CENTRAL BANK OF LIBERIA

RISK MANAGEMENT GUIDELINE- BSD1/01/10

23 October, 2009

BANKING SUPERVISION DEPARTMENT

MONROVIA, LIBERIA

PREFACE

This guideline shall be cited as the Central Bank of Liberia (CBL) **Risk Management Guideline BSD1/01/10** and shall be applicable to all financial institutions as defined by the Financial Institutions Act, 1999 and is effective from 2 January 2010.

The Central Bank of Liberia has prepared this set of guidelines which provides minimum requirements for sound risk management practices. These guidelines encompass the management of credit risk, liquidity risk, interest rate risk, foreign exchange risk, operational risk, legal and compliance risk, strategic risk and reputational risks; and internet and technological risk. The adoption of international best practice should facilitate a consistent approach to risk management and financial institutions are expected to have an integrated approach to risk management that adequately identifies, measures, monitors and controls risk.

1 INTRODUCTION

1.1 The process of financial intermediation is fraught with risks and rewards that need to be balanced through judicious and prudent risk management.

1.2 Banking institutions are exposed to a variety of risks including credit, operational, liquidity strategic legal and compliance risks. The complexity of these risks has been heightened by technological advancement and financial innovation. Failure to adequately manage these risks exposes banks not only to the possibility that they may suffer losses, but, more importantly, to the possibility that they may not achieve their strategic business objectives. In the worst case, inadequate risk management may result in bank failure.

1.3 To facilitate a consistent approach to risk management and the adoption of international best practice, and implementation of risk-based supervision, the Central Bank of Liberia (CBL) has prepared this set of guidelines which provides minimum requirements for sound risk management practices.

1.4 These guidelines aim to provide financial institutions supervised by the CBL with guidance on sound risk management practices. They cover the general risk management framework for credit, market, interest rate, liquidity, operational, reputation, legal and strategic, internet and technological risk and the role of an institution's board of directors (board) and senior management.

1.5 The guidelines call attention to four cornerstones of effective risk management and sound internal controls. These are:

a) the role of the board in its oversight of risk management policies and their implementation;
b) the role of senior management in ensuring that sound policies, effective procedures and robust systems are in place;
c) the presence of sound risk management processes and operating procedures that integrate prudent risk limits with appropriate risk measurement, monitoring and reporting;

d) the presence of competent personnel in the risk management, control and audit functions.

1.6 The practices articulated in these guidelines are not intended to be exhaustive, nor do they prescribe a uniform set of risk management requirements for all institutions. The sophistication of processes, systems and internal controls for risk management is expected to vary according to the nature, size and complexity of the business activities of an institution.

1.7 Nevertheless, these guidelines have broad applicability as there is a high degree of commonality in the risk management challenges faced by financial institutions operating in an environment of global interdependencies. At the same time, institutions should also take into account relevant regulatory requirements and industry standards where applicable.

1.8 While these guidelines are organized by risk type, it is important to note that these risk types, as well as the risks arising from lapses of internal controls, are often inter-related. Different risk types can be manifested concurrently. Such a confluence of risks is particularly pronounced in stress situations and systemic events. An institution should therefore consider the potential inter-linkages of risk types in its risk management approach and manage risks in its activities on an aggregate basis.

1.9 In addition, banking institutions that are part of banking groups should adequately assess the impact on their financial condition, of risks assumed or associated with other entities in the group. Intra-group exposures complicate risk measurement in individual entities.

1.10 Under its risk-based supervisory approach, the Central Bank of Liberia exercises continuous supervision of banks' risk profiles through a combination of risk-focused on-site examinations, off-site reviews and prudential meetings. Banking institutions should establish comprehensive enterprise-wide risk management frameworks and adopt the sound practices recommended in these guidelines. These guidelines would be reviewed on a periodic basis to ensure their relevance.

2 GENERAL RISK MANAGEMENT FRAMEWORK

2.1 Introduction

a) Risk-taking is an integral part of banking business. Each banking institution has to find an appropriate balance between the level of risk it is willing to take and the level of return it desires to achieve. An effective risk management system that is commensurate with the size and complexity of its operations needs to be in place to help ensure that the risks undertaken are well managed within the banking institution's risk appetite and that it achieves the intended results.

b) For the purpose of this guideline, "risk management" refers to policies, procedures and limits which are put in place to identify, measure, monitor and control the various types of risk a banking institution is exposed to.

c) As set out in the Central Bank of Liberia's "Risk-Based Supervisory Approach", banks are generally subject to eight major types of risk - credit, market, interest rate, liquidity, operational, reputation, legal and strategic. They are expected to establish a sound and effective system to manage each of them.

d) According to Principles 8 to 13 of the Basel Committee's "Core Principles for Effective Banking Supervision", banking supervisors should be satisfied that banks have in place a comprehensive risk management process to identify measure, monitor and control credit risk (including concentration and country risks), market risk and other material risks, e.g. liquidity, interest rate, operational and reputation.

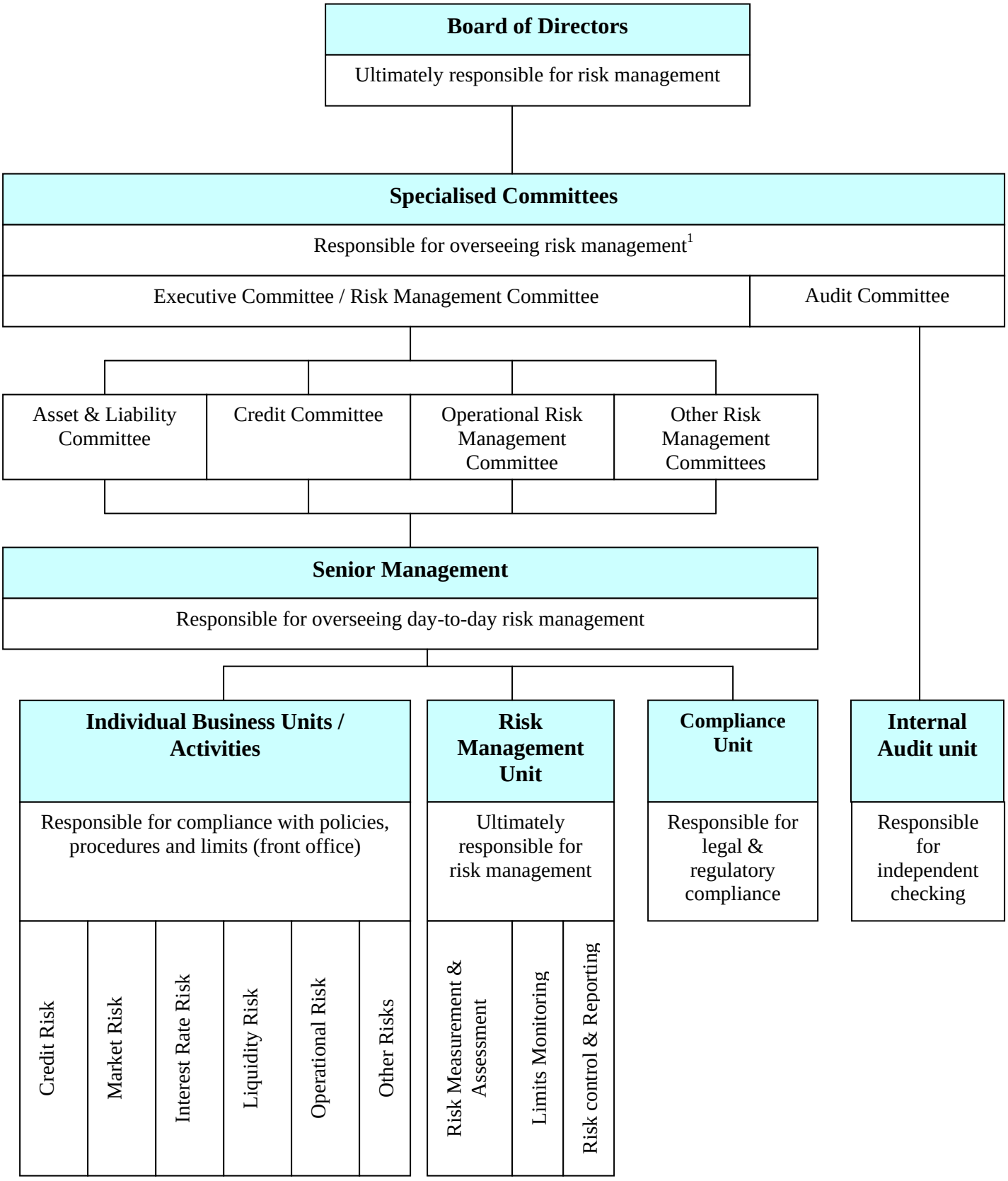
2.2 Scope and overview

a) This Guideline is intended to cover general controls relating to risk management. While risk management systems may vary among banks, the basic elements contributing to a sound risk management environment are:

i. appropriate board and senior management oversight;
ii. adequate organisational policies, procedures and limits to manage different aspects of risk arising from the business activities;
iii. adequate risk measurement, monitoring and reporting systems to support the business activities; and
iv. well-established internal controls and comprehensive audits to detect any deficiencies in the internal control environment in a timely fashion.

b) An overview of how the various elements above fit together is illustrated below. It is not intended to be prescriptive but is only indicative of a sound risk management system.

Elements of a Sound Risk Management System



c) Failure to adhere to the general requirements set out in this Guideline, taking into account the size and complexity of a bank's operations, may call into question whether the bank continues to satisfy the minimum criteria for authorization in the Financial Institutions Act and cast doubt on the fitness and propriety of its directors, chief executives and senior management.

2.3 Board and senior management oversight

2.3.1 Role of the Board

a) The ultimate responsibility for understanding the risks run by a bank and ensuring that they are properly managed lies with the board of directors. To establish an effective risk management framework, the Board should be satisfied that adequate controls and procedures are in place in respect of the following functions:

i. setting the overall tone of the bank's risk appetite and ensuring that this is well enshrined in its corporate culture;

ii. approving a firm-wide definition for different types of risk (e.g. operational risk);

iii. identifying, understanding and assessing the types of risk inherent in the bank's business activities or major new products or services to be launched; laying down the risk management strategies ;

iv. approving a risk management framework consistent with the bank's business strategies and risk appetite; determining that the risk management framework is properly implemented and maintained;

v. reviewing the risk management framework periodically to determine that it remains adequate and appropriate under the prevailing business environment;

vi. determining that there are clear reporting lines and responsibilities for the risk management function;

vii. approving the allocation of resources to business units or divisions in accordance with the bank's risk appetite;

viii. maintaining continued awareness of any changes in the bank's risk profile; and

ix. approving the provision of adequate resources (e.g. financial, technical expertise and systems technology) for risk management purposes.

b) While the Board is ultimately responsible for risk management, it may delegate authority to a specialized committee such as Credit Committee or Asset and Liability Committee. Delegation of authorities should be done on a formal basis, e.g. with a clear mandate or terms of reference. Appropriate reports should be submitted regularly to the board by the designated committee to which such authority has been delegated.

c) While the responsibilities may be delegated, the board members are expected to have an adequate understanding of the risks and the framework including the major controls (e.g. limits) used to manage the risks for various activities. If the board members lack the relevant expertise, bringing in new board members with such knowledge or appointing external consultants should be considered.

2.2.2 Role of the senior management

a) Senior management should be responsible for developing detailed policies, procedures and limits for managing different aspects of risk arising from the bank's business activities, based on the risk management strategies laid down by the Board.

b) Senior management should also have the responsibility for designing and implementing the risk management framework approved by the board. The framework should be implemented throughout the whole institution and all levels of staff should understand their responsibilities with respect to risk management.

2.4 Policies, procedures and limits

a) Banking institutions should have clearly defined policies and procedures for risk management. These documents should be approved by the board or its designated committee.

b) The policies and procedures should cover all material risks associated with a bank's business. They should be prepared on a firm-wide or group-wide basis. Accountability should be spelt out clearly and lines of authority for each business activity and product area should be clearly defined.

c) The development of the risk management policies and procedures should take account of the following factors:

   i. a bank's overall business strategy and activities; appropriateness to the size, nature and complexity of the bank's business;
   ii. risk tolerance level of the bank;
   iii. sophistication of the bank's risk monitoring capability, risk management systems and processes;
   iv. past experience and performance;
   v. management expertise; and
   vi. any legal and regulatory requirements.

d) The risk management policies and procedures should keep pace with the changing environment. The board or its designated committee should review these documents on a regular basis (e.g. at least annually). If the review is carried out by the committee or senior management, any material amendment to the policies and procedures should be submitted to the board for adoption and formal ratification.

e) Where appropriate, the risk management policies and procedures should also cover the use of risk mitigation techniques (e.g. hedging, buying insurance protection or using credit derivatives).

2.4.1 Risk limits

a) A set of limits should be put in place to control a bank's exposure to various quantifiable risks associated with its business, e.g. credit risk, market risk, interest rate risk and liquidity risk. These limits should be documented and approved by the board or its designated committee.

b) Risk limits should be set in line with a bank's risk appetite. To ensure consistency between risk limits and business strategies, the board may wish to approve limits as part of the overall annual budget process.

c) Risk limits should be suitable to the size and complexity of a bank's business and compatible with the sophistication of its products or services. Excessively high limits may fail to trigger prompt management actions while overly restrictive limits that are frequently exceeded may undermine the purpose of the limit structure.

d) Risk limits may be set at various levels, e.g. individuals, business units, the firm or the group as a whole. Banks should have a clearly documented methodology for allocating the overall risk limits across their business units.

e) The Board or its designated committee should ensure that limits are subject to regular review and are reassessed in the light of changes in market conditions or business strategy.

f) Risk limits should be clearly communicated to the business units and understood by the relevant staff.

g) Limit utilisation should be closely monitored. Any excesses or exceptions should be reported promptly to the senior management for necessary actions.

2.5 New products and services

a) Services and activities that are new to a bank should be subject to a careful evaluation or pre-implementation review to ensure that the board or its designated committee and management fully understand the risk characteristics and that there are adequate staffing, technology and financial resources to launch the product or service.

b) Proposals to introduce new products or services should generally include:
   i. a description of the product or service;
   ii. a detailed risk assessment;

iii. a cost and benefit analysis;

iv. consideration of the related risk management implications and identification of the resources required to ensure effective risk management of the new product or service (e.g. system enhancement);

v. an analysis of the proposed scale of new activities in relation to the bank's overall financial condition and capital strength; and

vi. the procedures to be used for measuring, monitoring and controlling the risks.

c) All the relevant departments e.g. risk control, accounting, operations, legal and compliance should be consulted as appropriate, before a new product or service is launched. New products or services which could have a significant impact on a bank's risk profile should be brought to the attention of the board or its designated committee.

d) Banking institutions should perform a post launch evaluation of new products, the results of which should be taken into account for the development of any similar products or services in the future.

2.6 Risk measurement, monitoring and reporting

2.6.1 Risk management function

a) To carry out the day-to-day risk management function, a dedicated risk management unit is should be established by banks.

b) An effective risk management function should:

i. have clearly defined responsibilities;

ii. have a direct reporting line to the relevant risk management committee or senior management;

iii. be independent from the business units that generate risks;

iv. be supported by an effective management information system; and be given adequate resources to perform its duties and staffed by persons with the relevant expertise and knowledge.

c) The responsibilities of the risk management unit include:

i. to ensure that the risks are well understood and adequately assessed before a transaction is entered into;

ii. to ensure that the established policies and control procedures in respect of risk management are implemented and complied with;

iii. to monitor the use of risk limits and ensure that quantifiable risks are within the approved limits structure. This will include ensuring that the risk exposures of individual business units in respect of various risks are properly aggregated and monitored against the aggregate limits for the institution as a whole; and

iv. to ensure that the risks are properly measured and promptly reported to the relevant risk management committee or senior management.

2.6.2 Risk management information system

a) Banking institutions should establish and maintain a management information system which can effectively measure and report on the risks of major functions, products or business activities.

b) An effective risk management information system should produce timely, accurate and reliable reports to the board, senior management and line managers to support decision making at the different levels.

c) The level of sophistication of the system depends on the nature, scale and complexity of a banking institution's business and the products involved. Generally, it should be capable of: measuring the risk of a product or an activity in accordance with the measurement methods or models adopted;

i. aggregating data on a product, functional, geographical and group basis;

ii. conducting variance analysis against annual budget or targets;

iii. alerting the management, e.g. when a risk exposure approaches a pre-set limit;

iv. reporting excesses and exceptions;

v. facilitating the allocation of capital charges to the business products and activities according to the level of risk-taking;
vi. calculating risk-adjusted performance; and
vii. conducting sensitivity analysis and stress-testing

d) To remain effective, the system should be subject to regular upgrades and modification.

2.6.3 Risk measurement methods

a) Banking institutions should have in place effective systems for the measurement of the various types of quantifiable risk and for the assessment of other risks which are not easily quantifiable.

b) Different methods or models may be used to assess or measure each type of risk. For example, a number of value-at-risk approaches such as historical simulation, variance/co-variance method or Monte Carlo simulation can be used to estimate the exposure of a bank to various types of market risk. The bank may also choose to use a risk mapping process, key risk indicators or scorecards as a means of assessing its operational risk. Detailed principles on the measurement of individual risks are discussed under the respective risk modules in this Guideline.

c) In determining the methods or models to be adopted for risk measurement, a bank should consider the following factors:
i. nature, scale and complexity of its business activities;
ii. the business need (e.g. for pricing);
iii. assumptions of the methods or models;
iv. data availability;
v. the sophistication of its management information system; and
vi. staff expertise.

d) The board or its designated committee and senior management should understand the underlying assumptions used and constraints of the methods or models chosen. They

should also satisfy themselves as to the adequacy and appropriateness of the key assumptions, data sources and procedures used to measure the risks.

e) The accuracy and reliability of a risk measurement method or model should be verified against the actual results through regular back-testing. The measurement method or model should also be subject to periodic updates to reflect changing market conditions.

2.6.4 Risk-adjusted performance measurement

a) To effectively measure the performance of business units or activities, the trend is for a risk-adjusted performance measurement to be used. Banking institutions may wish to introduce such a system to enable them to compare the financial performance of individual business units, taking into account the risks associated with their activities. This ensures that business units are not rewarded for taking on excessive risks.

b) To enable efficient allocation of capital and other financial resources to individual business units, the system used should be able to comprehensively measure the risks associated with the business activities. Management information systems should be able to attribute risk and earnings to their appropriate sources and to measure earnings against capital allocated to the activity, after adjusting for various risks (such as the expected loss on credit facilities).

2.7 Sensitivity analysis and stress-testing

a) Banking institutions should have the capability to measure the sensitivity of earnings to the change in individual risk factors (e.g. interest rates).

b) Banking institutions should also have in place a system to conduct stress tests or scenario analysis regularly on major business or functional areas so as to assess the potential impact under unusual market conditions. The results of the sensitivity

analysis and stress-testing should be reviewed regularly by the board and senior management and should be reflected in the policies and limits.

2.8 Internal Controls and Audit

2.8.1 Internal control system

a) A critical element to support an effective risk management system is the existence of a sound internal control system and a properly structured internal control system should:

i. help to promote effective and efficient operation;
ii. provide reliable financial information;
iii. safeguard assets;
iv. minimise the operating risk of loss from irregularities, fraud and error;
v. ensure effective risk management systems; and
vi. ensure compliance with relevant laws, regulations and internal policies.

b) A banking institution's internal control system should cover the following:

i. high level controls, including clear delegation of authority, written policies and procedures, separation of critical functions (e.g. marketing, risk management, accounting, settlement, audit and compliance);
ii. controls relating to major functional areas, including, retail banking, corporate banking, institutional banking, private banking and treasury. Such controls should include segregation of duties, authorization and approval, limit monitoring, physical access controls, etc.;
iii. controls relating to financial accounting (e.g. reconciliation of nostro accounts and review of suspense accounts), annual budgeting, management reporting and compilation of prudential returns to the regulators;
iv. controls relating to information technology;
v. controls relating to compliance with statutory and regulatory requirements; and
vi. controls relating to the prevention of money laundering.

c) An effective internal control system requires a strong control environment to which the board and senior management provide their full support, and an audit function to evaluate its performance on a regular basis.

2.8.2 Internal Audit

a) Banking institutions' internal audit function should, among other things, perform periodic checking on whether the risk management system approved by the board is properly implemented and the established policies and control procedures in respect of risk management are complied with.

b) 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.

c) To carry out their function effectively, internal auditors should: have unfettered power to choose which departments or business products or activities to be audited and to access records and documents;

d) Have appropriate independence and status within the banking institution to ensure that senior management reacts to and acts upon their recommendations;

e) Have sufficient resources and staff that are suitably trained and have relevant expertise and experience to understand the risk management process and the measurement models or methods employed; and

f) Employ a methodology that identifies the key risks run by the banking institution and allocates its resources accordingly.

2.8.3 Compliance Function

a) The compliance function plays an important role with respect to a sound risk management system. The role of the compliance function, among other things, is to ensure that the risk management system or process adopted is in compliance with the relevant statutory provisions and regulatory requirements.

b) Banking institutions with a significant scale of operation are expected to have a separate, independent compliance function. For smaller banks, other arrangements (such as hiring an external lawyer to provide legal advice on a need basis or an appropriate allocation of duties among departments) may be acceptable.

c) The organisation and responsibilities of the compliance function should be properly documented. An effective compliance function should be staffed by an appropriate number of competent staff who are sufficiently independent of the business units and have a direct reporting line to a designated committee or senior management.

2.8.4 Business Continuity Planning

a) Each banking institution should have in place contingency and business continuity plans, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption.
b) These plans should be regularly updated and tested to ensure their effectiveness.

3 CREDIT RISK

3.1 Introduction

a) This section provides guidance on sound practices in credit risk management. It also articulates broad principles that should be embedded in a risk management framework covering strategy, organisational structure, policy, as well as a credit control processes for origination, monitoring and administration of credit transactions and portfolio. The guidelines are applicable to both the banking and trading books.

b) Credit risk is the risk that a borrower or counterparty will fail to meet obligations in accordance with agreed terms. Credit risk could stem from both on- and off-balance sheet transactions. An institution is also exposed to credit risk from diverse financial instruments such as trade finance products and acceptances, foreign exchange, financial futures, swaps, bonds, options, commitments and guarantees. Thus, sources of credit risk exist throughout the activities of a bank both in the banking book as well as in the trading book.

c) Credit risk often does not occur in isolation. A risk event may engender both market and credit risks. An institution should therefore, adopt a holistic approach to assessing credit risk and ensure that credit risk management is part of an integrated approach to the management of all financial risks. Every institution should have comprehensive credit risk management systems appropriate to its type, scope, sophistication and scale of operations. These systems should enable the institution to identify, quantify, monitor and control credit risk and ensure that adequate capital resources are available to cover the risk assumed.

d) The effective management of credit risk is a critical component of a comprehensive approach to risk management underpinned by effective board and senior management oversight, well-defined policies and procedures, strong MIS and adequate internal control systems.

3.2 Board and Senior Management Oversight

3.2.1 Board of Directors

a) The board of directors should be ultimately responsible for providing overall strategic direction to the institution through approving and reviewing the credit risk strategy and credit risk polices.

b) A credit risk strategy should clearly set the acceptable risk appetite and tolerance of the institution. The credit risk strategy should adequately cover all the activities of the institution in which credit exposure is a significant risk. It should encompass the need to maintain sound credit quality, diversification, profits and business growth and allow for economic cycles and their effects on the credit portfolio during different stages of an economic cycle.

c) Reviews of the credit risk strategy and policies should be done at least annually in line with international best practices and any changes and concerns should be effectively communicated to all relevant staff

d) The board should ensure that:

i. the credit risk strategy has a statement on acceptable levels of exposure to the various economic sectors, currencies and maturities. It should also include the target markets and overall characteristics that the institution would want to achieve in its credit portfolio (including levels of diversification and concentration tolerances);

ii. the credit risk strategy and credit risk policies are reviewed, approved and effectively communicated throughout the institution;

iii. the credit risk strategy of the institution provides for continuity and proves viable in the long-run as well as take cognisance of cyclically (upturns and

downturns in economic cycles) which results in shift in the composition and quality of the overall credit portfolio;

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

v. the financial institution's remuneration policies do not contradict the credit risk strategy;

vi. the institution's capital level is adequate for the credit risks assumed;

vii. senior management team is fully capable of managing the credit risk activities conducted by the institution and that such activities are done within the risk strategy, policies and procedures approved by the board;

viii. there is an internal audit function capable of assessing compliance with the credit policies and management of the entire credit portfolio;

ix. the delegation of authority and approval levels are clearly defined; and

x. management provides periodic reports on insider loans, provisioning and write-offs on credit loan losses and audit findings on the credit granting and monitoring processes.

3.2.2 Senior Management

a) It is the responsibility of senior management to implement the credit risk strategy and credit risk policies approved by the board of directors and develop procedures that include identifying, measuring, monitoring and controlling credit risk.

b) Senior management should ensure that:

i. the credit granting activities conform to the laid down procedures;

ii. written policies and procedures are developed, implemented and responsibilities of the various functions are clearly defined;

iii. the credit policies are implemented on a consolidated basis and at the individual institution or affiliate level, communicated throughout the institution and its affiliate, monitored and reviewed periodically to address any changes;

iv. compliance with internal exposure limits, prudential limits and regulatory requirements is enforced; and

v. internal audit reviews of the credit risk management system and credit portfolio are undertaken regularly.

3.2.3 Risk Management Structure

a) An institution should adopt a risk management structure that is commensurate with the size and the nature of its activities. The organisational structure should facilitate effective management oversight and execution of credit risk management and control processes.

b) A senior management committee should be formed to establish and oversee the credit risk management framework. The framework should cover areas such as recommendation of business and credit risk strategy and credit risk policy to the board, review of the credit portfolio and profile, delegation of credit approving authority within board approved limits and evaluation of the credit processes. This committee should comprise of senior management from the business line and control functions.

c) An institution should also establish risk management and control functions independent of the credit originating function. Such functions include policy formulation, limit setting, exposure and exception monitoring and reporting, custody and monitoring of documentation, and input of credit limits. Staff performing sensitive functions such as custody of key documents, funds transfer and limit inputs should report to managers who are independent of business origination and the credit approving process.

d) There should be adequate measures to address potential conflicts of interest where individuals performing the loan origination function are also involved in credit reviews and analyses. While there may be separate departments responsible for credit origination and credit risk control, the credit origination department should also be mindful of credit risk in its pursuit of business opportunities.

3.3 Policies, Procedures and Limits

a) The Board should approve credit policies, including concentration limits and lending to related parties. It should also be the approving authority for changes and exceptions to such policies. Senior management should set out operational processes and procedures to implement the credit policies.

b) Credit policies should set out the conditions and guidelines for the granting, maintenance, monitoring and management of credit, at both the individual transaction and portfolio levels. Such policies should be documented, well-defined, consistent with prudent practices and regulatory requirements, and adequate for the nature and complexity of the institution's activities.

c) Every institution should be very clear about its credit risk tolerance, including the nature and level of risk it is prepared to undertake. Risk tolerance should be compatible with the institution's strategic objectives.

3.3.1 Credit granting

a) Every institution should have a clearly established process for approving credit facilities. This includes amending, renewing and refinancing of existing credit facilities.

b) At a minimum, the (credit) policy should document the following:

i. roles and responsibilities of business units and staff involved in the granting, administration and monitoring of credit facilities;
ii. delegation of credit authority to various levels of management and staff (including authority to approve deviations and exceptions);
iii. credit risk acceptance criteria;
iv. general terms and conditions of the facility structure, such as pricing, tenure and limit;
v. acceptable types of collateral and security documents;
vi. standards for credit review and monitoring; and
vii. guidelines on management of concentration risk and stress testing.

c) Credit approvals should be made in accordance with the institution's written guidelines and granted by the appropriate level of management. There should be an audit trail documenting the approval process and identifying the individuals and committees providing input and making the credit decision.

d) Credit analysis requires that management should have a clear understanding of the borrower or counter-party and obtain adequate information to enable a comprehensive assessment of the risk profile of the customer. This will include the purpose of the loan, repayment sources, financial statements, integrity and reputation of the borrower or counter-party. The policies should articulate the principle of Know Your Customer even for existing clients.

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

f) In addition, institutions should establish checks and balances that ensure all credit facilities are granted at arms' length in all respects. Extension of credit to directors, senior management and other influential parties, for example, shareholders should not override the established credit granting and monitoring processes of the financial institution.

3.3.2 Credit limits

a) An institution should have sound and well-defined policies and procedures incorporating credit concentrations, limits and level of credit risk a financial institution is willing to assume. These limits should ensure that credit activities are adequately diversified. Institutions are expected to develop their own limit structure while remaining within the exposure limits set by the Financial Institutions Act.

b) The policy on large exposures should be well documented to enable financial institutions to take adequate measures to ensure that concentration risk is limited. The

policy should stipulate the percentage of the institution's capital that can be lent to any individual or related entities in compliance with the applicable regulation.

c) The credit policy should provide for close monitoring and reporting of lending and writing-off of loans to related parties. Credit transactions with related parties should be subject to the approval of the board (excluding board members with potential conflicts of interest). Such transactions should also be disclosed to the public as part of the institution's financial reporting programme.

d) The main exposure limits covered under the policies should include the following:
   i. acceptable exposure to individual borrowers;
   ii. maximum exposure to connected groups and insider dealings;
   iii. the overall limit on the credit portfolio in relation to capital, assets or liabilities;
   iv. maximum exposure to individual economic sectors (e.g. commercial, consumer, real estate, agricultural); and
   v. acceptable limits on specific products.

e) Credit risk limits should, among others factors, take account of the institution's:
   i. historical loss experience;
   ii. capital adequacy;
   iii. desired level of return; and
   iv. diversification objectives.

f) The institution should consider the results of stress tests in its overall limit setting and monitoring. Limits should be based on the interrelationship of risk and reward and may be stated in absolute terms e.g. an established ceiling for each loan category, or expressed in relative proportions, such as a percentage of capital, total loans or total assets, or a combination of these.

g) Credit limits should be reviewed on a periodic basis to take into account changes in the counterparty's credit strength and environmental conditions. All requests to increase credit limits should be substantiated.

3.3.3 Credit products

a) Every institution should maintain adequate documentation relating to various types of loan products and credit instruments. The products should also have a maturity profile and the pricing of these products should be included and reviewed periodically.

b) Prior approval for all new products should be obtained from the board as well as clearance from independent control functions such as audit and risk management. All material risks arising from new products should be assessed before introduction to the customers.

3.3.4 Credit risk mitigation

a) In controlling credit risk, an institution can use a variety of mitigating techniques which include collateral, guarantees and netting off of loans against pledged deposits of the same counter-party. While the use of these techniques will reduce or transfer credit risk, other risks may arise which include legal, operational, liquidity and market risks. Therefore, an institution should have comprehensive procedures and processes to control these risks and have them well documented in the policies.

b) Security held by an institution to mitigate against credit risk should satisfy the following conditions:

i. There must be legal certainty. All documentation used for collateralised lending must be binding to all parties and be legally enforceable;

ii. the legal environment must provide for right of liquidation or right of possession in a timely manner in the event of default;

iii. necessary steps must be taken for obtaining and maintaining an enforceable security, for example registration, right of set-off or transfer of title must meet all the legal requirements;

iv. procedures for timely liquidation of collateral should be in place;

v. on-going valuations of the collateral should be undertaken to confirm that it remains realizable; and

vi. guidance on the various acceptable forms of collateral should be documented.

c) The institution should primarily assess the borrowers' capacity to repay and should not use collateral to compensate for insufficient information.

3.3.5 Management of problem credits

a) An institution's credit policy should establish the procedures for dealing with problem credits. Early recognition of weaknesses in the credit portfolio is important and allows for effective determination of loan loss potential.

b) An institution must have clearly articulated and documented policies in respect of past due credit facilities, and should at a minimum have approval levels and reporting requirements in respect of granting extensions, deferrals, renewals and additional credits to existing accounts.

c) The policy should define a follow-up procedure for all loans and identify the reports to be submitted both to management and board of directors.

3.3.6 Provisioning policy

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

3.4 Credit Risk Measurement and Monitoring

3.4.1 Measuring credit risk

a) Every institution should have procedures for measuring and monitoring actual exposures against established limits including exposures to related parties, products, customers, market segments and industries for appropriate risk management decisions to be made.

b) A financial institution must have comprehensive internal systems and models that effectively measure credit risk.

c) An institution should have robust MIS capable of providing timely, accurate and detailed reports to the board and senior management.

d) Credit risk measurement tools and techniques should take into account the nature of the credit, maturity, exposure profile, existence of collateral or guarantees and potential for default and environmental circumstances.

3.4.2 Monitoring Credit Risk

a) Every institution should have an internal risk rating system that comprises methods, processes, controls, data collection and IT systems that support the quantification of default and loss estimates.

b) An effective monitoring system should ensure that the institution:

i. understands the current financial condition of the borrower;
ii. monitors compliance with the existing terms and conditions;
iii. assesses collateral in relation to the borrowers current condition; and
iv. identifies non-performing accounts and enforces proper classification and loan loss provisioning.

c) The institution should undertake a detailed credit portfolio review which covers the following:

i. loans to borrowers with aggregate exposure larger than 10 percent of the institution's capital;
ii. loans to shareholders and connected parties;
iii. loans for which interest or repayment terms have been restructured since the granting of the loan;
iv. loans for which cash payment of interest and / or principal is more than 30, 60, 90 and 180 days past due, including those for which interest has been capitalized or suspended; and
v. loans classified as substandard, doubtful or loss.

d) The frequency of credit portfolio review should reflect the level of credit risk.

e) The specific objective of these reviews is to assess the likelihood that the credit will be repaid and the classification of the loan is adequate. When the amount exceeds 10% of a bank's capital, the analysis should also consider the borrower's business plans for the future and the potential consequences for debt service capacity and principal repayment.

3.4.3 Credit administration

a) Every institution should have a system for the on-going administration of its various portfolios containing credit risks.

b) Management should set-up a credit administration team to ensure that credit portfolios are properly maintained and administered. This will include record keeping, preparation of the terms and conditions as well as perfection and safe custody of the securities. Credit files should at a minimum contain the following information:
i. credit application;
ii. evidence of approval;
iii. latest financial information;
iv. record and date of all credit reviews;
v. record of all guarantees and securities;
vi. record of terms and conditions of facility;

vii. evidence of securities validation function that should include, legal validity, existence, valuation, registration of charge and safekeeping; and

viii. internal rating.

c) Institutions should develop controls to ensure compliance with the applicable laws and regulations and internal policy. Adequate segregation of duties between approval and administration process should be maintained.

3.4.4 Stress testing of the Credit Portfolio

a) A financial institution should stress test its credit portfolio. This involves identification of possible events or future changes that could have a negative impact on the institution's credit portfolio and the institution's ability to withstand the changes.

b) Institutions should subject their credit portfolios to changes relating to:

i. economic or industry developments;

ii. market – risk events; and

iii. liquidity conditions.

c) Examples of stress testing parameters include the following:

i **Increases in non-performing loans and provisioning levels:** This type of shock is used to assess the impact of such increases on profitability and capital adequacy. In estimating the additional provisions resulting from the applied shocks, financial institutions may use their internal systems and/or the provisioning levels prescribed in the Financial Institutions Act.

ii. **Failure of major counterparties**: This shock is used to estimate the impact of failure of a banking institution's major counterparties, including corporate and inter-bank counterparties, on its ***profitability*** and ***capital adequacy***. The test can be extended to cover aggregate exposures to major industries, market sectors, countries and regions (e.g. by assuming that a significant number of defaults occur within such aggregate

exposures). This could also refer to assessing the impact of a certain number of the top borrowers defaulting (e.g. default of the top three borrowers);

iii. **Economic downturn:** This shock is used to assess the impact of adverse changes in selected macroeconomic variables (e.g. GDP growth, unemployment rate etc.) on a institution's asset quality, profitability and capital adequacy; and

iv. **Decline in the real estate market**: This shock is used to assess the impact of decline in property prices on collateral coverage, default risk and provisioning needs for loans secured by properties. In the case of a residential mortgage portfolio, institutions can assess the impact of resultant increase in loans in negative equity and specific provisions (based on assumptions of the probability of default for such loans).

d) An institution must be in a position to analyze the various situations in the economy or certain sectors to determine the event that could lead to substantial losses or liquidity problem.

e) Whatever methods are used for stress testing, the output of these should be reviewed periodically and appropriate action taken by senior management in cases where results exceed agreed tolerance.

3.4.5 Credit exposure and risk reporting

a) Credit risk information should be provided to board and senior management with sufficient frequency and should be reliable with appropriate desegregation.

b) Reports should be generated on the on-balance sheet and off-balance sheet credit activities. The reports should show credit exposures:

   i. by business line such as commercial, industrial sector, real estate, construction, credit cards, mortgage and leasing;

   ii. relating to the composition of on and off balance sheet credits by major types of counterparties, including government, foreign corporate, domestic corporate, consumer and other financial institutions;

iii. in relation to significant individual borrowers or counterparties, related borrowers or group of borrowers;

iv. by major asset category showing impaired and past due amounts relating to each category; and

v. restructured during a certain period and credits which special conditions have been granted.

3.4.6 Internal controls and audit

a) Financial institutions should have an independent internal system for assessment of the credit risk management process in order to assist the board to determine the effectiveness of the risk management process.

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

c) Internal audit reviews should assess compliance with the institution's credit policies and procedures. This will require confirming the following:

i. the credit granting function is carried out effectively;

ii. the credit exposures are within the prudential and internal limits set by the board of directors;

iii. validation of significant change in the risk management process;

iv. verification of the consistency, timeliness and reliability of data used for internal risk rating system;

v. adherence to internal risk rating system;

vi. identification of areas of weaknesses in the credit risk management process; and

vii. exceptions to the policies, procedures and limits.

d) Internal audit reviews should be conducted on a periodically and ideally not less than once a year. The audits should also identify weaknesses in the credit risk management process and any deficiencies with the policies and procedures.

e) Institutions should establish internal control practices which ensure that deviations from policies, procedures, limits and prudential guidelines are promptly reported to the appropriate level of management.

4 LIQUIDITY RISK

4.1 Introduction

a) Liquidity risk is the risk of financial loss to an institution arising from its inability to fund increases in assets and /or meet obligations as they fall due without incurring unacceptable cost or losses.

b) Liquidity risk is inherent in banking institutions activities. Financial institutions' balance sheets are such that long-term assets are funded by short-term liabilities such as demand and short-term and time deposits.

c) Liquidity risk and other inherent risks such as credit, market, interest rate, operational, reputation and strategic faced by institutions are not mutually exclusive and should not be considered in isolation. Any real or perceived problems associated with an institution in relation to these risks may affect the institution from accessing funds at a reasonable cost and thus increase its liquidity risk.

d) Liquidity problems can have an adverse impact on a bank's earnings and capital and, in extreme circumstances, may even lead to the collapse of a bank which is otherwise solvent. A liquidity crisis besetting individual banks that play an active or major role in financial activities may have systemic consequences for other financial institutions and the banking system as a whole. It could also affect the proper functioning of payment systems and other financial markets. Sound liquidity risk management is therefore pivotal to the viability of every bank and the maintenance of overall banking stability.

e) The CBL recognises that the degree of sophistication of a banking institution's liquidity risk management systems and controls will depend on the nature, scale and complexity of its operations as well as the level of liquidity risk assumed. The focus of this Guideline is therefore on an institution's ability to apply the principles and guidance laid down to developing systems and controls that are appropriate to its particular circumstances.

f) The CBL adopts a risk-based supervisory approach that includes continuous supervision of banks' liquidity risk through a combination of risk-focused on-site examinations, off-site reviews and prudential meetings. The objectives are to obtain sufficient and timely information for evaluation of banks' liquidity risk profile and to assess the adequacy and effectiveness of their liquidity risk management process.

4.2 Sources of liquidity risk

a) Liquidity risk arises from both sides of a banking institution's balance sheet and from off-balance sheet transactions.
b) Managing liquidity risk involves understanding the characteristics and risks of different sources of liquidity, determining the appropriate funding strategies (including the mix of funding sources) to meet liquidity needs and deploying the strategies in a cost-effective manner.

Asset liquidity …

c) The asset portfolio of a banking institution provides liquidity through the maturity of an asset, sale of an asset and the use of an asset as collateral for borrowing or repurchase agreements (repos).
d) A banking institution should maintain a portfolio of liquid assets (e.g. money market placements and marketable securities) to supplement its funding sources.
e) A banking institution is exposed to liquidity risk where inflows from the realization of assets (either upon maturity or at the time of sale) are less than anticipated because of default risk or price volatility.
f) In addition, significant concentrations within the asset portfolio (e.g. in relation to the distribution of exposures by counterparty, instrument type, geographical location or economic sector) increase the level of liquidity risk.
g) In managing asset liquidity, a banking institution should establish a clear strategy for holding liquid assets, develop procedures for assessing the value, marketability and liquidity of the asset holdings under different market conditions, and determine the appropriate volume and mix of such holdings to avoid potential concentrations.

Liability liquidity …

h) Every banking institution should employ liability funding strategies which are appropriate to the nature and scale of the banking institutions' activities, including the proper mix of liabilities to avoid potential concentrations.
i) In managing liability liquidity, a banking institution should be able to distinguish the behavior and characteristics of different funding sources and monitor their trends separately.
j) Every banking institution should pay particular attention to the impact of changing market conditions on its funding structure.

Off-balance sheet items...

k) Off-balance sheet items, depending on the nature of transactions, can either supply or use liquidity. Examples include standby or committed facilities given by other

financial institutions and loan commitments given by banking institutions to their customers.

l) Banking institutions should ensure that they have the ability to assess how their involvement in off-balance sheet activities would affect cash flows and liquidity risk.

4.3 Framework for Managing Liquidity Risk

a) The framework for managing liquidity risk is anchored on an effective board and senior management oversight, formulation of a liquidity strategy, adequate policies and procedures, effective internal controls and independent reviews, as well as a sound process for identifying, measuring, monitoring and controlling liquidity risk.

b) The liquidity strategy should set out the financial institutions' general approach to liquidity management, including various quantitative and qualitative targets.

c) The strategy should be communicated throughout the banking institution and all relevant business units should operate under the approved policies, procedures and limits.

4.3.1 Board and Senior Management Oversight

a) Effective board of directors and senior management oversight is a critical element of an institution's liquidity risk management process. Sound liquidity risk management requires an informed board, capable management and appropriate staffing.

Board of Directors

b) The board of directors should have ultimate responsibility for liquidity risk management and establish the level of tolerance for liquidity risk.

Board of Directors…

c) The board of directors' responsibilities in relation to liquidity risk management should include:

i. approving significant policies and strategies that govern or influence the institution's liquidity risk and ensure that senior management translates them into clear guidance and operating standards;

ii. establishing an appropriate structure for the management of liquidity risk and identifying lines of authority and responsibility for managing liquidity risk exposures;

iii. approving reviews of the liquidity risk management strategy and policies;

iv. monitoring the institution's overall current and prospective liquidity risk profile on a regular basis;

v. taking steps to ensure that liquidity risk is adequately identified, measured, monitored and controlled;

vi. reviewing adequacy of the contingency plans of the institution;

vii. ensuring that senior management and appropriate personnel have the necessary expertise and systems to measure and monitor all sources of liquidity; and

viii. reviewing regular reports on the liquidity position of the institution.

Senior Management

d) Senior management is responsible for developing and implementing a liquidity risk management strategy in accordance with the institution's risk tolerance and one appropriate for the nature, scale and complexity of the institution's activities.

e) The responsibility for managing the overall liquidity of the institution should be placed with a specific, identified group within the institution. This might be in form of an Asset and Liability Management Committee (ALCO), comprising senior management from key functional areas.

f) The Committee should ensure that the liquidity strategy approved by the board can be effectively implemented, establish a schedule of liquidity reviews with appropriate frequency and depth.

Asset and Liability Management Committee

g) The board of directors may delegate the responsibility for managing the overall liquidity of an institution to the Asset Liability Management Committee.

h) ALCO meetings should be held at least monthly.

i) The effective management of assets and liabilities should, at a minimum, incorporate the following activities:

i. assessing current balance sheet position;
ii. reviewing previous results;
iii. projecting exogenous factors such as economic outlook, performance of counterparties;
iv. developing asset and liability strategies;
v. simulating the strategies;
vi. determining the most appropriate strategies;
vii. setting measurable targets;
viii. communicating the targets to appropriate managers and staff; and
ix. monitoring actions regularly and reviewing performance.

4.4 Liquidity Strategy, Policies, Procedures and Limits

Every banking institution should have documented liquidity strategy, policies, procedures and limits approved by the board of directors.

4.4.1 Liquidity Strategy

The liquidity strategy should set out the general approach to liquidity management (including goals and objectives) and specific aspects of liquidity risk management, such as:

i. Specific policies on liquidity;
ii. Approach to managing liquidity across borders and across business lines and legal entities;
iii. Approach to intraday liquidity management;
iv. The assumptions on the liquidity and marketability of assets;
v. Liquidity needs under normal conditions as well as liquidity implications under periods of liquidity stress;

The strategy should also define the institution's liquidity approach to meeting potential funding needs in the short and long-term.

4.4.2 Liquidity Policies

a) Every institution should have a set of liquidity policies even where liquidity is managed on a consolidated global basis at head office level, in the case of regional and international banking groups. Managing liquidity risk on a consolidated basis does not absolve the senior management of each affiliate entity from the responsibility for ensuring the safety and soundness of the particular institution and compliance with local regulatory requirements.

b) While specific details vary across institutions according to the nature of their business, the key elements of any liquidity policy include:

i. **Management's responsibilities** – outline of responsibilities of the liquidity risk management functions, including structural balance sheet management, pricing, marketing, contingency planning, management reporting, lines of authority and responsibility for liquidity decisions;

ii. **Liquidity risk management structure** – systems for monitoring, reporting and reviewing liquidity;

iii. **Liquidity risk management tools** – approach 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);

iv. **Contingency plan** – strategy for handling liquidity crisis.

c) The policy must be reviewed at the board and senior management/ALCO level at least annually or more frequently when there are material changes in the institution's current and prospective liquidity risk profile.

4.4.3 Procedures

a) An institution should establish documented procedure and/or process manuals in order to implement its liquidity policies. The procedure manual should detail the necessary operational steps and processes to execute the relevant liquidity risk controls.

b) Procedure manuals should be periodically reviewed and updated to take into account new activities, changes in risk management approaches and systems.

4.4.4 Limits and Ratios

a) The board of directors and or senior management should establish limits for the nature and amount of liquidity risk that the institution is willing to assume. The limits should incorporate the nature of the institution's strategies and activities, its past performance, level of earnings and capital available to absorb potential losses, and the tolerance for risk.

b) Every institution should factor the impact of the internal environment (expertise, experience or past performance) and external environment (market conditions, peer indicators, macroeconomic performance) when setting limits and benchmarks.

c) Limits should be documented in the liquidity policies and reviewed periodically (at least annually) or when conditions or risk tolerances change.

d) Senior management/ALCO should have the means to review compliance with established limits. The responsibility for monitoring limits should be assigned to a function independent of the funding areas. There should also be a defined procedure for reporting limits exceptions to senior management/ALCO. While the use of limits would not prevent a liquidity crisis, limit exceptions can be early indicators of excess risk or inadequate liquidity risk management.

e) However, liquidity ratios should always be used in conjunction with more qualitative information such as funding capacity to reveal material liquidity trends. Liquidity ratios are useful for quantifying liquidity risk. Ratios and limits that banking institutions should use to monitor liquidity risk may be categorized as follows:

i. **Cash flow Ratios and Limits –** liquidity risk may arise from an institution's failure to roll-over maturing liabilities or realize anticipated cash flows from assets. Cash flow ratios and limits attempt to measure and control the volume of liabilities maturing during a specified period of time.

ii. **Liability Concentration Ratios and Limits –** these ratios and limits help to prevent an institution from relying on few funding sources. Limits should be expressed as either a percentage of liquid assets or an absolute amount.

iii. **Other Balance Sheet Ratios –** institutions should use the following ratios: total loans/total deposits, total loans/total equity capital, borrowed funds/total assets among ratios to monitor current and potential funding levels.

4.5 Liquidity Measurement and Monitoring

a) Every institution should establish a risk measurement system to ensure that the institutions is able to identify, measure, monitor and control the liquidity risk position for:

i) All future cash flows of assets and liabilities;

ii) All sources of contingent liquidity demand and related triggers associated with off-balance positions;

iii) Special purpose vehicles;

iv) Financial derivatives;

v) Guarantees and commitments;

vi) All currencies in which an institutions is active; and

vii) Correspondent, custody and settlement activities.

b) An institution should employ a range of customised measurement tools, or metric, as there is no single metric that can comprehensively quantify liquidity risk.

c) Management should tailor the measurement and analysis of liquidity risk to the institutions business mix, complexity and risk profile. The measurement and analysis should be comprehensive and incorporate the cash flows and liquidity implications arising from all material assets, liabilities, off-balance sheet positions and other activities of the institutions.

4.5.1 Management Information System

a) Every institution should have adequate management information system (MIS) for measuring, monitoring, controlling and reporting liquidity risk under normal and stressed situations.

b) The MIS should encompass all significant aspects of liquidity risk, including those associated with new products and business initiatives, and capable of evaluating their effect on cash flows and liquidity ratios. In particular, the MIS should be capable of:

i. Calculating cash flows and maturity mismatch positions arising from the full range of an institution's assets, liabilities and off-balance sheet positions on a day-to-day basis;

ii. Analyzing cash flows and maturity mismatch positions in all currencies in which an institution trades, both individually and on an aggregate basis;

iii. Calculating and projecting various limits and ratios in relation to liquidity for both statutory and internal risk management purposes;

iv. Checking compliance with established liquidity policies and limits, and generating exceptions reports; and

v. Reporting risk measures and liquidity trends to management on a timely basis.

c) The MIS should be capable of providing' on a timely basis, accurate and relevant liquidity reports to senior management / ALCO and other responsible personnel for assessment of the level of liquidity risk under different operating circumstances.

4.5.2 Time Bands

a) The maturity profile should have adequate time bands to effectively monitor both an institution's short term liquidity needs and its longer-term liquidity profile. An institution at a minimum should construct daily time bands over a period that ranges

from one week to one month for the purposes of managing its short-term liquidity needs.

b) Wider time bands may be used to manage long-term liquidity.

4.5.3 Behavioural Assumptions

a) In most instances, the actual maturities of assets and liabilities do not reflect their contractual maturities. Therefore, in preparing the maturity profile, an institution should detail the assumptions underlying the behaviour of assets and liabilities and off-balance sheet items.

b) For liabilities with embedded optionality, such as retail deposits where the timing and amount of withdrawals are uncertain, an institution should analyse historical observations to determine their cash flow patterns and derive behavioural assumptions applicable to the cash flows.

c) An institution should also examine the potential for significant cash flows from its off-balance sheet activities. The contingent nature of most off-balance sheet instruments increases the complexity of managing the associated cash flows. Every institution should therefore ascertain a “normal” level of net cash flows arising from off-balance sheet activities on an on-going basis.

d) All behavioural assumptions and their justifications should be documented and approved by senior management/ALCO.

4.5.4 Limit on Net Cumulative Funding Mismatch

a) An institution should specify acceptable limits for the size of the cumulative funding mismatch position for the short-term time bands.

b) Greater emphasis of mismatch analysis should be on short-term cash flows, particularly positions from sight up to one month. However, an institution’s cash flow mismatch position for medium to long-term time bands is important in providing early warning of potential future liquidity problems.

4.5.5 Funding Capacity

a) Every institution should estimate its "normal" funding capacity in both retail and wholesale markets. Deterioration in the institutions' funding capacity can result from the following, among other circumstances:

i. difficulty in accessing the inter-bank and wholesale markets;
ii. concentration in funding sources;
iii. deterioration in asset quality;
iv. increased competition for funds;
v. worsening of earnings performance;
vi. negative media attention; and
vii. adverse change in credit rating.

b) For retail markets, an institution should consider its market share, competitive pressures, economic conditions, and other factors when estimating its funding capacity.

c) An institution that relies heavily on wholesale funds should continuously assess its market acceptance by counterparties to detect any hint of resistance in the funding market.

d) The board of directors and/or senior management must ensure that the relevant personnel are aware of any strategies or events that could affect the market's perception of the institution.

4.5.6 Intra-group Liquidity

a) For institutions that are part of a group, effective liquidity risk management requires a good understanding of the funding positions of all entities in the group that might affect the institution's liquidity. Intra-group liquidity analysis and monitoring require an integrated review of all relevant cash flows.

b) Institutions should analyse and monitor intra-group liquidity on a continuous basis.

4.5.7 Intraday liquidity

c) Structural and operational changes in payment systems will increase the importance of managing intraday liquidity. Banking institutions that participate directly in clearing and settlement systems should take appropriate steps to ensure that they have sufficient collateral to cover cash positions and systems capable of monitoring intraday liquidity positions and cash needs.

4.5.8 Liquidity Stress Testing

a) A financial institution should conduct regular stress tests that include measures aimed at ensuring that the institution can continue to operate in a period of institution-specific stress, market stress and the combination of the two.

b) The board of directors and senior management should examine stress-testing results and formulate appropriate strategies to address the cash-flow needs reflected from 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.

c) Institution-specific stress scenario covers 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 stress scenario is one where liquidity at a large number of institutions in one or more markets, is affected.

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

e) The assumptions may differ quite sharply from scenario to scenario as cash flow timing and size can behave differently in different situations.

f) Institutions should assign an appropriate liquidity discount factor to each asset to take into account the price risk when performing cash flow analysis under each scenario, and should also factor in the settlement period or the expected time needed for liquidating assets.

g) The key assumption underlying an institution-specific stress 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.

h) The minimum criteria for using various assumptions when stress testing liquidity risk are as follows:

   i. The assumptions have to be consistent and reasonable for each scenario;
   ii. The assumptions should be verified and supported by sufficient evidence, experience and performance rather than arbitrarily selected;
   iii. 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; and
   iv. Senior management should ensure that key assumptions are evaluated at least annually for reasonableness.

i) Under a general market stress scenario, it is assumed that an 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 institutions due to the occurrence of a severe tearing of their perceived credit quality (i.e. flight to quality).

j) 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 but could prove to be ineffective if the crisis impinged upon the group as a whole.

k) Institutions should perform scenario analysis on a periodic basis. Senior management/ALCO should review the results of this analysis periodically. Institutions should also review the behavioural assumptions utilized in managing cash flows under the various crisis scenarios on a periodic basis. These assumptions are to be approved by senior management/ALCO.

l) Institutions should document in their stress testing policy the following:

i. The cash-flow assumptions for the institution specific and general market crisis scenarios; and

ii. Their own estimate of the minimum number of days needed to arrange emergency funding support from other sources.

4.5.9 Early Warning Indicators

a) To assess whether a potential liquidity problem may be developing, banks may have regard to various internal and market indicators, including:

i. Internal indicators

- deteriorating asset quality;
- excessive concentrations on certain assets and funding sources;
- decline in earnings and interest margins;
- increase in overall funding costs;
- rapid asset growth being funded by volatile wholesale liabilities; and
- worsening cash-flow positions as evidenced by widening negative maturity mismatches, especially in the short-term time bands.

ii. Market indicators

- credit rating downgrades;
- persistent drop in the bank's stock price;
- widened spread on the bank's senior and subordinated debt;
- reduction in available credit lines from correspondent banks;
- counterparties unwilling to extend unsecured or longer dated transactions to the bank; and

- increasing trend of deposit withdrawals.

a) Banks should have a system for identifying and tracking such indicators to spot potential problems at an early stage.

4.5.10 Contingency Liquidity Plan

a) Every institution should have a contingency liquidity plan for handling liquidity crisis situations. A contingency liquidity plan is a projection of future cash flows and funding sources of an institution under stressed market scenarios including aggressive asset growth or rapid liability erosion.

b) The contingency liquidity plan needs to be commensurate with the institutions complexity, risk profile, scope of operations and role in the financial systems in which the institution operates. In addition, contingency liquidity plan need to be closely integrated with the firm's ongoing analysis of liquidity risk and with the results of the scenarios and assumptions used in stress tests.

c) The contingency liquidity plan should be updated and reviewed on a periodic basis (at least semi-annually) by senior management/ALCO to ensure that it remains robust over time and reflects the institution's changing operating circumstances.

d) At a minimum, the contingency liquidity plan should include the following:

i. designate the personnel responsible for the identification of crisis and for contingency management. This should include provisions for prompt notification of problems to the Central Bank. Responsibilities should be clearly defined so that all personnel understand their roles in a crisis situation;

ii. specify the early warning indicators that are used to signal an approaching crisis event. There should be mechanisms to facilitate constant monitoring and reporting of these indicators;

iii. contain reporting procedures to ensure that all necessary information is available for senior management to make quick decisions;

iv. set out procedures for making up cash flow shortfalls in crisis situations. These should clearly spell out sources of funds, their expected reliability and the priority ranking of the sources;

v. outline courses of action for altering asset and liability structure and assess the likely impact of these on the market's perception of the institution; and include details for handling public relations issues and media management.

4.5.11 Media Relationship and Public Disclosure

a) Good public relations management can help an institution counter rumours that can result in a significant run-off by retail depositors and institutional investors.

b) Public disclosure is also an important element of liquidity management. Banks should provide adequate information on an ongoing basis to the public and, in particular, to major creditors and counterparties so that it is easier for them to manage market perceptions during crisis situations.

4.5.12 Internal Controls and Audit

a) Each institution must have an adequate system of internal controls over its liquidity risk management process.

b) The internal controls 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 controls for liquidity risk management includes;

i. An adequate process for identifying and evaluating liquidity risk;

ii. The establishment of control measures such as policies and procedures;

iii. Adequate management information systems; and

iv. Continual review of adherence to established policies and procedures.

c) An important element of an institution's internal control system over its liquidity risk management process is regular evaluation and independent 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.

d) Management should ensure that all such reviews and evaluations are conducted regularly by individual who are independent of the function being reviewed. When revisions or enhancements to internal controls are warranted, these should be implemented in a timely manner.

e) Limit breaches should receive the prompt attention of appropriate management and should be resolved according to the process described in approved policies.

f) The internal audit function should also periodically review the liquidity management process in order to identify any weaknesses or problems. In turn, these should be addressed by management in a timely and effective manner.

5 INTEREST RATE RISK

5.1 Introduction

a) Interest rate risk is the exposure of a banking institution’s on- and off-balance sheet positions to adverse movements in interest rates resulting in a loss to earnings and capital.

b) Changes in interest rates affect an institution's earnings by changing its net interest income and the level of other interest-sensitive income and operating expenses. Changes in interest rates also affect the underlying value of the financial 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.

c) While interest rate risk is assumed by financial institutions as part of normal financial intermediation, excessive interest rate risk poses a significant threat to a banking institution’s financial condition. In this regard, the board and senior management should design and implement sound interest rate risk management systems that minimise the bank’s vulnerability to movements in interest rates.

5.2 Sources of Interest Rate Risk

a) The primary forms of interest rate risk to which financial institutions are typically exposed include:

i. **Repricing risk*:*** This arises from timing differences in the maturity and repricing of financial institutions’ assets, liabilities and off-balance sheet (OBS) positions.

ii. **Yield curve risk***:* Yield curve risk arises when unanticipated shifts of the yield curve have adverse effects on an institution's income or underlying economic value.

iii. **Basis risk***:* arises from imperfect correlation in the adjustment of the rates earned and paid on different instruments with otherwise similar repricing characteristics.

iv. **Price risk:** arise from changes in the value of marked-to-market financial instruments that occur when interest rates change.

v. Optionality risk*:* It arises from the options embedded in many banking institution assets, liabilities and OBS portfolios.

b) As such, banking institutions' risk management systems should incorporate methodologies for identifying, measuring, monitoring and controlling all the primary forms of interest rate risk.

5.3 Sound Interest rate Risk Management Practices

a) A strong interest rate risk control environment is built on the foundation of a well designed strategy and policy, adequate management information systems, rigorous internal controls, competent staff and timely reporting.

b) At a minimum, a bank should have an interest rate risk management framework comprising four basic elements:

i. appropriate board and senior management oversight;
ii. adequate risk management policies and procedures;
iii. appropriate risk measurement, monitoring, and control functions; and
iv. comprehensive internal controls and independent audits.

5.4 Board and Senior Management Oversight

5.4.1 Board Oversight

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

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

d) approve policies that identify lines of authority and responsibility for managing interest rate risk exposures;

e) delegating responsibility for establishing interest rate risk policies to the Asset and Liability Committee (ALCO) or other designated committee.

5.4.2 Senior Management Oversight

Senior management is responsible for:

a) Senior management should ensure that the structure of the bank's business and the level of interest rate risk it assumes are correctly aligned and effectively managed.

b) Management should ensure that the bank has adequate policies and procedures for managing interest rate risk on both long-term and day-to-day bases and that the banking institution maintains clear lines of authority and responsibility for managing and controlling this risk.

c) It is the responsibility of management to maintain:

i. appropriate limits on risk taking;

ii. adequate management information systems and standards for measuring interest rate risk;

iii. standards for valuing positions and measuring performance;

iv. a comprehensive interest rate risk reporting and management review process; and

v. effective internal controls.

d) In order to fulfill the above responsibilities senior management should:

i. periodically review the organisation's interest rate risk management policies and procedures to ensure that they remain appropriate and sound;

ii. set aside adequate capital commensurate with the level of interest rate risk assumed by the banking institution;

iii. periodically update the board of directors regarding interest rate risk measurement, reporting and management procedures;

iv. ensure that there is sufficient depth and skill in staff resources to manage interest rate risk and to accommodate the temporary absence of key personnel;

v. define lines of authority and responsibility for developing and implementing strategies and conducting the risk measurement and reporting functions of the interest rate risk management process;

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

vii. ensure that there is adequate separation of duties in key elements of the interest rate risk management process to avoid potential conflicts of interest;

viii. 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, and the conduct of back-office functions;

ix. ensure that the nature and scope of these safeguards is in accordance with the size and structure of the bank. They should also be commensurate with the volume and complexity of interest rate risk incurred by the bank and the complexity of its transactions and commitments; and

x. ensure that the bank has a designated independent function responsible for the design and administration of the bank's interest rate risk measurement, monitoring, and control functions.

5.4.3 Policies and Procedures and Limits

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

b) Interest rate risk policies should identify quantitative parameters that define the level of interest rate risk acceptable for the institution. Where appropriate, limits should be further specified for certain types of instruments, portfolios, and activities.

c) 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.

d) Policies should clearly identify:

i. the types of instruments and activities that an institution may employ or conduct, as a means of communicating the institution’s risk tolerance;

ii. permissible instruments, either specifically or by their characteristics, and should also describe the purposes or objectives for which they may be used; and

iii. a delineated set of institutional procedures for acquiring specific instruments, managing portfolios, and controlling the banking institution's aggregate interest rate risk exposure.

iv. clearly define approvals necessary for exceptions to policies, limits, and authorizations.

e) Products and activities that are new to the institution should undergo a careful pre-acquisition review to ensure that the 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 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.

f) 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. The procedures for undertaking new instruments or new strategies should at least contain these features:

i. description of the relevant product or strategy;

ii. identification of the resources required to establish sound and effective interest rate risk management of the product or activity;

iii. analysis of the impact of the proposed activities on the banking institution’s overall financial condition and capital levels;

iv. procedures to be used to measure, monitor, and control the risks of the proposed product or activity; and

v. be reviewed and approved by the board at least on an annual basis.

5.4.4 Limits

a) Financial institutions should put in place risk taking guidelines in order to bantam an 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 institution and those limits could be applied on individual portfolios, activities or business units.

b) 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.

c) Interest rate risk limits clearly articulating the amount of interest rate risk acceptable to the 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 institution as well as its ability to measure and manage its risk.

d) 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.

5.5 Risk Measurement, Monitoring and Control

Interest rate risk management process encompasses risk measurement, monitoring and control.

5.5.1 Risk Measurement

a) Financial institutions should have interest rate risk measurement systems that capture all sources of interest rate risk, which assess the effect of interest rate changes in ways that are consistent with the scope of their activities.
b) Interest rate risk measurement systems should also assess the effects of rate changes on both earnings and economic value as follows:

   i. ***Earnings perspective:*** The focus of analysis is the impact of changes in interest rates on accrual or reported earnings. Variation in earnings is an important focal point for interest rate risk analysis because reduced earnings or outright losses can threaten the financial stability of an institution by undermining its capital adequacy and by reducing market confidence.

   ii. ***Economic value perspective*****:** Variation in market interest rates can also affect the economic value of an institution's assets, liabilities and OBS positions. Thus, the sensitivity of an 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.
   iii. ***Embedded losses:*** The earnings and economic value perspectives focus on how future changes in interest rates may affect an institution's financial performance. When evaluating the level of interest rate risk it is willing and able to assume, an institution should also consider the impact that past interest rates may have on future performance.

c) The methodology for measuring interest rate risk should be based on adequate information on current positions, market conditions and instrument characteristics. A bank should have at least two techniques for measuring interest rate risk.
d) A number of techniques are available for measuring interest rate risk exposure of both earnings and economic value. Their complexity ranges from simple calculations to

static simulations using current holdings and highly sophisticated dynamic modeling techniques that reflect potential future business and business decisions.

e) The techniques that can be used to measure interest rate risk include gap analysis, duration, simulation and Value at Risk (VaR).

Gap Analysis

i. To evaluate earnings exposure, interest rate-sensitive liabilities in each timeband should be subtracted from the corresponding interest rate-sensitive assets to produce a repricing "gap" for that time band. This gap should be multiplied by an assumed change in interest rates to yield an approximation of the change in net interest income that would result from such an interest rate movement.

ii. The size of the interest rate movement used in the analysis can be based on a variety of factors, which include historical experience, simulation of potential future interest rate movements, and the judgment of bank management.

Duration

i. Duration is the weighted average term to maturity of assets/liabilities.

ii. Duration-based weights can be used in combination with a maturity/repricing schedule to provide a rough approximation of the change in a bank's economic value that would occur given a particular change in the level of market interest rates. Typically, such weights should be based on estimates of the duration of the assets and liabilities that fall into each time band. In some cases, different weights should be used for different positions that fall within a time band, reflecting broad differences in the coupon rates and maturities (for instance, one weight for assets, and another for liabilities).

iii. In addition, different interest rate changes are sometimes used for different time bands, generally to reflect differences in the volatility of interest rates along the yield curve. The weighted gaps are aggregated across time bands to produce an estimate of the change in economic value of the bank that would result from the assumed changes in interest rates.

Simulation

i. Banking institutions with complex risk profiles or which use complex financial instruments should employ more sophisticated interest rate risk measurement systems than those based on simple maturity/repricing schedules.
ii. These simulation techniques typically involve detailed assessments of the potential effects of changes in interest rates on earnings and economic value by simulating the potential direction of interest rates and their impact on cash flows.

Static simulation

i. When measuring interest rate risk using static simulations, the cash-flows arising solely from the bank's current on and off balance-sheet positions should be 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.
ii. 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 bank's holdings and discounted back to their present values, an estimate of the change in the bank's economic value should be calculated.

Dynamic simulation

i. The simulation should build in more detailed assumptions about the future course of interest rates and the expected changes in a bank's business activity over that time. These more sophisticated techniques allow for dynamic interaction of payment streams and interest rates, and better capture the effect of embedded or explicit options.
ii. The usefulness of simulation-based interest rate risk measurement techniques depends on the validity of the underlying assumptions and the accuracy of the basic methodology. The output of sophisticated simulations should be assessed largely in

the light of the validity of the simulation's assumptions about future interest rates and the behaviour of the bank and its customers.

Value at Risk (VaR)

i. VaR is a summary measure of the predicted loss (or worst loss) over a target horizon within a given confidence level. Generally three ways of calculating VaR can be used;
   - Parametric method or Variance/Covariance approach;
   - Historical simulation; and
   - Monte Carlo method.

ii. Banking institutions using VaR models should carry out back tests.

iii. VaR is not unique to market risk as it can also be used to measure other types of risk, namely credit and operational risks.

f) Banking institutions should design measurement methodologies that should:

i. evaluate all significant interest rate risk arising from the full range of a bank's assets, liabilities and off-balance sheet positions, both trading and non-trading. If the same measurement systems and management methodologies are not used for all activities, an integrated view of interest rate risk across products and business lines should be available to management;

ii. utilise generally accepted financial concepts, models and risk measurement techniques;

iii. have accurate and timely data (in relation to rates, maturities, repricing, embedded options and other details) on current positions;

iv. have well-documented assumptions and parameters on which they are based. Any manual adjustments to underlying data and assumptions should be clearly documented and the nature and reasons for the adjustments should be understood;

v. cover all significant sources of interest rate risk. Banking institutions should pay special attention to the largest concentrations and positions as well as instruments which might have a material effect on a bank's overall position; and

vi. assess exposures in different currencies.

g) Senior management should have an integrated view of interest rate risk across products and business lines.

h) A bank should ensure that all material positions and cash-flows, whether stemming from on or off-balance sheet positions, are incorporated into the measurement system on a timely basis.

i) Assumptions used in assessing the interest rate sensitivity of complex instruments and instruments with uncertain maturities should be subject to thorough documentation and review.

j) Banking institutions with multi-currency exposures should include techniques to aggregate their exposures in different currencies using assumptions about the correlation between interest rates in different currencies in their risk measurement process. A banking institution should periodically review the stability and accuracy of the correlation assumptions and evaluate what its potential risk exposure would be in the event that such correlations break down.

5.5.2 Risk Monitoring

a) Financial institutions should establish and enforce operating limits that maintain exposures within levels consistent with their internal policies and that are in accordance with their approach to measuring interest rate risk.

b) The 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.

c) Aggregate interest rate risk limits should be approved by the board of directors and reviewed at least once a year. These limits should be appropriate to the size, complexity and capital adequacy of the bank as well as its ability to measure and manage its risk.

d) At a minimum, banking institutions should have limits in the following categories:

   i. change in net portfolio value;
   ii. Value at Risk (VaR);
   iii. factor sensitivity;
   iv. interest rate sensitivity gap;
   v. impact on earnings; and
   vi. impact on capital.

e) Interest rate risk limits should be linked to specific scenarios of movements in market interest rates. Specified scenarios should take account of the full range of possible sources of interest rate risk to the bank.

5.5.3 Stress testing

a) The risk measurement system should support a meaningful evaluation of the effect of stressful market conditions on the institution. Assumptions used in building stress testing scenarios should be clearly documented and reviewed periodically. 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 institution.

b) The following are typical factors that must be considered when stress testing for interest rate risk:

i. **Re-pricing risk**: this assesses the effects on a banking institution's profitability of timing differences in interest rate changes and cash flows in respect of fixed and floating rate assets, liabilities and off-balance sheet instruments;

Basis risk: this evaluates the effects on a banking institution's profitability of unfavourable differential changes in key market rates (e.g. interbank and the prime rate);

ii. **Yield curve risk:** this assesses the effects on a banking institution's profitability of parallel yield curve shifts (up and down) and non-parallel yield curve shifts (i.e. steepening, flattening or twisting of the yield curve); and

iii. **Option risk:** this evaluates the effects of changes in the value of both standalone option instruments and embedded options (e.g. loans which give borrowers the right to prepay and deposits that might be withdrawn at any time).

iv. **Price risk:** arise from changes in the value of marked-to-market financial instruments that occur when interest rates change.

c) Stress scenarios to be used for interest rate risk should include:

i. historical scenarios in which sharp changes in interest rates were experienced;

ii. hypothetical changes in the general level of interest rates;

iii. changes in the relationships between key market rates (i.e. basis risk), e.g. a surge in term and savings deposit rates and interbank rate but no change in the prime lending rate, and a drop in the prime lending rate but no change in term and savings deposit rates and interbank rate;

iv. changes in interest rates in individual time bands to different relative levels (i.e. yield curve risk);

v. changes in the liquidity of key financial markets or changes in the volatility of market rates; and

vi. changes in key business assumptions and parameters, in particular, changes in assumptions used for illiquid instruments and instruments with uncertain contractual maturities help in the understanding of a banking institution's risk profile.

d) Assumptions used in building stress testing scenarios should be clearly documented
and reviewed at least on an annual basis and;

e) Management and the board of directors should periodically review both the design and the results of stress tests, and ensure that appropriate contingency plans are in place.

5.5.4 Reporting MIS

a) 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.

b) Reports detailing the interest rate risk exposure of the 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 institution's interest rate risk profile, they should, at a minimum include the following:

i. summaries of the institution's aggregate interest rate exposures;
ii. reports demonstrating compliance with policies and limits;
iii. key assumptions, for example, non-maturity deposit behaviour and prepayment information;
iv. results of stress tests including those assessing breakdowns in key assumptions and parameters; and
v. 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.

5.5.5 Internal Controls

(a) Financial 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:

i. effective and efficient operations,
ii. reliable financial and regulatory reporting, and
iii. compliance with relevant laws, regulations and institutional policies.

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

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

(c) Financial 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:

i. the quantity of interest rate risk, e.g.

a) the volume and price sensitivity of various products;
b) the vulnerability of earnings and capital under differing rate changes including, yield curve twists; and
c) the exposure of earnings and economic value to various other forms of interest rate risk, including basis and optionality risk.

ii. the quality of interest rate risk management, e.g.

a) whether the institutions' internal measurement system is appropriate to the nature, scope, and complexities of the entity and its activities;
b) whether the institution has an independent risk control unit responsible for the design and administration of the risk measurement, monitoring and control functions;
c) whether the board of directors and senior management are actively involved in the risk control process;
d) whether internal policies, controls and procedures concerning interest rate risk are well documented and complied with;
e) whether the assumptions of the risk measurement system are well documented, data accurately processed, and data aggregation is proper and reliable; and
f) whether the institution has adequate staffing to conduct a sound risk management process.

6 FOREIGN EXCHANGE RISK

6.1 Introduction

a) Foreign exchange risk is the potential adverse impact on earnings and economic value due to currency rate movements. 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.

b) The foreign exchange positions arise from the following activities:

i. 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;

ii. holding foreign currency positions in the banking book (e.g. in the form of loans, bonds, deposits or cross-border investments); or

iii. engaging in derivative transactions (e.g. structured notes, synthetic investments and structured deposits) that are denominated in foreign currency for trading or hedging purposes.

c) There are various types of foreign exchange risk which include;

i. exchange rate risk which is the risk of loss as a result of adverse movements in the exchange rate;

ii. interest rate risk which arises from maturity mismatches on foreign currency positions;

iii. credit risk which is due to counterparty default on foreign exchange loans or contracts; and

iv. sovereign risk which arises from country risk or political risk.

6.2 Risk Management Process

a) Sound foreign exchange risk management involves four basic elements in the management of on and off-balance sheet assets and liabilities:

i. Board and Management Oversight;
ii. Policies, Procedures and Limits;
iii. Risk Identification and Measurement, Monitoring and Management Information Systems; and
iv. Internal Controls.

6.3 Board and Senior Management Oversight

Board of Directors

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

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

c) The board and senior management's responsibilities include;
   i. setting the foreign exchange risk management strategy and tolerance levels;
   ii. ensuring that effective risk management systems and internal controls are in
   iii. place;
   iv. monitoring significant foreign exchange exposures;
   v. ensuring that foreign exchange operations within the banking institution are
   vi. in compliance with foreign exchange control regulations;
   vii. ensuring that foreign exchange operations are supported by adequate
   viii. management information systems which complement the risk management
   ix. strategy; and
   x. reviewing policies, procedures and currency limits regularly in line with changes in the economic environment.

6.4 Policies, Procedures and Limits

a) 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.

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

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

d) These policies and procedures should:
   i. define lines of responsibility and identify individuals or committees responsible for developing foreign exchange risk management strategies,
   ii. making foreign exchange risk management decisions, and conducting oversight;
   iii. identify authorized types of financial instruments and hedging strategies;
   iv. describe a set of strategies for controlling the institution's aggregate foreign exchange rate risk exposure;
   v. 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
   vi. define procedures and conditions for dealing with exceptions to policies, limits, and authorizations.

6.5 Risk Identification, Measurement, and Control

6.5.1 Risk Identification

Foreign exchange rate risk can be split into translation, transaction and economic exposure:

(i) Translation exposure: arises from accounting based changes in consolidated financial statements caused by changes in exchange rates;

(ii) Transaction exposure: occurs when exchange rates change between the time that an obligation in incurred and the time it is settled, thus affecting actual cash flows; and

(iii) Economic exposure: 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.

6.5.2 Risk Measurement

a) Measuring risk is very critical to understanding the potential loss an institution may be exposed to in the event of any loss. At a minimum, the measurement system should include, among other things:

i. evaluate all foreign exchange risks by maturity, on both gross and net bases, arising from the full range of a bank's assets, liabilities and off-balance sheet positions;

ii. employ accepted financial models or methods for measuring risk of foreign exchange options;

iii. be able to calculate comprehensive risk factor sensitivities for the purpose of capturing the non-linearity nature of price risk of foreign exchange positions;

iv. have accurate and timely data;

v. incorporate daily mark-to-market of trading positions;

vi. enable banks to monitor their foreign exchange settlement risk in real-time in order to ensure that settlement limits will not be exceeded..

6.5.3 Risk limits

(a) a comprehensive framework of limits to control foreign exchange risk exposures should be established for different levels of reporting;

(b) At a minimum, financial institutions should have the following limits for foreign exchange operations:

i. open position limits for individual currencies to which 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;

ii. open position limits on the aggregate of all currencies, both during the day and overnight;

iii. open position limits by each centre where the institution operates;

iv. stop loss and/or management-action-trigger limits; and

v. limits for settlement risk of all counterparties.

(c) the limits should be reviewed at least annually or more frequently in line with changes in the operating environment.

6.5.4 Stress Testing

a) Financial institutions should conduct stress tests on their foreign currency positions. The stress for exchange rate risk assess the impact of changes in exchange rates on the profitability and economic value of a financial institution's equity;

b) The effects of significant exchange rate movements, including sharp reductions in liquidity, of individual currencies should be considered when setting stress scenarios;

c) Stress testing results should be incorporated in the review of business strategies policies and limits on foreign exchange risk.

d) 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.

6.5.5 Risk Monitoring and control

a) Foreign exchange risk monitoring processes should be established to evaluate the performance of a financial institutions' risk strategies, policies and procedures in achieving its overall goals;

b) The monitoring function should be independent of units taking risk and should report directly to senior management and board of directors;

c) Ordinarily 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 institutions' ALCO.

d) The middle office should reconcile regularly positions of trader to ensure that these are within assigned limits. Internal reports comparing actual positions against internal limits should be routinely prepared for management.

6.5.6 Management Information System

a) Accurate and timely information systems are critical to the management of foreign currency positions, and for ensuring compliance with relevant risk limits. Financial institutions should:

   i. Devote the resources necessary to generating information on compliance with relevant risk limits.
   ii. Design standardised reports to communicate the information regarding open foreign exchange positions, forward interest rate positions, liquidity positions, counterparty and country exposures.
   iii. Ensure that positions and exposures are reported on a consolidated basis. Such reports should be prepared and verified by persons not responsible for transacting foreign currency business.

b) At a minimum reports should include:

   i. individual and aggregate foreign exchange risk exposures;
   ii. information on adherence to policies and limits; and
   iii. findings of risk reviews on foreign exchange risk policies and procedures.

6.6 Internal Controls and Audit

a) Internal audit should review and assess the foreign exchange risk management process subsequent to the quantification of foreign exchange risk. It should also ensure that foreign exchange traders / dealers observe their instructions and the code of behaviour required of them and that accounting procedures meet the necessary standards of accuracy, promptness and completeness. It will also be necessary for management to establish and implement procedures governing the conduct and practices of foreign exchange traders/dealers.

b) Periodically, Audit Committee should review the foreign exchange risk management process so as to enhance the quality of reports and the reasonableness of foreign exchange risk management information supplied to the board, the management and the Central Bank of Liberia.

7 OPERATIONAL RISK

7.1 Introduction

a. Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. It is associated with human error, system failures and inadequate procedures and controls. Operational risk also includes legal risk, which arises when a transaction proves unenforceable in law, but excludes strategic and reputation risk.

b. Developments such as deregulation and globalisation of financial markets, and, if not properly controlled, the greater use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems. Further, 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. The increased prevalence of outsourcing are making the activities of banking institutions more diverse and complex leading to high levels of operational risk.

c. Financial institutions are expected to establish a sound and effective system to manage operational risk as a distinct class of risk. Failure to implement proper processes and procedures to control operational risks can result in a misstatement of the institution's risk/return profile and expose the institution to significant losses.

d. The objective of operational risk management is to:

   i. To find out the extent of the financial institution's operational risk exposure;
   ii. To understand what drives it;
   iii. To allocate capital against it; and

iv. Identify and employ tools both internally and externally, that would help in risk mitigation.

7.2 Operational Risk Management Framework

a) Every institution is expected to develop an appropriate framework for managing operational risk, commensurate with the size and complexity of its operations. 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.

b) The operational risk management framework should consist of the following components:

i. board and senior management oversight;
ii. operational risk management strategy, policies and procedures;
iii. identifying, measuring, monitoring and reporting operational risk;
iv. adequate operational risk management information system; and
v. sound internal controls and reviews.

7.3 Board and Senior Management Oversight

7.3.1 Board of Directors

The ultimate responsibility for operational risk management rests with the board of directors. To fulfil this responsibility, the board or its delegated committee should:

a) understand the major aspects of the institution's operational risk as a distinct category of risk that should be managed;
b) define the operational risk strategy and ensure that the strategy is aligned with the institution's overall business objectives;

c) approve and periodically review a written enterprise-wide operational risk management framework;
d) approve the operational risk policies developed by senior management;
e) review periodic high-level reports on the institution's overall operational risk profile, which identify material risks and strategic implications for the institution;
f) establish a management structure with clear lines of accountability and reporting. In addition, there must be segregated responsibilities and reporting lines between control functions and the revenue generating business lines;
g) ensure that senior management is taking necessary steps to implement appropriate policies, processes and procedures as approved by the board;
h) ensure that the operational risk management framework is subject to independent review by internal audit or other oversight functions; and
i) ensure compliance with regulatory disclosure requirements on operational risk.

7.3.2 Senior Management oversight

In developing the operational risk management framework for approval by the board of directors, senior management should:

a) define the institution's organizational structure and clearly assign authority, responsibility and reporting relationships to encourage accountability;
b) implement the board approved operational risk management policy;
c) ensure that appropriate operational risk control systems are in place;
d) ensure that the institution's activities are conducted by qualified staff with the necessary experience and technical capabilities and that staff responsible for monitoring and enforcing the institution's operational risk policy are independent from the business units they oversee;
e) ensure that staff with responsibility for operational risk communicate effectively with staff responsible for the procurement of external services as failure to do so may result in significant gaps or overlaps in a banks' overall risk management programme;
f) ensure that the institution's operational risk management policies, processes, and procedures are documented and clearly communicated to staff at all levels;

g) pay particular attention to the quality of documentation controls and to transaction-handling practices;

h) put in place clear reporting systems of operational risk failures and provide for their subsequent resolution;

i) ensure that the operational risk management framework is subjected to independent reviews, which will provide assurance that the framework is adequate; and

j) ensure that the institution's remuneration policies are consistent with its appetite for risk.

7.4 Policies and Procedures

a) A financial institution should have policies and procedures to control or mitigate material operational risk which should clearly set out the strategy, objectives and the major elements of the operational risk management framework, including identifying, measuring, monitoring, and controlling operational risk.

b) The policies and procedures should outline all aspects of the institution's operational risk management framework, including:

   i. the organisational structure, which defines operational risk management roles, responsibilities and reporting lines of the board, committees, senior management, risk management function, business line management and other operational risk related functions.

   ii. a definition for operational risk, including the loss event types that will be monitored;

   iii. the capture and use of internal and external operational risk loss data, including large potential events (scenario analysis);

   iv. an outline of the reporting framework and types of data/information to be included in the risk management reports;

   v. the development and incorporation of business environment and internal control factor assessments into the operational risk framework;

   vi. the internally derived analytical framework that quantifies the operational risk exposure of the institution;

vii. qualitative factors and risk mitigants and how they are incorporated into the operational risk framework;

viii. factors that affect the measurement of operational risk; and

ix. provisions for the review and approval of significant policy and procedural exceptions.

c) The risk management policy should be supported by a set of principles that apply to specific components of operational risk, such as new customer approval, new product approval, new information technology systems approval, outsourcing, business continuity planning, crisis management, and anti-money laundering.

7.4.1 Operational Risk Function

The responsibilities of the Operational Risk Function are as follows:

a) Management should ensure that a separate function independent of internal audit is established for effective management of operational risks in the financial institution. Such a functional set-up would assist management to understand and effectively manage operational risk.

b) The function would assess, monitor and report on operational risk and ensure that the management of the operational risk is carried out in terms of the institutions' strategy and policy.

c) To accomplish the task, the function would help establish policies and standards and coordinate various risk management activities. In addition, the function should also provide guidance relating to various risk management tools, monitor risk and prepare reports for management and the board.

7.5 Operational Risk Identification and Measurement

7.5.1 Identification and assessment

a) Management should establish a process that identifies the nature and types of operational risk, its causes and impact on the institution. Effective operational risk identification and assessment processes are vital for an institution to understand its risk profile and effectively focus risk management resources.

b) Risk identification should include both internal factors (such as the complexity of the institution's structure, the nature of the institution's activities, and the quality of personnel, 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 institution's objectives.

c) institutions should ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is adequately assessed.

d) Every institution should adopt techniques that provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate or control that risk. An institution should use at least one of the following processes, among others, to identify and assess operational risk:

   i. **Self Risk Assessment**: Every financial institution's business unit should assess its operations and activities against a menu of potential operational risk vulnerabilities. The process should incorporate checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment.

   ii. **Risk Mapping**: Institutions should have structures in place to map various business units, organizational functions or process flows by risk type in order to prioritize corrective actions.

iii. **Key Risk Indicators**: Key risk indicators are early warning statistics and/or metrics, often financial, which may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions. These objective measures allow the risk manager to forecast losses through the application of regression techniques. These indicators should be reviewed on a quarterly basis to alert management to changes that may be indicative of risk concerns.

iv. **Scorecards:** An institution must have techniques for:

1) translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures;
2) allocating economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk; and
3) addressing factor inherent risks, as well as the controls to mitigate them.

v. **Thresholds/limits:** The institution's operational risk framework must stipulate limits to be adhered to. Threshold levels in key risk indicators should be used to alert management on areas of potential problems when exceeded.

vi. **Earnings volatility:** Institutions can use this tool after stripping the effect of market and credit risk on their portfolios, to assess operational risk. The approach consists of taking a time-series of earnings adjusted for trends, and computing its volatility

vii. **Casual Networks:** This technique describes how losses can occur from a cascade of different causes. Causes and effects are linked through conditional probabilities. An institution can then run simulations on the network, generating a distribution of losses.

viii. **Actuarial models:** Institutions can use this approach which combines the distribution of frequency of losses with their severity distribution to produce a distribution of losses due to operational risk.

ix. **Audit oversight:** Institutions can engage the services of external auditors to provide independent reviews of business processes.

7.5.2 Measurement

a) A banking institution should adopt a comprehensive operational risk analytical framework that provides an estimate of the institution's operational risk exposure.

b) Management should document the assumptions underpinning the operational risk management framework, including the choice of inputs, distributional assumptions, and the weighting across qualitative and quantitative elements. Management should also document and justify any subsequent changes to these assumptions.

c) The institution's operational risk analytical framework should use a combination of internal operational loss event data, relevant external operational loss event data, business environment and internal control factor assessments, and scenario analysis. The institution should combine these elements in a manner that most effectively enables it to quantify its operational risk exposure. The institution should choose the analytical framework that is most appropriate to its business model.

d) A bank's operational risk analytical framework should clearly identify:
   i. the different inputs that are combined and weighted to arrive at the overall operational risk exposure so that the analytical framework is transparent.
   ii. The documentation should demonstrate that the analytical framework is comprehensive and internally consistent;
   iii. quantitative and qualitative assumptions embedded in the methodology and provide explanation for the choice of these assumptions;
   iv. results based purely on quantitative methods separately from results that incorporate qualitative factors. This will provide a transparent means of determining the relative importance of quantitative versus qualitative inputs;
   v. a comparison of the operational risk exposure estimates generated by the analytical framework with actual loss experience over time, to assess the reasonableness of the framework's outputs (back testing);
   vi. all changes to assumptions, and provide explanations for such changes; and
   vii. the results of an independent verification of the analytical framework.

7.5.3 Monitoring and Reporting

a) To facilitate monitoring of operational risk, results from the measurement system should be summarized in reports that can be used by the bank-wide operational risk and functional business lines to understand, manage, and control operational risk and losses. These reports should serve as a basis for assessing operational risk and related mitigation strategies and creating incentives to improve operational risk management throughout the institution.

b) The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. The internal control system should be integrated into the bank's operations. The results of these monitoring activities should be included in management and board reports, as should compliance reviews performed by the internal audit and/or risk management functions.

c) Senior management should receive regular reports from both business units and the internal audit function. These reports should:
   i. contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making;
   ii. be distributed to appropriate levels of management and to areas of the bank which may be directly affected by the events and/or conditions;
   iii. outline trend analysis to assess and manage operational risk exposures at the business line level and bank-wide level;
   iv. fully reflect operational risk loss experience of the bank by business line, event type and/or problem areas; and
   v. motivate timely corrective action on outstanding issues.

d) The results of monitoring activities, findings of compliance reviews performed by internal audit and/or the risk management function, management letters issued by external auditors, and reports generated by supervisory authorities should be included

in regular reports to the board and senior management to support proactive management.

e) The board of directors should receive sufficient higher-level information to enable them to understand the bank's overall risk profile and focus on the material and strategic implications of operational risk to the business.

f) To ensure the usefulness and reliability of the reports management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls.

7.5.4 Risk Control and Mitigation

a) The board and senior management should establish policies, processes and procedures to control and/or mitigate operational risks that the bank has identified. A bank should also have a system in place for ensuring compliance with a documented set of internal policies concerning the banks' risk management system.

b) The risk management control infrastructure should keep pace with growth or changes in business activities (e.g. new products, operations in subsidiaries and entry into new markets).

c) A critical element to the control of operational risk is the existence of a sound internal control system. When properly designed and consistently enforced, a sound internal control system will help management safeguard the institution's resources, produce reliable financial reports, and comply with laws and regulations. Sound internal controls will also reduce the possibility of significant human errors and irregularities in internal processes and systems, and will assist in their timely detection when they do occur.

d) A banking institution should have an effective internal control system which ensures:
    i. appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest.

ii. close monitoring of adherence to assigned risk limits or thresholds and investigation of breaches;
iii. maintaining safeguards for access to and use of bank assets and records;
iv. staff has appropriate expertise and training;
v. identifying of business lines or products where returns appear to be significantly out of line with reasonable expectations; and
vi. regular verification and reconciliation of transactions and accounts.

e) A bank should utilise risk mitigation tools to reduce the exposure to, or frequency and/or severity of significant operational risks with low probabilities and potentially very large financial impact, and uncontrolled risk events.

f) The bank should use risk mitigation tools as complementary to, rather than a replacement for, thorough internal operational risk control. Careful consideration should also 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).

g) A banking institution should have relevant policies and procedures to control/mitigate their exposures arising from the following operational risk drivers, among others:
i. new products and activities;
ii. change of IT systems, facilities and equipments;
iii. e-banking services;
iv. outsourcing arrangements;
v. money laundering;
vi. suitability of customers, and
vii. external documentation e.g. contracts and transaction statements.

7.6 Business Continuity Management

a) Business Continuity Management ("BCM") aims to minimize the impact to businesses due to operational disruptions. It not only addresses the restoration of information technology ("IT") infrastructure, but also focuses on the rapid recovery and

resumption of critical business functions for the fulfillment of business obligations. One important tangible evidence that the institutions have embraced BCM is the formulation of a business continuity plan ("BCP").

7.6.1 Board and Senior Management Oversight

b) The responsibility for the state of business continuity preparedness of an institution ultimately lies with the Board of directors and senior management. Senior management is responsible for steering BCM with policies and strategies necessary for the continuation of critical business functions.

c) In addition, they should demonstrate that they have sufficient awareness of the risks, mitigating measures and state of readiness by way of an attestation to the Board of directors. The attestation should be updated at least once a year or more frequently should there be material change within the institution.

7.6.2 Embed BCM into Business-As usual Operations

a) Institutions should strive to build organizational cultures that embed BCM as part of their business-as-usual operations and day-to-day risk management.

b) Depending on the scale and complexity of the businesses, institutions could adopt sound BCM practices that include the following components:

i. Clear BCM policy, strategy and budget
ii. Well-defined roles and responsibilities for the BCM programme
iii. BCP comprising of detailed tasks and activities
iv. Succession plans for critical staff and senior management
v. Business impact analysis or similar process
vi. Programme for the development, implementation, testing and maintenance of BCP
vii. Programmes for training and awareness
viii. Emergency responses

ix. External communications and crisis management coordination programmes

x. Coordination with external parties (including authorities, interdependent parties, etc.)

7.6.3 Regular Business Continuity Plans

a) Testing is a vital element for implementing an effective BCM. Changes in technology, business processes and staffs' roles and responsibilities can affect the appropriateness of the BCP; and ultimately the business continuity preparedness of institutions.

b) It is therefore important for banks to regularly test its functionality and effectiveness assurance that should they activate their BCP, they would be able to continue to operate reliably, responsively, and efficiently as planned.

7.6.4 Comprehensive Recovery Strategies

a) The establishment of recovery strategies enables institutions to execute their BCP in an orderly and predefined manner that minimises disruption and financial loss. Recovery strategies form the basis for defining recovery time objectives of critical business functions. Without these clear markers, scarce resources may be inappropriately diverted to less important activities. This may adversely affect the institutions' reputation and survivability.

b) Critical business functions

Institutions should therefore identify business functions that are critical (including support operations and related IT systems) and the potential losses (in monetary and non-monetary terms) should their operations be disrupted.

c) Determining recovery time objectives for critical business functions

Banking institutions are responsible for determining their critical business functions, recovery strategies and the corresponding recovery time objectives that is

commensurate with the nature, scale and complexity of their business functions and business obligations.

7.6.5 Mitigation of Interdependency Risk of Critical Business Functions.

a) Banking institutions should mitigate the risk arising from these complex dependencies as far as practically possible and consider such dependencies in their recovery strategies and recovery time objectives.
b) Institutions should proactively seek assurances that their service providers' BCP are regularly tested.

7.6.6 Planning For Wide-area Disruptions.

a) Banking institutions should demonstrate that they have planned and catered for a wide-area disruption in their BCM. Some planning parameters that institutions may consider are; the geographical concentration of institutions, transactional processing activities, and dependencies on internal or external service providers.

7.6.7 Mitigation of Concentration Risk.

a) To mitigate concentration risk of critical business functions, institutions could consider the following approaches:
    i. **Primary-secondary site separation.** Separate the primary and secondary sites of critical business functions into different zones. This would mitigate the risk of losing both sites in a wide-area disruption.
    ii. **Critical business functions separation and intra-function separation.** Separating critical business functions into different zones would mitigate the risk of losing multiple critical business functions from a single-zone disruption. Similarly, diversifying critical business functions (e.g. back-office settlement operations and critical IT support, etc.), such that another labour pool in a different zone is able to take over these functions during disruptions, would eliminate the dependency on a single labour pool. These approaches

have different cost implications and institutions are encouraged to be innovative and explore different avenues of mitigating concentration risk.

7.6.8 Public disclosure

An institution should publicly disclose information on operational risk losses incurred by the institution on an on-going basis to enable market participants to make informed judgement about the soundness of its operational risk management

8 LEGAL AND COMPLIANCE RISK

8.1 Introduction

a) 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, related self regulatory organisation standards and codes of conduct applicable to its activities. Compliance risk can also exist when governing laws or rules related to specific institution products or activities may be ambiguous or untested.

b) Compliance laws, rules and standards generally cover matters such as observing regulatory requirements, proper standards of market conduct, managing conflicts of interest, treating customers fairly, and ensuring the suitability of customer advice.

c) 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.

d) Compliance risk, therefore, goes beyond what is legally binding and embrace broader standards of integrity and ethical conduct.

8.2 Compliance Risk Management

a) Every financial institution should ensure compliance with all relevant laws, rules and standards. The ultimate responsibility to ensure compliance rests with the Board of directors. As such, the board and senior management should allocate sufficient resources for compliance programs covering legal and compliance issues associated with the institution’s operations.

b) The board and management must recognise the scope and implications of laws and regulations that apply to their institutions. The board should understand the nature and level of compliance risk to which the institution is exposed and how its risk profile fits within the overall business strategy.

8.3 Board Oversight

a) The board of directors is responsible for ensuring a financial institution’s compliance with all relevant laws, rules and standards.

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

i. reviewing compliance and legal risk in order to minimize risk exposure;
ii. approving broad business strategies of the institution with respect to compliance and legal risk and ensuring that management takes the steps necessary to identify, measure, monitor, and control compliance and legal risk;
iii. approving policies that identify lines of authority and responsibility for managing legal and compliance risk; and
iv. delegating responsibility for establishing legal and compliance risk policies to the appropriate senior management committee.

8.3.1 Senior Management Oversight

a) Senior management should ensure that the structure of the institution's business and the level of legal and compliance risk it assumes are correctly aligned and effectively managed.

b) Management should establish a compliance function that is sufficiently independent from operations.

c) Management should ensure that the institution has adequate policies and procedures for managing legal and compliance and that it maintains clear lines of authority and responsibility for managing and controlling this risk.

d) The responsibilities of senior management include:

i. periodically reviewing the organization's legal and compliance risk management policies and procedures to ensure that they remain appropriate and sound;

ii. periodically update the board of directors regarding risk measurement, reporting, and management procedures;

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

iv. provide reasonable assurance, through the audit function, that all activities and all aspects of legal and compliance risk are covered by an institution's risk management process.

8.4 Policies and Procedures

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

a) Clearly define lines of authority of responsibility and accountability for compliance risk management decisions;
b) clearly define approvals necessary for exceptions to policies, limits, and authorizations;
c) Relationship of the Compliance function with other functions of the institution such as risk management and internal audit functions;
d) How responsibilities are shared and allocated among departments in the case where compliance responsibilities are carried out by staff in different departments;
e) Right to obtain access to information to carry out compliance duties effectively; and
f) Right to conduct investigations of possible breaches of compliance policy.

8.5 Compliance Risk Analysis

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

i. **Self assessment.** This is probably the most widely used tool and emphasizes the primary responsibility which senior 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.

ii. **Risk maps and process flows.** These two tools are widely used by internal audit and they can be very useful for reviewing compliance risk. 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.

iii. **Key indicators.** Senior management should develop risk indicators to assess the level of compliance risk by different business functions in the institution. The compliance indicators should reflect the nature of characteristics of each of the strategic business units. The 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.

iv. **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 given 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.

v. **Breach logs and near miss logs.** Keeping a log of regulatory breaches and near misses can be instructive if used positively. Analysis of the logs assists assessment of current mitigation policies and controls and senior management can gain comfort on the effectiveness of the compliance risk policies. Such logs can also be helpful in identifying trends and in assisting to focus resources.

vi. **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 minimization of regulatory risk in the institution as a whole. These may 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.

8.6 Compliance Risk Monitoring

Financial institutions should ensure that they have adequate management information system to effectively monitor compliance risk.

The monitoring function should:

i. identify, in a structured manner, the regulatory risks to which the 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; and

iii. meet the requirements for the conduct of comprehensive monitoring prescribed by the Central Bank through rules and guidance

8.6.1 Compliance Testing

a) **Compliance agenda**

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.

b) **Education, training and communication**

Effective education, training and regular communication are three essential elements of an effective compliance system. 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 training should cover:

i. monitoring techniques used by internal audit.
ii. scheduling compliance activities, effective communication, people and management skills.
iii. Conflict resolution

c) **Identifying and controlling danger areas**

Financial Institutions shall consider likely or known danger areas in respect of each compliance system that it establishes. Regular inspections shall be made and statistics for each danger area obtained. If anomalies show up, investigations should be made

promptly. There may well be a proper explanation, but pre-emptive action can prevent a lot of trouble.

d) **Effective monitoring**

Effective monitoring aims to check that people are doing what they ought to be doing and that the system is operating satisfactorily. Other purposes of monitoring are to:

i. ensure that the required procedures are being followed properly;
ii. help resolve difficulties at an early stage;
iii. serve as an early-warning device.
iv. See how the system is working in practice;
v. See if and where problems are being encountered, or are likely;
vi. Seek, and listen to, any suggestions for improvements; and
vii. Maintain communication.

e) **An effective compliant system** that maintains effective records is a valuable part of compliance systems and also act as an invaluable early-warning device.

8.7 Certifications

This involves requiring the compliance function to approve certain processes and business activities in order to minimize compliance risk. It has a number of advantages which include the following:

i. they draw attention to possible problem areas in a way that otherwise might not happen in a busy operating environment;
ii. they 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; and

8.8 Records, statistics and information technology

a) The important link in effective compliance is to keep valid and effective records and statistics, without allowing this to snowball into a bureaucratic nightmare. The record keeping period should be in compliance with the provisions of an applicable statute.

b) Information technology can be used in relation to monitoring, compliant handling, and statistics and records management.

8.9 Compliance Reporting

a) Financial institutions should ensure that they have a robust management information system that provides timely information reports on compliance.

Internal audit reports

b) The head of compliance should review audit reports and extract compliance risk information from these reports.

8.10 LEGAL RISK

a) Legal risk is the risk that a financial institution will conduct activities or carry out transactions in which they are inadequately covered or are left exposed to potential litigation.

b) As it is impossible to adequately address all aspects of liabilities that may be faced by a bank 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.

c) The legal risk management framework should provide an outline of the important issues that directors and/or executive staff of a financial institution may need to consider in ensuring due diligence in the operation of the financial institution as well as an overview of liability exposure against this risk.

d) 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 institution. The legal

function should be managed in an integrated manner with compliance to promote efficiency and effectiveness.

8.10.1 Policies and procedures

The board should approve the policies and procedures for managing legal risk which should provide for the following:

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

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

c) regular review and assessment of legal risk in the institution’s activities including new products;

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

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

f) maintenance of confidentiality provisions.

9 STRATEGIC RISK

9.1 Introduction

a) Strategic risk refers to the current and/or prospective impact on a bank's earnings, capital or business viability arising from adverse business decisions and implementation of strategies which are inconsistent with internal factors and the external environment.

b) Strategic risk management enables the mitigation of risks and protects the stability of a bank. It also acts as a tool for planning systematically about the future and identifying opportunities. In addition strategic risk management assists in effective utilization of capital and can be used to turn strategic threats into growth opportunities.

c) In order to effectively manage strategic risk, the board of directors and senior management should establish appropriate internal structures for implementation of strategic plans. At a minimum every banking institution should have strategic plans which should be supported by appropriate organisational and functional structures, skilled and experienced personnel, an adequate budget, management information systems, as well as risk monitoring and controlling systems.

d) In this guideline, a strategic plan is defined as a roadmap indicating the vision, mission and the business direction of a banking institution, generally for a period of at least one year. A good strategic plan must be consistent with the organisational goals and should be adjustable to changing environmental factors.

e) On the other hand, an operational plan specifies the overall operational framework of a banking institution required to support successful implementation of a strategic plan and acts as a guideline for each business unit to set an action plan. Generally, an operating plan is a short-term plan, not exceeding one year, comprising goals, budgeted profits, responsibilities, resources to be used, work timeframe, and monitoring criteria for performance

9.2 Common Sources of Strategic Risk

a) Strategic risk arises from two main sources, namely, **external risk factors** and **internal risk factors.**

b) **External risk factors** are events which a banking institution has no control over, which negatively affect the effective implementation of a strategic plan. The following are some of the external factors which affect strategic planning and implementation by banking institutions:

i. industry competition;
ii. behavioral change of target customers;
iii. technological changes and developments;
iv. economic factors; and
v. regulations.

c) **Internal risk factors** are those, which can be controlled by a banking institution but can, affect or deter the effective implementation of a strategic plan. Examples of internal factors include the following:

i. organisational structure;
ii. work processes and procedures;
iii. adequacy and quality of personnel;
iv. adequacy of information for decision-making ; and technology.

9.3 Strategic planning process

a) 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 financial institution to strategic risk.

b) Every institution should have an appropriate strategic planning process encompassing the following:

i. support or participation of the board, delegated committees, and senior management;

ii. participation of staff from various departments;

iii. adequacy of information in developing assumptions in relation to economic factors, position of the financial institution compared to competitors, current competitive position, future market trends and customer needs, among others;

iv. consistency of the operational plans with the overall objective of a financial institution, and

v. assessment of actual performance against strategic plans.

9.4 Risk Mitigation Factors

Financial 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.

9.5 Board Oversight

(a) Board of Directors 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 financial institution's strategic plan.

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

i. ensure that risk management practices are an intrinsic part of strategic planning;

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

iii. ensure that the financial institution's overall strategic risk exposure is maintained at prudent levels, and is compatible with developed business strategies;

iv. 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;

v. assess management's success in implementing the financial institution's strategic plan and achieving targets and results;

vi. 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

vii. 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.

9.5.1 Senior Management Oversight

Senior management has 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 financial institution's strategic plan and how such risks fit within the overall business strategies.

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

i. ensure that a comprehensive Strategic Risk Management process that is commensurate with the strategic goals of the financial institution is in place;

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

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

iv. 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.

9.6 Policies, Procedures & Limits

a) Effective management of strategic risk requires that the financial institution establishes prudent policies, procedures and limits approved by the Board to ensure its objective evaluation and responsiveness to the financial institution's business environment.

b) Policies and procedures should cover all material risks associated with the financial institution's business segments defined in the strategic plan.

c) Accountability should be spelt out clearly and lines of authority for all the financial 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.

d) The policies should establish clear guidelines on frequency and procedures for review of its business strategies. Policies should be consistent with the organization's broader

business strategies, capital adequacy, technical expertise and risk tolerance. It should take into account the size, nature and complexities of the financial institution's business plans and consider past experiences and performances.

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

i. the institution's inherent strengths;
ii. its identified weaknesses;
iii. opportunities external to the institution; and
iv. external factors that pose threats to the institution.

f) 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 financial institution's exposure to various quantifiable risks associated with its strategic plan.

g) 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:

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

9.7 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 timeously identify and measure the risks associated with the financial institution's strategic plan. In general the MIS should enable management to monitor:

i. current and forecasted economic conditions, e.g., economic growth, inflation, foreign exchange trends, etc.
ii. current and forecasted industry and market conditions, such as;

iii. increasing competition by new market entrants;
iv. number and size of mergers and acquisitions;
v. changing customer behavior;
vi. new products/substitutes;
vii. exposure to different sectors, and associated sector risks; and
viii. mechanisms that are in place to detect exceptions to limits and guidelines.

9.8 Internal Controls and Audit

i. A financial institution's internal control structure is critical to the safe and sound functioning of the organization generally and the management of the financial institution's strategic direction in particular. Financial institutions need strong internal control systems to ensure that they are not unduly exposed to strategic risks. Internal controls are required to ensure that:

i. the organization's structure establishes clear lines of authority;

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

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

b) Internal and external audits are integral to the implementation of a risk management process to control risk associated with a financial institution's business strategy.

ii. A financial 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.

iii. 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.

10 REPUTATION RISK

10.1 Introduction

a) Reputation risk means the risk that a bank's reputation is damaged by one or more than one reputation event, as reflected from negative publicity about its business practices, conduct or financial condition. Such negative publicity, whether true or not, may impair public confidence in the bank, result in costly litigation, or lead to a decline in its customer base, business or revenue.

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

i. **Corporate reputation risk** which relates to a financial 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 financial 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 financial institution.

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

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

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

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

10.2 Categories of Reputation Risk

Financial 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.

10.3 Roles and Responsibilities

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

b) The financial 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.

c) 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 financial institution's reputation within the market place.

10.4 Policies and Procedures

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

a) Adopt sound risk management practices that include the practice of building good reputation and earning the goodwill of key stakeholders;

b) Manage reputation risk through a process of anticipation, risk analysis and planning, and then attempting to manage both internal and external expectations;

c) Measure trends in a financial institution's reputation as a precursor to remedial action; and

d) Identify risk events as being either specific or systemic as this will determine the course of corrective action.

10.5 Reputation Risk Management and Monitoring

a) Management should exploit opportunities to grow a financial institution's reputation capital. Positive information about a financial institution should also be communicated appropriately to the market place. Management should be fully aware of events that have the potential to impact a financial institution's reputation.

b) All material events should immediately be escalated to the Compliance or Risk Manager, Managing Director or Public Relations. A financial institution should ensure that it establishes a crisis management procedure to manage potential impact of reputation events. Financial institution should also ensure that there is no general release of information to the public, press without approval from senior management.

c) 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.

d) 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.

10.6 Risk Methodology Components

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

b) 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 financial institution should incorporate both subjective and objective risk standards in the risk template.

10.7 Reputation Risk Analysis Methodology and Process

a) Every financial 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 financial

institution to uncover the key risk factors with high likelihood to give rise to reputation risk.

b) 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.

c) Reputation risk management should continue on an on-going basis. Every financial 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 financial institution with special training regarding potential high risk areas.

d) Finally, all aspects of reputation risk management should be subject to internal audit review.

11 INTERNET AND TECHNOLOGICAL RISK MANAGEMENT

11.1 Introduction

a) Continuing technology developments and innovations are having significant impact on the way banks interact with their customers, suppliers and counterparties, and how they undertake their operations. Banks face the challenge of adapting, innovating and responding to the opportunities posed by computer systems, telecommunications, networks and other technology-related solutions to drive their businesses in an increasingly competitive domestic and global market.

b) The internet in particular offers major opportunities for banks to reach new markets and expand the range of products and services they provide to customers. The very accessibility and dynamism of the internet brings both benefits and risks. Due to the open and complex nature of the internet, the risks associated with using this infrastructure for electronic banking are accentuated. Banks should take this factor into account in their risk management process.

c) Technology risks relate to any adverse outcome, damage, loss, disruption, violation, irregularity or failure arising from the use of or reliance on computer hardware, software, electronic devices, and online networks and telecommunications systems. These risks can also be associated with systems failures, processing errors, software defects, operating mistakes, hardware breakdowns, capacity deficiencies, network vulnerabilities, control weaknesses, security shortcomings, internal sabotage, espionage, malicious attacks, hacking incidents, fraudulent conduct and defective recovery capabilities.

d) As banks rely increasingly on information technology and the internet to operate their business and interact with the markets, their awareness and recognition of the magnitude and intensification of technology risks should correspondingly be more perceptive and discerning, both for individual banks and the financial industry as a whole. All banks providing internet banking must erect a sound and robust risk

management process that will enable them to identify, assess, measure and respond to technology risks in a proactive and effective manner.

11.2 Board and Senior Management Oversight

a) The board of directors and management of a bank are responsible for managing its risks, including technology risks which are becoming more complex, dynamic and pervasive. The risk management process requires the board and management to review and appraise the cost-benefit issues on what and how much to invest in controls and security measures relating to computer systems, networks, data centres, operations and backup facilities To this end, senior management should establish an effective technology risk management framework. This normally comprises IT governance, a continuous technology risk management process, and implementation of sound practices in respect of IT controls.

b) As a general principle, a risk management framework would require the following actions to be taken:

i. Identify, classify and assess risks that are relevant to the bank's operations and systems.

ii. Develop a documented plan containing policies, practices and procedures that address and control these risks.

iii. Implement and regularly test the plan.

iv. Monitor risks and the effectiveness of the plan on an ongoing basis.

c) A sound and robust risk management framework requires the board and management to be responsible and accountable for managing and controlling technology risks. This responsibility calls for banks to perform risk analysis by identifying information systems assets, determining security threats and vulnerabilities, estimating the likelihood of exploitation or attacks, assessing potential losses associated with these risk events and taking appropriate security measures and controls for asset protection.

11.3 IT Control Policies

a) Achieving a consistent standard of sound practices for IT controls across a banking institution requires clear direction and commitment from the Board and senior management. In this connection, senior management, who may be assisted by a delegated sub-committee, is responsible for developing a set of IT control policies which establish the ground rules for IT controls. These policies should be formally approved by the Board or its designated committee and properly implemented among IT functions and business units.

b) Policies, procedures and practices to define risks, stipulate responsibilities, specify security requirements, implement safeguards to protect information systems, administer internal controls and enforce compliance should be set up as essential specifications of the risk framework.

c) IT control policies should be reviewed regularly, and where necessary updated to accommodate changing operating environments and technologies.

d) Senior management should ensure that processes used to verify compliance with IT control policies and the process for seeking appropriate approval for dispensation from IT control policies are specified clearly. Senior management should also define the consequences associated with any failure to adhere to this process. In general, the responsibility for ensuring compliance with IT control policies and the process for seeking dispensation rests with individual business units and IT functions, with the assistance of the technology risk management function

e) Senior management may put in place mechanisms (e.g. periodic reminders for relevant staff and policy orientation for new recruits) to promote awareness of IT control policies among relevant personnel on a regular basis.

11.4 Oversight and Organisation of IT Functions

a) Senior management should establish an effective organisation of IT functions to deliver technology services and to provide day-to-day technology support to business

units. A clear IT organisation structure and related job descriptions of individual IT functions should be documented and approved by senior management.

b) Proper segregation of duties within and among various IT functions is crucial for ensuring an effective IT control environment. In the event that a bank finds it difficult to segregate certain IT control responsibilities, it should put in place adequate compensating controls (e.g. peer reviews) to mitigate the associated risk.

c) It is recommended that banks establish an IT planning or steering committee which oversees whether IT resources are used effectively to support business strategies. This committee should normally consist of representatives of senior management, key business units and IT functions. It should meet regularly and report to senior management, and where appropriate to the Board or its designated committee on the status of major technology-related initiatives and any material IT-related issues.

d) In general, the IT planning or steering committee should also be responsible for developing an IT strategy to cover longer and short-term technology-related initiatives, taking into account new business initiatives, organizational changes, technological evolution, regulatory requirements, staffing and control related issues. The IT strategy should be formally documented, endorsed by the Board or its designated committee and senior management, as well as reviewed and updated at least on an annual basis.

11.5 Technology Risk Management Function

a) Banking institutions should have in place effective risk management systems and that new products and services should be subject to careful evaluation (including a detailed risk assessment) as well as a post-launch review. The same risk management controls apply to the technology risk management of banks.

b) Senior management should establish clearly which function in the banking institution is responsible for implementing and managing the technology risk management process (the TRM function). Depending on the business and operational needs of individual banks, the TRM function may refer to a dedicated department of a bank, or

a group of departments or support units collectively performing the roles defined for this function.

c) The TRM function has a role to assist business units and IT functions in performing the technology risk management process which identifies, measures, monitors and controls technology-related risks. In addition, this function helps to ensure awareness of, and compliance with, the bank's IT control policies, and to provide support for investigation of any technology-related frauds and incidents.

d) The TRM function should formulate a formal technology risk acknowledgement and acceptance process for reviewing, evaluating and approving any major incidents of non-compliance with IT control policies. Typical reasons for such non-compliance are technology limitations (e.g. certain proprietary operating systems are only able to provide primitive password controls), business constraints (e.g. undesirable impact on customer services) and the costs outweighing the associated benefits. The process includes:

i. a description of the risk being considered for acknowledgement by the owner of the risk and an assessment of the risk that is being accepted;
ii. identification of mitigating controls;
iii. formulation of a remedial plan to reduce the risk; and
iv. approval of the risk acknowledgement from the owner of the risk and senior management.

11.6 Technology Audits

a) As regards technology audits, banks are expected to assess periodically their technology risk management process and IT controls. To ensure adequate coverage of the IT control environment and critical computer systems, an annual technology audit plan should be developed. Banks should also ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.

b) It is recognised that the internal audit function of some banks may find it difficult to build up in-house technology audit expertise. In these circumstances, technology audit

support may be supplemented by external specialists or internal technology auditors of other offices of the same banking group.

11.7 Staff Competence and Training

a) Given the rapid pace of technological development, senior management needs to ensure that staff of IT functions, the TRM function and internal technology auditors is competent and able to meet required levels of expertise and experience on an ongoing basis. It is also important to ensure that staffing levels are sufficient to handle present and expected work demands, and to cater reasonably for staff turnover.

b) To ensure that an adequate training programme is in place for IT personnel, it is essential to establish a process to identify any material skill gaps of staff of technology-related functions. Banks may encourage and, where appropriate, facilitate their staff to acquire relevant professional qualifications, such as for those who are responsible for security management, technology risk management and technology audits.

11.8 IT Support Provided by Overseas Offices

a) Some banks may rely upon or work with their overseas offices (e.g. parent banks, subsidiaries, head offices or other regional offices of the same banking group) with regard to certain IT controls or support activities. Senior management should ensure that the respective responsibilities of the local and overseas offices in these areas are clearly set out in the relevant documents (e.g. policies, procedures or service agreements).

11.9 Security Management

11.9.1 Information Classification and Protection

a) For each application system, banks should preferably assign an individual as the information owner. The information owner normally needs to work with the TRM and IT functions to ensure confidentiality and integrity of information, and to protect the information in accordance with the level of risk present and envisaged.

b) Information can be classified into different categories according to the degree of sensitivity (e.g. highly sensitive, sensitive, internal and public) to indicate the extent of protection required. To aid the classification process, banks should ideally develop guidelines and definitions for each classification and define an appropriate set of procedures for information protection in accordance with the classification scheme. The level of detail of the information classification scheme adopted should be practicable and appropriate to banks' circumstances.

c) Protection of information confidentiality should be in place regardless of the media (including paper and electronic media) in which the information is maintained. Banks should ensure that all media are adequately protected, and establish secure processes for disposal and destruction of sensitive information in both paper and electronic media.

d) If cryptographic technology is used to protect the confidentiality and integrity of banks' information, banks should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys. Sound practices of key management generally include:
    i. provision of a secure control environment for generation, distribution, storage, entry, use and archiving of cryptographic keys to safeguard against modification and unauthorized disclosure. In particular, the use of tamper-

resistant storage is recommended to prevent the disclosure of the cryptographic keys; and

ii. adequate off-site back-up and contingency arrangements for cryptographic keys which are subject to the same security controls as the production cryptographic keys.

11.9.2 Authentication and Access Control

a) Access to the information and application systems should be restricted by an adequate authentication mechanism associated with access control rules. Access control rules determine what application functions, system resources and data a user can access. For each application system, all users should be identified by unique user-identification codes (e.g. user IDs) with appropriate method of authentication (e.g. passwords) to ensure accountability for their activities.

b) Banking institutions should implement effective password rules to ensure that easy-to-guess passwords are avoided and passwords are changed on a periodic basis. Stronger authentication methods should be adopted for transactions/activities of higher risk (e.g. payment transactions, financial messages and mobile banking). These usually entail multiple factors for user authentication which combine something one knows (e.g. passwords) and something one has (e.g. a smart card or hardware security tokens).

c) Extra care should be exercised when controlling the use of and access to privileged and emergency IDs. The necessary control procedures include:

   i. granting of authorities that are strictly necessary to privileged and emergency IDs; formal approval by appropriate personnel prior to being released for usage;

   ii. monitoring of the activities performed by privileged and emergency IDs (e.g. peer reviews of activity logs);

   iii. proper safeguard of privileged and emergency IDs and passwords (e.g. kept in a sealed envelope and locked up inside the data centre); and

iv. change of privileged and emergency IDs' passwords immediately upon return by the requesters.

11.9.3 Security Administration and Monitoring

a) A security administration function and a set of formal procedures should be established for administering the allocation of access rights to system resources and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities. In particular, the function should cover the following areas:
   i. granting, changing and removing user access rights subject to proper approval of the information owners. In particular, proper procedures should be in place to ensure that a user's relevant access rights are removed when he leaves the bank or when his job responsibilities no longer require such rights;
   ii. ensuring the performance of periodic user access re-certification (e.g. on an annual basis) that confirms whether user access rights remain appropriate and obsolete user accounts have been removed from the systems;
   iii. reviewing security logs and violation reports in a timely manner; and
   iv. performing incident analysis, reporting and investigation.

b) Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be in place to mitigate the risk of unauthorized activities being performed by the security administration function.

c) Banks should establish incident response and reporting procedures to handle information security-related incidents during or outside office hours. The incident response and reporting procedures should include timely reporting to the CBL of any confirmed IT-related fraud cases or major security breaches.

11.9.4 System Security

a) Control procedures and baseline security requirements should be developed to safeguard application programs, operating systems, system software and databases. The following to be noted:

i. deploy hardened operating systems – systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of updates, patches and enhancements recommended by system vendors; change all default passwords for new systems immediately upon installation.

ii. access to data and programs should be controlled by appropriate methods of identification and authentication of users together with proper authorization;

iii. integrity of static data (e.g. system parameters) should be periodically checked to detect unauthorized changes;

iv. clear responsibilities should be established to ensure that the necessary patches and security updates developed from time to time by relevant vendors are identified, assessed, tested and applied to the systems in a timely manner;

v. all configurations and settings of operating systems, system software, databases and servers should be adequately documented.

vi. Periodic certifications of the security settings should be performed (e.g. by the TRM function or the technology audit function); and adequate logging and monitoring of system and user activities should be in place to detect anomalies, and the logs should be securely protected from manipulation.

vii. Install firewalls between internal and external networks as well as between geographically separate sites.

viii. Install intrusion detection-prevention devices (including denial-of-service security appliances where appropriate).

ix. Develop built-in redundancies for single points of failure which can bring down the entire network.

x. Perform application security review using a combination of source code review, stress loading and exception testing to identify insecure coding techniques and systems vulnerabilities.

xi. Engage independent security specialists to assess the strengths and weaknesses of internet-based applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff who are operationally or functionally responsible for the system or activity.

xii. Establish network surveillance and security monitoring procedures with the use of network scanners, intrusion detectors and security alerts.

11.9.5 End-User and Mobile Computing

a) The internet is a global network which is intrinsically insecure. Security threats arising from denial of service attacks, spamming, spoofing, sniffing, hacking, key logging, middleman interception, mutating virus, worms etc, pose heightened technology risk levels which banks encounter with increasing frequency and malignancy. It is imperative that banks implement strong security measures that can adequately address and control these types of risks and security threats. This would require a security strategy to be established to enable the following objectives to be met: data confidentiality, system integrity, system availability, customer and transaction authenticity and customer protection.

b) While end-user computing may offer advantages (e.g. higher productivity) to a bank, it may also increase the difficulty in controlling the quality of, and access to, the system. Banking institutions should where necessary, therefore, establish control practices and responsibilities with respect to end user computing to cover areas such as data security, documentation, data/file storage and back-up, system recovery, audit responsibilities and training.

c) Controls over mobile computing are required to manage the risks of working in an unprotected environment. In protecting banks' information, banks should establish control procedures covering:

i. an approval process for user requests for mobile computing;

ii. authentication controls for remote access to networks, host data and/or systems;

iii. protection (e.g. against theft and malicious software) of equipment and devices for mobile computing;

iv. use of data encryption software to protect sensitive information and business transactions in the mobile environment and when being transmitted; and

v. back-up of data and/or systems in the mobile computing devices.

d) Software and information processing facilities are vulnerable to attacks by computer viruses and other malicious software. Procedures and responsibilities should be established to detect and prevent attacks. Banks should put in place adequate controls such as:

i. prohibiting the download and use of unauthorized files and software, and the access to doubtful web sites;

ii. installation and timely update of anti-virus software provided by reputable vendors;

iii. disallowing the download of executable files, and mobile codes, especially those with known

iv. vulnerabilities (e.g. through the use of corporate firewalls and proper configuration of the browser software); and

v. prompt and regular virus scanning of all computing devices and mobile users' computers, and procedures for recovering from virus infections.

11.9.6 Bank Disclosure

a) Banks should provide clear information to their customers about the risks and benefits of using internet banking before they subscribe to internet banking services.

b) Customers should be informed clearly and precisely on the respective rights, obligations and responsibilities of the customers and the bank on all matters relating to online transactions, and in particular, any problems that may arise from processing errors and security breaches.

c) Banks should publish their customer privacy and security policy. Customer dispute handling, reporting and resolution procedures, including the expected timing for the

banks' response, should also be clearly defined. All this information should be posted on the banks' websites.

11.9.7 Customer Education

a) The importance of educating customers on the security and reliability of their interaction with the bank should not be underestimated. Customer's confidence in the safety and soundness of the bank's online products and services depends to a large extent on their understanding of and compliance with the security requirements connected with the operation of their banking accounts and transaction services.

b) Customer education may include web-based online education or other media whereby a guided learning experience may be defined. When new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, the bank should ensure that customers have sufficient instruction and information to be able to properly utilise the banking services.

11.9.8 Physical and Personnel Security

a) Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access. Critical information processing facilities should be housed in secure areas such as data centres and network equipment rooms with appropriate security barriers and entry controls. Access to these areas should be restricted to authorized personnel only and the access rights should be reviewed and updated regularly. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities.

b) Banks should consider fully the environmental threats (e.g. proximity to dangerous factories) when selecting the locations of their data centres. Moreover, physical and environmental controls should be implemented to monitor environmental conditions

which could affect adversely the operation of information processing facilities (e.g. fire, explosives, smoke, temperature, water and dust). Equipment and facilities should be protected from power failures and electrical supply interference by, for example, installing uninterruptible power supply (UPS) and a backup generator.

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

d) Security awareness, training and education programmes should also be conducted internally and externally to promote and nurture a security conscious environment.

11.10 System Development and Change Management

11.10.1 Project Management

a) Banks should establish a general framework for management of major technology-related projects. This framework should, among other things, specify the project management methodology to be adopted and applied to these projects.
b) The methodology should cover, at a minimum, allocation of responsibilities, activity breakdown, budgeting of time and resources, milestones, check points, key dependencies, quality assurance, risk assessment and approvals.

11.10.2 Project Life Cycle

a) Banks should adopt and implement a full project life cycle methodology governing the process of developing, implementing and maintaining major computer systems. In general, this should involve phases of project initiation, feasibility study, requirement definition, system design, program development, system and acceptance testing, training, implementation, operation and maintenance.

b) The project life cycle methodology should define clearly the roles and responsibilities for the project team and the deliverables from each phase. It also needs to contain a process to ensure that appropriate security requirements are identified when formulating business requirements, built during program development, tested and implemented.

c) An independent party (e.g. the quality assurance function, the TRM function or the technology audit team), which is not involved in the project development, should conduct a quality assurance review of major technology-related projects, with the assistance of the legal and compliance functions if necessary. This review is to ensure compliance with the project life cycle methodology, other internal policies, control requirements, regulations and applicable laws.

d) A formal acceptance process should be established to ensure that only properly tested and approved systems are promoted to the production environment. System and user acceptance testing should be carried out in an environment separated from the production environment. Production data should not be used in development or acceptance testing unless the data has been desensitized (i.e. not disclosing personal or sensitive information) and prior approval from the information owner has been obtained. Performance testing should also be performed before newly developed systems are promoted to the production environment.

e) Software package acquisition is an alternative to in-house systems development and should be subject to broadly similar controls as the project life cycle. As inappropriate handling of software licences may expose banks to a significant risk of patent infringement, and financial and reputation losses, banks should establish a formal software package acquisition process. In particular, the process should involve detailed evaluation of the software package (e.g. in terms of software licence, functionality, system performance and security requirements) and its supplier (e.g. its financial condition, reputation and technical capabilities).

f) Banks should ensure that on-going maintenance and adequate support of software packages are provided by the software vendors and are specified in formal contracts. For mission-critical software packages, banks may consider including in the contracts an escrow agreement, which allows them to obtain access to the source code of the software packages under certain circumstances, such as when the software vendors cease their business.

11.10.3 Change Management

a) Change management is the process of planning, scheduling, applying, distributing and tracking changes to application systems, system software (e.g. operating systems and utilities), hardware, network systems, and other IT facilities and equipment. An effective change management process helps to ensure the integrity and reliability of the production environment.

b) Banks should develop a formal change management process that includes:
   i. classification and prioritisation of changes and determination of the impact of changes;
   ii. roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel;
   iii. program version controls and audit trails;
   iv. scheduling, tracking, monitoring and implementation of changes to minimise business disruption;
   v. a process for rolling-back changes to re-instate the original programs, system configuration or data in the event of production release problems; and
   vi. a post implementation verification of the changes made (e.g. by checking the versions of major amendments).

c) To enable unforeseen problems to be addressed in a timely and controlled manner, banks should establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner (for application system or

production data related changes) and other relevant parties at the time of change. If the change needs to be introduced as a matter of urgency and it is impracticable to seek the approval of the information owner, endorsement should be sought from the information owner after the implementation as soon as practicable (e.g. on the following business day).

d) Emergency changes should be logged and backed up (including the previous and changed program versions and data) so that recovery of previous program versions and data files is possible if necessary. Emergency changes need to be reviewed by independent personnel to ensure that the changes are proper and do not have an undesirable impact on the production environment. They should be subsequently replaced by proper fixes through the normal acceptance testing and change management procedures.

11.11 Information Processing

11.11.1 IT Operations Management and Support

a) Management of IT functions should ideally formulate a service level agreement with business units to cover system availability and performance requirements, capacity for growth, and the level of support provided to users. The responsible IT functions should ensure that adequate procedures are in place for managing the delivery of the agreed technology support and services.

b) Detailed operational instructions such as computer operator tasks, and job scheduling and execution (e.g. instructions for processing information, scheduling requirements and system housekeeping activities) should be documented in an IT operations manual. The IT operations manual should also cover the procedures and requirements for on-site and off-site back-up of data and software in both the production and development environments (e.g. the frequency, scope and retention periods of back-up).

c) Banks should have in place a problem management system to respond promptly to IT operational incidents, to escalate reported incidents to relevant IT management staff and to record, analyse and keep track of all these incidents until rectification of the incidents. A helpdesk function can be set up to provide front-line support to users on all technology-related problems and to relay the problems to relevant IT functions for investigation and resolution.

11.11.2 Performance Monitoring and Capacity Planning

a) Banks should implement a process to ensure that the performance of application systems is continuously monitored and exceptions are reported in a timely and comprehensive manner. The performance monitoring process should include forecasting capability to enable problems to be identified and corrected before they affect system performance. This process should help the preparation of workload forecasts to identify trends and to provide information needed for the capacity plan, taking into account planned business initiatives.

b) Capacity planning should be extended to cover back-up systems and related facilities in addition to the production environment.

11.12 IT Facilities and Equipment Maintenance

a) To ensure the continued availability of banks' technology related services, banks should maintain and service IT facilities and equipment (e.g. computer hardware, network devices, electrical power distribution, UPS and air conditioning units) in accordance with the industry practice, and suppliers' recommended service intervals and specifications.

b) Proper record keeping (including suspected or actual faults and preventive and corrective maintenance records) is necessary for effective facility and equipment maintenance. A hardware and facility inventory should be kept to control and track all

hardware and software purchased and leased. These records can also be used for regular inventory taking.

11.13 Disaster Recovery and Business continuity

a) As part of the risk control framework, disaster recovery and business continuity planning is crucial in the development and preparation of contingency arrangements for restoring and resuming critical business operations in the aftermath of a disaster occurring at the primary computer processing site. No system is infallible or immune from mishaps. Hence, effective means to rapid recovery is critical.

b) A bank must identify comprehensively what types of disasters are catered for in the recovery plan. Disasters can range from a total loss of service due to a natural disaster to a catastrophic system failure caused by system faults, hardware malfunction or operating errors. A substantial task in disaster recovery planning is putting together a reliable assemblage of contingency operating procedures that cover varying scenarios of operational disruption or system breakdown.

c) A recovery site geographically separate from the primary site must be established to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site. A hot-site rapid recovery capability should be created and maintained. The required speed of recovery will depend on the criticality of resuming business operations, the type of online services and whether there are alternative ways and processing means to maintain adequate continuing service levels to satisfy customers.

d) Incident response, disaster recovery and business continuity preparations need to be regularly reviewed, updated and tested to ensure their effectiveness and that responsible staff are capable of undertaking emergency and recovery procedures when required. Recovery preparedness should fully anticipate a total shutdown or incapacitation of the primary computer site.

e) Banks which have networks and systems linked to specific service providers and vendors should conduct bilateral or multilateral recovery testing and ensure inter-dependencies are also fully catered for.

11.14 Communications Networks

11.14.1 Network Management

a) Communications networks convey information and provide a channel of access to application systems and systems resources. Given their technical complexity, communications networks can be highly vulnerable to disruption and abuse. Safeguarding communications networks requires robust network design, well-defined network services and sound discipline to be observed in managing networks.

b) Overall responsibility for network management should be clearly assigned to individuals who are equipped with the know-how, skills and resources to fulfil their duties. Network standards, design, diagrams and operating procedures should be formally documented, kept up-to date, communicated to all relevant network staff and reviewed periodically.

c) Communications facilities that are critical to continuity of network services should be identified. Single points of failure should be minimised by automatic re-routing of communications through alternate routes should critical nodes or links fail (e.g. routing critical links to more than one external exchange or switching centre, and prearranging services with alternate telecommunications service providers).

d) The network should be monitored on a continuous basis. This would reduce the likelihood of network traffic overload and detect network intrusions. Monitoring activities include:

   i. monitoring network services and performance against pre-defined targets;
   ii. reviewing volumes of network traffic, utilisation of network facilities and any potential bottlenecks or overloads; and
   iii. detection of unusual network activities based on common attack characteristics.

e) Powerful network analysis and monitoring tools, such as protocol analysers, network scanning and sniffer tools, are normally used for monitoring network performance and detecting potential or actual intrusions. These powerful network tools should be

protected from unauthorized usage (e.g. viewing of unencrypted sensitive information). The use of network tools should also be tightly restricted to authorized staff only and be subject to stringent approval and review procedures.

11.14.2 Network Security and Certification

a) To prevent insecure connections to a bank's network, procedures concerning the use of networks and network services need to be established and enforced. These should cover:

a) the available networks and network services;
b) authorization procedures for determining who is allowed to access particular networks and network services; and
c) controls and procedures to protect access to network access points, network connections and network services.

b) Banks should consider segregating internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment. For instance, the production systems should be located in dedicated network segments separated from other segments so that production network traffic is segregated from other traffic (e.g. connections to the internet, extranet connections to external parties and market data feeds). Sensitive data traffic between different network segments should be properly controlled and protected from being tampered with.

c) Regular reviews of the security parameter settings of network devices such as routers, firewalls and network servers are required to ensure that they remain current. Audit trails of daily activities in critical network devices should be maintained and reviewed regularly. Network operational personnel should be alerted on a real-time basis to potential security breaches.

d) Network certification should be conducted when requesting local area network (LAN)/wide area network (WAN) additions or changes to banks' corporate network. The additions or changes cover dial-in/out ports, switches, terminal servers,

gateways/servers, routers, extranets and the public internet. The network certification process includes gathering data about the network environment, analysing any points of vulnerability and associated controls, and documenting whether approval is given or what additional controls are required for approval of connectivity.

11.14.3 Wireless Local Area Network

a) If wireless local area networks (WLANs) are to be deployed, banks should develop policies and procedures for approval, installation, operation and administration of WLANs. A risk assessment process for evaluating the sensitivity of information to be accessible via a WLAN should be formulated before a WLAN can be implemented. Banks should also develop a standard security configuration for WLAN products and follow the network certification process to ensure that WLANs are implemented in a secure manner so that they do not expose the corporate network to unmanaged risks.

b) Additional security measures may be needed between the wireless workstations and the wired network to provide stronger encryption and mutual authentication. WLANs should be segregated from the corporate network (e.g. by firewalls) to prevent any unauthorized access to the corporate network via WLANs.

11.15 Management of Technology Service Providers

11.15.1 Management of Technology Outsourcing

a. In internet banking, and critical technological systems, it has become quite common for banks to outsource some or all of their computer processing, systems and administrative operations to third party service providers, hardware and software vendors, telecommunications companies, specialist firms and other support operators (generically and collectively regarded as service providers)

b. The board and senior management must fully understand the risks associated with outsourcing its internet banking operations. Before a service provider is appointed, due

diligence should be carried out to determine its viability, capability, reliability, track record and financial position.

c. The management of technology outsourcing requires banking institutions to observe the following controls:

i. technology service providers should have sufficient resources and expertise to comply with the substance of the banks' IT control policies;

ii. in case of outsourcing of critical technology services (e.g. data centre operations), banks are expected to commission a detailed assessment of the technology service provider's IT control environment. The assessment should ideally be conducted by a party independent of the service provider.

iii. the contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all the contracting parties should be carefully and properly defined in written agreements. The substance covered in the agreements would usually include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

iv. banks technology service providers may further sub-contract their services to other parties, banks should consider including a notification or an approval requirement for significant sub-contracting of services and a provision that the original technology service provider is still responsible for its sub-contracted services;

v. unless acceptable arrangements have been made and mutually agreed, the service provider should be required to provide access to all parties nominated by the bank to its systems, operations, documentation and facilities to carry out any review or assessment for regulatory, audit or compliance purpose. Notwithstanding the foregoing, the power of regulatory authorities under the Financial Institutions Act to carry out any inspection, supervision or examination of the service provider's role, responsibilities, obligations, functions, systems and facilities must be recognised in the agreements.

vi. further to the regular monitoring activities, banks should conduct an annual assessment to confirm the adequacy of the IT control environment of the provider of critical technology services;

vii. Banks should develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the technology service provider. This may include an exit management plan and identification of additional or alternate technology service providers for such support and services.

11.15.2 Management of Other Technology Service Providers

a) Apart from technology outsourcing, banks may rely on some outside technology service providers in the provision of technology-related support and services (e.g. telecommunications and network operators).

b) Banks should have in place guidelines on how to manage different kinds of major outside technology service providers covering the selection process of service providers, the process for approving material exceptions, and the need to avoid over-reliance upon a single technology service provider in
critical technology services.

NOTES