have in place to manage operational risk.

The board should review the framework regularly to ensure that the banking institution is managing the operational risks associated with new products, activities or systems. This review process should also aim to assess industry best practice in operational risk management appropriate for the banking institution's activities, systems and processes. If necessary, the board should ensure that the operational risk management framework is revised in light of this analysis, so that material operational risks are captured within the framework.

8.2.2 Senior Management Oversight

Senior management should have the responsibility for implementing the operational risk management framework approved by board of directors. The framework should be consistently implemented throughout the whole banking organization, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all material products, activities, processes and systems.

Management should translate the operational risk management framework established by the board of directors into specific policies, processes and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability, and ensure that the necessary resources are available to manage operational risk effectively. Moreover, senior management should assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's policy.

Senior management should ensure that activities are conducted by qualified staff with the necessary experience, technical capabilities and access to resources, and that staff responsible for monitoring and enforcing compliance with the institution's risk policy have authority independent from the units they oversee. Management should ensure that the banking institution's operational risk management policy has been clearly communicated to staff at all levels in units that incur material operational risks.

Senior management should also ensure that the banking institution's remuneration policies are consistent with its appetite for risk. Remuneration policies which reward staff that deviate from policies (e.g. by exceeding established limits) weaken the risk management processes.

Particular attention should be given to the quality of documentation controls and to transaction-handling practices. Policies, processes and procedures related to advanced technologies supporting high transactions volumes, in particular, should be well documented and disseminated to all relevant personnel.

8.3 Policies, Procedures and Limits

Senior management should transform the strategic direction given by the Board through operational risk management policy. Although the Board may delegate the management on this process, it must ensure that its requirements are being executed. The policy should include:

a) the strategy given by the Board;
b) the systems and procedures to institute effective operational risk management framework; and
c) the structure of operational risk management function and the roles and responsibilities of individuals involved.

The policy should establish a process to ensure that any new or changed activity, such as new products or systems conversions, will be evaluated for operational risk prior to going online. It should be approved by the Board and documented. The management should ensure that it is communicated and understood throughout the institution. The management also needs to place proper monitoring and control processes in order to have effective implementation of the policy. The policy should be regularly reviewed and updated, to ensure it continues to reflect the environment within which the institution operates.

Banking institutions should also establish policies for managing the risks associated with outsourcing activities. Outsourcing of activities can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialised business activities. However, a banking institution's use of third parties does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcing banking institution. Furthermore, banking institutions need to manage residual risks associated with outsourcing arrangements, including disruption of services.

For reasons that may be beyond a banking institution's control, a severe event may result in the inability of the banking institution to fulfill some or all of its obligations, particularly where its physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the banking institution, as well as broader disruptions to the financial system through channels such as the payments system. This potential requires that banking institutions establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the banking institution may be vulnerable, commensurate with the size and complexity of its operations.

Banking institutions should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. For these processes, banking

institutions should identify alternative mechanisms for resuming service in the event of an outage. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption. Where such records are backed-up at an off-site facility, or where a banking institution's operations must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimize the risk that both primary and back-up records and facilities will be unavailable simultaneously.

Banking institutions should have **disaster recovery and business continuity plans** to ensure its ability to operate as a going concern and minimize losses in the event of severe business disruption. The business disruption and contingency plans should take into account different types of scenarios to which the banking institution may be vulnerable and should be commensurate with the size and complexity of its operations. Management should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. For critical business processes, the banking institutions should:

i. identify alternative mechanisms for resuming service in the event of an outage;
ii. pay particular attention to the ability to restore electronic or physical records that are necessary for business resumption;
iii. ensure that the back-up records are at an off-site facility, and that where a banking institution's operations must be relocated to a new site, care is taken to ensure that the site is at an adequate distance from the affected operations;
iv. the business resumption and contingency plans should be reviewed periodically so that they are consistent with the banking institution's current operations and business strategies. Further, these plans should be tested periodically to ensure that they be executed in the unlikely event of a severe business disruption.

8.4 Risk Identification, Assessment, Monitoring, Control and Management Information System

8.4.1 Risk Identification and Assessment

Banking institution should identify and assess the operational risk inherent in all material products, activities, processes and systems. Furthermore, before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them should be subjected to adequate assessment procedures.

Risk identification is paramount for the subsequent development of a viable operational risk monitoring and control system. Effective risk identification considers both internal factors (such as the banking institution's structure, the nature of activities, quality of the bank's human resources, organizational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

In addition to identifying the most potentially adverse risks, banking institutions should assess their vulnerability to these risks. Effective risk assessment allows

the banking institution to better understand its risk profile and most effectively target risk management resources.

Amongst the possible tools used by banking institutions for identifying and assessing operational risk are:

- **Self- or Risk Assessment**: a banking institution assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment. **Scorecards,** for example, provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address inherent risks, as well as the controls to mitigate them. In addition, scorecards may be used to allocate economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk.

- **Risk Mapping**: in this process, various business units, organisational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action.

- **Risk Indicators**: risk indicators are statistics and/or metrics, often financial, which can provide insight into a banking institution's risk position. These indicators tend to be reviewed on a periodic basis (such as monthly or quarterly) to alert banking institutions of changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions. **Threshold/ limits** could be tied to these indicators such that when exceeded, could alert management on areas of potential problems.

- **Measurement:** Some institutions have begun to quantify their exposure to operational risk using a variety of approaches. For example, data on a banking institution's historical loss experience could provide meaningful information for assessing its exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events. Institutions may also combine internal loss data with external loss data (from other institutions), scenario analyses, and risk assessment factors.

8.4.2 Risk Monitoring and MIS

Banking institutions should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

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 event.

In addition to monitoring operational loss events, banking institutions should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, and so on. When thresholds are directly linked to these indicators, an effective monitoring process can help identify key material risks in a transparent manner and enable the banking institution to act upon these risks appropriately.

The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring should be an integrated part of a banking institution's activities. The results of these monitoring activities should be included in regular management and board reports, as should compliance reviews performed by the internal audit and risk management functions.

Senior management should receive regular reports from appropriate areas such as business units, group functions, the operational risk management office and internal audit. The operational risk reports should contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should be distributed to appropriate levels of management and to areas of the banking institution on which areas of concern may have an impact. Reports should fully reflect any identified problem areas and should motivate timely corrective action on outstanding issues. To ensure the usefulness and reliability of these risk and audit reports, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management may also use reports prepared by external sources (auditors, supervisors) to assess the usefulness and reliability of internal reports. Reports should be analysed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

In general, the board of directors should receive sufficient higher-level information to enable them to understand the overall operational risk profile and focus on the material and strategic implications for the business.

8.4.3 Risk Control/Mitigation

Banking institutions should have policies, processes and procedures to control and/or mitigate material operational risks. Banking institutions should also periodically review their risk limitation and control strategies and should adjust

their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

Control activities are designed to address the operational risks that have been identified. For all material operational risks that have been identified, the banking institution should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, the banking institution should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

Depending on the scale and nature of the activity, banking institutions should understand the potential impact on their operations and their customers of any potential deficiencies in services provided by vendors and other third-party or intra-group service providers, including both operational breakdowns and the potential business failure or default of the external parties. The board and management should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. The extent of the external party's liability and financial ability to compensate the banking institution for errors, negligence, and other operational failures should be explicitly considered as part of the risk assessment. Banking institutions should carry out an initial due diligence test and monitor the activities of third party providers, especially those lacking experience of the banking industry's regulated environment, and review this process (including re-evaluations of due diligence) on a regular basis. For critical activities, the banking institution may need to consider contingency plans, including the availability of alternative external parties and the costs and resources required to switch external parties, potentially on very short notice.

Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or programmes can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies can be used to externalise the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

However, risk mitigation tools should be viewed as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly recognise and rectify legitimate operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, or transfer the risk to another business sector or area, or even create a new risk (e.g. legal or counterparty risk).

Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, banking institutions should be aware that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by factors

beyond the banking institution's immediate control (e.g., external events). Such problems may cause serious difficulties and could jeopardise an institution's ability to conduct key business activities. Banking institutions should therefore establish disaster recovery and business continuity plans that address this risk.

8.5 Internal Control

Internal control system should be established to ensure adequacy of the risk management framework and compliance with a documented set of internal policies concerning the risk management system. Principal elements of this could include for example:

- top level reviews of the banking institution's progress towards stated objectives;
- checking for compliance with management controls;
- policies, processes and procedures concerning the review, treatment and resolutions of non-compliance issues; and
- a system of documented approvals and authorizations to ensure accountability to an appropriate level of management.

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. Both the board of directors and senior management are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of a banking institution. Controls that are an integral part of the regular activities enable quick responses to changing conditions and avoid unnecessary costs.

Operational risk can be more pronounced where banking institutions engage in new activities or develop new products (particularly where these activities or products are not consistent with its core business strategies), enter unfamiliar markets, and/or engage in businesses that are geographically distant from the head office. It is therefore incumbent upon banking institutions to ensure that special attention is paid to internal control activities including review of policies and procedures to incorporate such conditions.

Banking institutions should have in place adequate internal audit coverage to verify that operating policies and procedures have been implemented effectively. The board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the audit programme is appropriate to the risk exposures. Audit should periodically validate that the institution's operational risk management framework is being implemented effectively across the institution.

To the extent that the audit function is involved in oversight of the operational risk management framework, the board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the operational risk management process. The audit function may provide valuable input to those responsible for operational risk management, but should not itself have direct operational risk management

responsibilities. In practice, it is recognized that the audit function at some banking institutions (particularly smaller ones) may have initial responsibility for developing an operational risk management programme. Where this is the case, banking institutions should see that responsibility for day-to-day operational risk management is transferred elsewhere in a timely manner (subject to review after getting clearance as to the responsibilities of risk management).

An effective internal control system also requires that there be appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to individuals, or a team, may enable them to conceal losses, errors or inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimized, and subjected to careful independent monitoring and review.

In addition to segregation of duties, banking institutions should ensure that other internal practices are in place as appropriate to control operational risk. Examples of these include:

- Close monitoring of adherence to assigned risk limits or thresholds;
- Maintaining safeguards for access to, and use of, bank assets and records;
- Ensuring that staff have appropriate expertise and training;
- Identifying business lines or products where returns appear to be out of line with reasonable expectations (e.g., where a supposedly low risk, low margin trading activity generates high returns that could call into question whether such returns have been achieved as a result of an internal control breach); and
- Regular verification and reconciliation of transactions and accounts.

9 COMPLIANCE RISK MANAGEMENT GUIDELINES

9.1 Introduction

Compliance risk is the risk of legal or regulatory sanctions, material financial loss or damage to reputation that an institution may suffer as a result of failure to comply with laws, regulations, rules, self regulatory organization standards and codes of conduct applicable to its activities.

Compliance laws, rules and standards have various sources, including primary legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to staff members. Compliance risk, therefore, goes beyond what is legally binding and embrace broader standards of integrity and ethical conduct.

9.1.1 Compliance Risk Management

The board of directors is responsible for ensuring a banking institution's compliance with all relevant laws, rules and standards. As such, the board and senior management should allocate sufficient resources for compliance programs covering legal and compliance issues associated with the banking institution's operations. Management should establish a compliance function that is sufficiently independent from operations.

9.2 Board and Senior Management Oversight

9.2.1 Board Oversight

Effective Board oversight is the cornerstone of an effective compliance risk management process. The Board should understand the nature and level of compliance risk to which the banking institution is exposed and how its risk profile fits within the overall business strategy.

The responsibilities of the board of directors should encompass the following:

a) approving the bank's compliance policy, including a formal document establishing a permanent and effective compliance function;
b) reviewing the extent to which the bank is managing its compliance risk;
c) oversee the implementation of the compliance policy including ensuring that compliance issues are resolved effectively and expeditiously; and
d) ensuring that management takes steps necessary to identify, measure, monitor and control compliance risk.

9.2.2 Senior Management Oversight

Senior management is responsible for the effective management of a banking institution's compliance risk. As such, senior management is responsible for establishing a written compliance policy that contains the basic principles to be followed by management and staff and explains the main processes by which compliance risks are to be identified and managed at all levels of the organisation.

Senior management should, with the assistance of the compliance function:

i) identify and assess the main compliance risk issues facing the banking institution and plans to manage any shortfalls as well as the need for any additional policies or procedures to deal with new compliance risks;

ii) ensure that the banking institution's compliance risk management framework has clear lines of authority, reporting and communication;

iii) periodically report to the board of directors or a committee of the board on management of compliance risk;

iv) report promptly to the board of directors or a committee of the board on any material compliance failures (e.g. failures that may attract a significant risk of legal or regulatory sanctions, material financial loss or loss to reputation);

v) ensure that there is sufficient depth and skill in staff resources to manage legal and compliance risk;

vi) provide reasonable assurance, through the audit function, that all activities and all aspects of legal and compliance risk are covered by a banking institution's risk management process;

vii) at least once a year conduct a compliance risk assessment, and;

viii) periodically review the organisation's compliance risk management framework to ensure that it remains appropriate and sound.

9.3 Policies and Procedures

Compliance risk management policies and procedures should be clearly defined and consistent with the nature and complexity of a banking institution's activities.

The compliance policy should address the following issues with respect to the compliance function:

a) delineate responsibilities and ultimately ensure that the board and senior management are fully apprised of material compliance events;

b) its relationship with other risk management functions within the banking institution and with the internal audit function;

c) in cases where compliance responsibilities are carried out by staff in different departments, how these responsibilities are to be allocated among the departments;

d) define its right to obtain access to information necessary to carry out its responsibilities and the corresponding duty of banking institution staff to co-operate in supplying this information;

e) its right to conduct investigations of possible breaches of the compliance policy;

f) its right to be able freely to express and disclose its findings to senior management; and

g) its right of direct access to the board of directors or a committee of the board.

9.3.1 Compliance Risk Analysis

Banking institutions should use the following tools in legal and compliance risk analysis:

9.3.2 Self Assessment

This is probably the most widely used tool and emphasizes the primary responsibility which line management carries in relation to the proper management and mitigation of compliance risk. Self assessment as its name suggests, is carried out in the department giving rise to the risk. A key advantage of self assessment is that it raises compliance awareness within the business units that are undertaking it.

9.3.3 Risk Maps and Process Flows

These two tools are widely used by internal audit and they can be very useful for reviewing compliance risk. These are summary charts and diagrams that help the banking institution to identify, discuss, understand and address risks by portraying sources and types of risks and functions involved. Reviews of the risk maps and process flows by the compliance function will enable compliance risks to be identified and appropriate mitigation procedures to be implemented.

Risk maps will also assist in developing suitable procedures and mitigation measures for the risks identified.

9.3.4 Key Indicators

Senior management should develop risk indicators to assess the level of compliance risk by different business functions. The compliance indicators should reflect the nature and characteristics of each of the strategic business units. The banking institution should design a scorecard of risk metrics that will enable the compliance officer to use actual figures from the organization together with qualitative assessments. A detailed awareness of each business unit's sensitivities is necessary for the indicators to be fully useful as the degree of applicability of each indicator will vary with the sensitivity of each business unit.

9.3.5 Escalation Triggers

These are fundamental to the reporting of potential compliance problems to higher levels of management. They can provide an early warning of an increase in compliance risk or a potential breach in regulatory requirements. A set of compliance indicators that have previously been agreed with business unit management and compliance management are a necessary prerequisite of escalation triggers.

When the trigger level is reached the indicators are highlighted and reported to senior management. Escalation trigger points can be set at different levels, which may vary over time. The advantage of escalation triggers is that they allow management by exception.

9.3.6 Breach Logs and Near Miss Logs

Keeping a log of regulatory breaches and near misses can be instructive if used positively. The banking institution should learn lessons from such logs rather than merely apportion blame.

Analysis of the logs assists in the evaluation of current mitigation policies and controls and senior management can conclude on the effectiveness of the compliance risk policies. Such logs can also be useful in identifying trends and focusing resources.

9.3.7 Internal Audit Reports

Although internal audit reports contain elements of an independent self assessment, a breach log and a near miss log, they are on their own vital tools in surveying compliance risk. Additionally, internal audit will often use compliance procedures and manuals as a starting point for its own risk assessment.

There is therefore great value to the head of compliance in reviewing audit reports and extracting the relevant elements of compliance risk from those reports.

Each tool is valuable in its own right although no single tool is sufficient to provide an adequate compliance analysis. Using a number of tools together will mitigate the limitations of each one.

9.3.8 Front-line Prevention Controls

The first layer of control can be considered to be front-line prevention controls which are used by compliance officers to ensure that things go right in the first place and operate as the foundation for minimisation of regulatory risk in the institution as a whole. These commonly include:

i) Clarity of roles and responsibilities;

ii) access to accurate, timely and clear management information; and

iii) establishing processes with minimal manual interfaces and intervention.

9.4 Compliance Monitoring and Reporting

Banking institutions should ensure that they have adequate management information systems that provide management with timely reports on compliance.

The monitoring function should:

i) identify, in a structured manner, the regulatory risks to which the banking institutions is exposed;

ii) highlight instances where procedures or controls designed to minimise or eliminate regulatory risk have collapsed and resulted in a breach of the relevant laws, guidelines or regulations. Such breaches should to be investigated and any procedural or control issues resolved;

iii) work with line management and corporate staff to incorporate legal and regulatory requirements into the business quality assurance processes and management reporting;

9.4.1 Tools to Manage the Compliance Process

Compliance Programme

To control the compliance process, it is important to prepare a program or agenda. The program should show all aspects and the specific activities of the compliance function for a given period. It should schedule how, when and by whom the program shall be executed.

Education, training and communication

Effective education, training and regular communication are three essential elements of an effective compliance system. Proper education ensures that people understand the relevant topics. Training ensures that those who have to carry out compliance tasks understand how their job fits into the wider context and that they know how to perform the necessary functions.

Compliance training is needed for those whose jobs contain specific compliance tasks or responsibilities. Compliance staff should receive specific training in the type of monitoring techniques used by internal audit. They may need training in

matters such as scheduling compliance activities, effective communication, some specifics of the law and effective people and management skills. Conflict resolution will also often be useful training. Others also need compliance training to the extent appropriate to their duties.

Effective monitoring

Effective monitoring aims to check that people are doing what they ought to be doing and that the system is operating satisfactorily. An important part of monitoring is to identify the main potential danger areas and pay special attention to those areas on a regular basis. Other purposes of monitoring are to:

i) ensure that the required procedures are being followed properly;

ii) help resolve difficulties at an early stage; and

iii) serve as an early-warning device.

An effective complaint system

An effective complaints system that maintains effective records is a valuable part of compliance systems. It is an invaluable early-warning device.

Certifications

Certifications involve requiring the compliance function to approve certain processes and business activities in order to minimize compliance risk. Certifications have a number of advantages including the following:

i) draw attention to possible problem areas in a way that otherwise might not happen in a busy operating environment;

ii) can give maximum coverage and protection in areas where it is not practical to make independent checks regularly;

iii) having to issue a certificate directs minds to compliance with organizational standards and/or regulatory requirements; and

iv) if the compliance system ever has to be justified to a court, a proper system of certificates can demonstrate an intention to ensure that all areas are covered as well as possible, even if total coverage is not practicable.

9.5 Legal Risk

Legal risk is the risk that a banking institution will conduct activities or carry out transactions in which they are inadequately covered or are left exposed to potential litigation. The legal risk management framework should provide an outline of the

important issues that directors and/or executive staff of a banking institution may need to consider in ensuring due diligence in the operation of the banking institution as well as an overview of liability exposure against this risk.

As it is impossible to adequately address all aspects of liabilities that may be faced by a banking institution and the steps, which need to be taken to protect against such risks. The legal risk management framework should at a minimum provide general overview of some of the considerations that the board and senior management should be aware of in order to effectively identify and manage legal risk.

Effective legal risk management requires a proper organizational structure and reporting lines that accord legal function adequate powers to maximize coordination and the flow of legal information to all business units of the banking institution. The legal function should be managed in an integrated manner with compliance to promote efficiency and effectiveness.

9.5.1 Policies and Procedures

The board should approve the policies and procedures for managing legal risk. In general the policies and procedures should provide for the following among other considerations:

i) a framework for dealing with legal matters of varying complexity;

ii) maintenance of a central inventory of key documents such as contracts, licences, policy statements and others;

iii) regular review and assessment of legal risk in the banking institution's activities including new products;

iv) adequate documentation on all significant transactions including security administration;

v) record maintenance in line with relevant statutory requirements; and

vi) maintenance of confidentiality provisions.

10 REPUTATION RISK MANAGEMENT GUIDELINES

10.1 Introduction

Reputation 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.

Reputation risk can emerge at all business levels and has the following key components:

i) *Corporate reputation risk* which relates to a banking institution's performance, strategy, execution and delivery of its services. This is closely knotted with management's reputation risk in their ability to create shareholder value and managing capital pricing.

ii) *Operational or business reputation risk* where an activity, action, or stance taken by a banking institution, any of its affiliates or its officials will impair its image with one or more of its stakeholders resulting in loss of business, and/or disproportionate decrease in the value of a banking institution.

Reputation risk may arise from a variety of sources, namely:

- Fraud and non-compliance with statutory or regulatory requirements;

- Failing to safeguard non-public customer information through outsourcing relationships, a high volume of customer complaints, or public regulatory sanctions, and;

- Occurrences in other categories of risks which may threaten an organisation's image and stakeholder regard.

The task of managing reputation risk therefore represents a critical aspect of risk management.

Categories of Reputation Risk

Banking institutions should pay special attention to three general categories of events or circumstances which give rise to reputation risk. However, the risk methodologies employed must be broad enough to reach all risks in each category.

(i) Inherent Risk

These are risks that arise from, or are an intrinsic feature of products and services or mode of their delivery which negatively impact market and customer satisfaction. Thus, inherent risk mainly derives from challenges in operational risk, quality assurance and customer satisfaction.

(ii) Environmental Risk

This includes risks arising from the manner in which business is conducted (e.g. geographic, industrial, political, societal) which while unrelated to the quality of the products or services can negatively impact market and customer brand acceptance.

(iii) Governance and Control Risk

These risks arise from losses as a result of inadequate or failed internal processes, staff and systems. These may also include losses caused by an organization's failure to adhere to applicable laws, regulations, industry standards or practices which negatively impact the market and customer's perception of institutional integrity.

10.2 Policies and Procedures

Banking institutions are required to have policies and procedures under which they will:

i) Adopt sound risk management practices that include the practice of building reputation capital, and earning the goodwill of key stakeholders;
ii) Manage reputation risk through a process of anticipation, risk analysis and planning, and then attempting to manage both internal and external expectations;
iii) Measure trends in a banking institution's reputation as a precursor to remedial action; and
iv) Identify risk events as being either specific or systemic as this will determine the course of corrective action.

10.3 Reputation Risk Management and Monitoring

Management should exploit opportunities to grow a banking institution's reputation capital. Positive information about a banking institution should also be communicated appropriately to the market place.

Management should be fully aware of an event that has the potential to impact a banking institution's reputation. All material events should immediately be escalated to the Compliance or Risk Manager, Managing Director or Public Relations.

A banking institution should ensure that it establishes a crisis management procedure to manage potential impact of reputation events.

Banking institution should also ensure that there is no general release of information to the public, press without approval from senior management.

As mentioned earlier, reputation risk can arise from many aspects of an institution's operations. Failure to manage properly the other risks could result in loss of market share or credibility. Even where no monetary loss is incurred, there could still be reputation damage. Institutions thus have to implement a sound and comprehensive risk management process to identify, monitor, control and report all risks that may cause damage to the institution's reputation.

Senior management should establish non-financial reputation risk indicators so that appropriate action could be instituted to manage the communication of information into the market place.

10.4 Risk Methodology Components

In order to capture reputation risk, the board should adopt a risk template specifically developed to identify the structure of the control environment as well as the specific type of risk controls and metrics which will be put in place across the institution.

The banking institution should specifically design controls and metrics to address the categories of reputation risk from a qualitative perspective.

The reputation risk template should conform directly to the risk definition and should include risk tolerance levels with special emphasis on potentially high risk areas.

The banking institution should incorporate both subjective and objective risk standards in the risk template. Particular attention should be given to the horizontal aspects of "colliding" or "domino" risk. It should also incorporate "rapid escalation" policies and procedures and a "prompt remediation" policy (including procedures, delegated levels of authority etc).

10.5 Reputation Risk Analysis Methodology and Process

Every banking institution should conduct a risk diagnostic review to identify potentially reputation risk areas. The board should require that management must

use proven analysis methodologies as well as independent and objective reviews designed to bring out and analyze both quantitative and qualitative risk factors and to review critical control points within the institution.

This process should assist the banking institution to uncover the key risk factors with high likelihood to give rise to reputation risk. An institution should ensure that the analysis methodology used is highly sensitive to its particular needs and requirements as well as risk issues presented by the industry. The review process should be totally objective.

Reputation risk management should continue on an on-going basis. Every banking institution should develop a reputation data base and identify key controls and tracking reports. As part of on-going management of the risk the board should require staff awareness training at all levels of the banking institution with special training regarding potential high risk areas. Finally all aspects of reputation risk management should be subject to internal audit review.

10.6 Roles and responsibilities

The board is ultimately responsible for ensuring that an appropriate structure and process is in place to effectively manage reputation risk.

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

The Public Relations team should be responsible for applying these principles and managing the communication of information to the market so that it either builds reputation capital or minimises the impact of adverse reputation risk events. It should also be responsible for monitoring a banking institution's reputation within the market place.

Bibliography

1. Reserve Bank of Zimbabwe, Risk Management-Guideline No. 1-2006/BSD, 2006

2. Central Bank of Kenya, Risk Management Guidelines, August 2005

3. Bank of Tanzania, Risk Management Guidelines, August 2005

4. Bank of Uganda, Risk Management Guidelines, November 2002

5. Bank of Pakistan, Risk Management Guidelines for Commercial Banks & DFIs

6. Federal Reserve System, Framework for Risk Focused Supervision of Large Complex Institutions

7. Reserve Bank of Malawi, Prudential Regulations for banks and other financial institutions

8. Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, BIS publication, 2003

9. Community Bank Supervision Comptroller's Handbook, July 2003

10. Basle Committee, Basle Core Principles, October 2006

11. Basle Committee, Compliance and the Compliance Function in Banks April 2005