BANK LICENSING, SUPERVISION & SURVEILLANCE

GUIDELINE No. 1 - 2006/BSD

RISK MANAGEMENT

TABLE OF CONTENTS

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, liquidity, market, price, interest rate and legal 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 circumstances so catastrophic that the institutions cannot remain in business.

1.3 Traditionally, risk in banking institutions has been considered primarily from an operational point of view. Attention to risk other than operational risk has mainly been directed towards credit and interest rate risk.

1.4 It is clear, however, that attention to all types of risk is critical. Inadequate risk management can expose a bank to litigation, financial loss or damage to its reputation. Therefore, it is imperative that banks take the responsibility to carefully evaluate all types and levels of risk in their business operations and activities.

1.5 To facilitate a consistent approach to risk management and the adoption of international best practice, the Reserve Bank has prepared this set of guidelines which provides minimum requirements for sound risk management practices. These guidelines encompass the management of strategic, credit, market, liquidity operational, legal and compliance and reputational risks; and include guidelines on sound internal controls. The Reserve Bank expects banks to have an integrated approach to managing risk that adequately identifies, measures, monitors and controls risk.

1.6 These guidelines emphasise four key pillars of a sound risk management framework, namely, adequate board and senior management oversight, sound risk management policies and operating procedures, adequate management information systems, strong risk measurement, monitoring and control capabilities and adequate internal controls.

1.7 The principles recommended in these guidelines, which are based on best practices, are not intended to be exhaustive or to prescribe a uniform set of risk management requirements for all institutions. Institutions should note that the sophistication of the process, and internal controls used to manage risks, depends on the nature, scale and complexity of their activities.

1.8 Nevertheless, operational interdependencies and market forces result in substantial integration of functions among institutions. This gives rise to a high degree of commonality in the risk management challenges faced. As such, these guidelines are expected to have broad applicability. At the same time, institutions should also take into account relevant regulatory requirements and industry standards where applicable.

1.9 While the guidelines are organised by risk type, it is important to note that causal relationships exist between risk types, as well as different risk types manifesting themselves concurrently in a given situation. As such, banking institutions should have an enterprise-wide risk management framework designed to manage risks in an institution's activities on an aggregate basis.

1.10 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.

1.11 The nature of banking business requires sound internal controls. It is against this background that the first part of the guidelines is on internal controls, which transcend all the risk types. The rest of the guideline is organized by risk type namely credit, liquidity, interest rate, foreign exchange, operational, legal and compliance, strategic and reputational risks.

2. INTERNAL CONTROL ENVIRONMENT

2.1 Introduction

a) A system of effective internal controls is a critical component of a banking institution's risk management framework.

b) Internal controls are the policies, procedures and processes established by the board and senior management to provide reasonable assurance on the safety, effectiveness and efficiency of the institution's operations, the reliability of financial and managerial reporting, and compliance with regulatory requirements.

c) An effective internal control system is a fundamental mechanism for reducing the scope of risks faced by banking institutions.

2.2 Internal Control Environment

a) The following elements constitute a sound internal control environment.

2.2.1 Policies and procedures

b) Every banking institution should have comprehensive and sound policies, approved by the Board, for prudent management of significant risks arising from its business activities. The approved policies should be consistent with the nature, complexity and scale of the institution's activities. The institution should have a clear delineation of roles, responsibilities and accountability for the implementation of consistent policies across the institution.

c) The bank should establish appropriate procedures and processes to implement its policies. These should be documented in procedure manuals. The manuals should be periodically reviewed to ensure that they reflect current practices. There should also be adequate systems to monitor compliance with established policies and procedures. Deviations from such policies and procedures should be independently investigated, reported and addressed by the relevant parties.

2.2.2 Code of conduct

a) A banking institution should conduct its activities with prudence and integrity at all times. In this regard, the institution should establish a code of conduct that is commensurate with its structure and complexity of operations.

b) The code of conduct should state the ethical values of the institution and prescribe guidelines for employees to observe when discharging their duties. The code should cover areas such as acceptance of gifts and entertainment, conflicts of interest,

safeguarding confidentiality of information, and disclosure of and restrictions on personal investments.

c) In addition to general guidelines, a bank should prescribe specific guidelines for operations in functional areas such as investment banking, private banking and treasury.

d) An institution should ensure that all personnel understand and adhere to the code of conduct. The code should come under the purview of a senior staff member or an appropriate unit. Employees should be required to acknowledge in writing that they have read, understood and would observe the code. Disciplinary actions should be taken against those who breach the requirements.

e) The board or senior management should periodically review the code of conduct to incorporate changes in the internal and external environment.

2.2.3 Board and Senior Management Oversight

a) The board of directors has the ultimate responsibility for ensuring that an adequate and effective system of internal controls is established and maintained.

b) In this regard, the board's mandate in relation to internal controls should include:

i. ensuring that senior management has developed and implemented a properly structured internal control system;
ii. periodic discussions with management concerning the effectiveness of the internal control system;
iii. timely reviews of evaluations of internal controls performed by management, internal auditors, and external auditors;
iv. periodic checks to ensure that management has promptly followed up on recommendations and concerns expressed by auditors and supervisory authorities on internal control weaknesses; and
v. periodic reviews of the appropriateness of the bank's strategy and risk limits.

c) On the other hand, senior management should implement the strategies and policies approved by the board; develop processes that adequately identify, measure, monitor and control risks faced by the bank.

d) Further, management should maintain an organisational structure that clearly assigns responsibility, authority and reporting relationships and ensure that delegated responsibilities are effectively carried out.

2.2.4 Delegation of Authority

a) Institutions should clearly define the responsibilities and levels of authority required in relation to various types of activities and exposures for accountability purposes.

Approval limits assigned to personnel should be commensurate with their seniority and responsibilities.

b) The delegation of authority needs to be clearly documented and should specify, among others, the specific authority being delegated, the authority of recipients to further delegate authority, and restrictions placed on the exercise of delegated authority.

2.2.5 Segregation of Duties

a) Institutions should ensure adequate segregation of duties to mitigate the risk of unauthorised transactions or fraudulent activities. Senior management is responsible for ensuring that staff is not assigned incompatible duties which may allow an institution's data to be manipulated for personal gain, or for irregularities or financial losses to be concealed.

b) Banking institutions should conduct periodic reviews of the responsibilities of key personnel to minimise areas of potential conflict of interest and ensure independent checks are in place.

2.2.6 Audits

a) Every banking institution should be subject to an independent audit by external auditors at least annually.

b) Internal auditors should audit the risk management process and internal controls periodically, and scale the audit frequency according to the level of risk.

c) Results of audits and reviews by internal auditors or other persons and management responses or comments should be adequately documented.

2.2.7 Compliance

a) Banking institutions should take a proactive view of their compliance function by appointing senior personnel, or an appropriate unit, to oversee compliance issues. Compliance officers should be equipped with the necessary skills and expertise, the level of which should be commensurate with the complexity of the institution's products and activities.

b) Anomalies detected or instances of staff's failure to address compliance issues in a responsible manner should be promptly escalated to senior management for action.

2.2.8 Other elements of the control environment

a) **Succession planning** processes that are integrated with strategic plans should be developed to ensure business continuity.

b) Personnel policies requiring staff in key areas to take **mandatory block leave** each year to facilitate timely detection of unauthorised transactions and other irregularities, should be developed and approved by the board.

c) A banking institution should have adequate procedures for centralising, recording, investigating and monitoring **complaints from customers** which could be symptomatic of inadequate controls or non-compliance with existing procedures.

d) Banking institutions should ensure that **reward/compensation policies** are appropriate and sufficient to attract and retain competent and experienced risk management personnel and that they do not inadvertently provide incentives for inappropriate activities.

e) Personnel should be provided with **relevant and adequate training** at regular intervals to equip them with knowledge of new products, new or amendments to laws, rules and regulations, as well as to enhance their efficiency and effectiveness.

2.3 Business Process Controls

2.3.1 Legal Documentation

a) Institutions should have written agreements with counterparties, where appropriate and in line with market practice, specifying the duties and responsibilities of each party. For the institution's own protection, it should have clear guidelines and policies to ensure that the counterparty has the legal and necessary regulatory authority to enter into a transaction, prior to engaging in the transaction.

b) The banking institution should evaluate terms of any contract or agreement governing transactions to ensure that they are legally sound and enforceable in all relevant jurisdictions, and in the event of insolvency proceedings against the counterparty.

c) Legal protection also needs to be addressed in such documents, for instance, by ensuring that adequate remedies are available to parties and determination of risk allocation arising from external events.

2.3.2 Management Information Systems

a) Banking institutions should have adequate management information systems (MIS) to facilitate effective risk management and control of all aspects of their operations. The sophistication of the MIS should be consistent with the complexity and diversity of the institution's operations. Institutions should consider key elements such as timeliness, accuracy, consistency, completeness and relevance when developing their MIS.

b) The MIS should also be sufficiently flexible to cope with various contingencies and have the capability to monitor compliance with the institution's established policies, procedures and limits.

c) As timely and accurate reports are critical elements of an effective MIS, institutions should, as far as possible, reduce the amount of manual intervention required to prepare management reports and take steps to minimise inaccuracies in reports. Relevant levels of management should receive reports with adequate information to facilitate effective oversight of the institutions' activities.

2.3.3 New Products/Business Lines/Activities

a) An institution should have a new product policy to ensure that the risks inherent in new business lines or activities are properly assessed. Proposals on new products, business lines or activities should be accompanied, where appropriate, by a product programme document that includes:

i. an analysis of legal and regulatory requirements;

ii. a description of the relevant financial product and markets, and the underlying objectives of the transactions (e.g. customer service, risk management or trading);

iii. an analysis of the risks that may arise from these activities, and details of any risk management procedures and systems established, for identifying, measuring, monitoring and controlling risks;

iv. an evaluation of the impact of the proposed activities on the institution's overall financial condition and capital level, where applicable;

v. a description of the relevant accounting procedures; and

vi. a recommendation on the appropriate structure and staffing for trading as well as for the key risk control functions.

b) The new product policy should contain a definition of the term "new product", and provide for the proper review and authorisation of variations to existing products. The policy may require such variations to be approved by the Board or senior management. The policy should be updated when market conditions warrant it, when major assumptions have been changed, or when there are regulatory changes.

c) As new products frequently require different pricing, processing, accounting and risk measurement systems, an institution should ensure that it has the necessary resources to support these activities. The new product approval process should

include a sign-off by all relevant authorised personnel in areas such as risk control, operations, audit, accounting, legal and compliance, and by senior management.

d) Depending on the nature and complexity of a new product, a post implementation review of the new product should also be conducted at an appropriate period after its introduction, accompanied by proper documentation of the issues raised. Such a review would enable all the parties concerned to discuss the issues encountered during implementation and ensure that no risk remains unidentified.

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.

b) Credit risk is the risk that a borrower or counterparty will fail to meet obligations in accordance with agreed terms. An institution is exposed to credit risk from diverse financial instruments such as loans, acceptances, inter-bank transactions, trade financing, foreign exchange transactions, financial derivatives and other off-balance sheet activities. 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. An institution should 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 bank should have comprehensive credit risk management systems appropriate to its type, scope, sophistication and scale of operations. These systems should enable the bank 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 polices and procedures, strong management information systems 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 bank 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 bank in which credit exposure is a significant risk. It should encompass the need to maintain sound credit quality, profits and business growth and allow for economic cycles and their effects on the credit portfolio during different stages of an economic cycle.

c) 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, diversification and concentration of the credit portfolio;

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

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

iv. senior management should be fully capable of managing the credit activities conducted by the bank and that such activities are done within the risk strategy, policies and procedures approved by the board;

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

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

vii. 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) Senior management should implement the credit strategy and policies approved by the board of directors and develop procedures for effective management of 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 communicated throughout the institution, implemented, monitored and reviewed periodically to address any changes;

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

v. the development and implementation of appropriate reporting systems with respect to the content, format and frequency of information concerning the credit portfolio;

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

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

3.2.3 Risk Management Structure

a) An institution should adopt a risk management structure that is commensurate with the size and 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 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 senior management from the business line and control functions.

c) An institution should 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 bank 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 banking institution should have a clearly established process for approving credit facilities. This includes amending, renewing and refinancing of existing credit facilitiess.

b) At a minimum, the 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 bank'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, banks 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 bank.

3.3.2 Credit limits

a) A bank 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.

b) The policy on large exposures should be well documented to enable banks to take adequate measures to ensure that concentration risk is limited. The policy should stipulate the percentage of the bank's capital that the institution can lend to any individual or related entities.

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 parties 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 bank'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 banking institution should maintain adequate documentation relating to various types of loan products and credit instruments.

b) Prior approval for all new products should be obtained from the board as well clearance from independent control functions such as audit and risk management. All material risks arising from new products should be assessed before introduction to customers. Such policies should stipulate the credit risk analysis procedures and the administration of these credit instruments.

3.3.4 Credit risk mitigation

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

b) Security held by a banking 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's decision to lend should be based on the borrowers' capacity to repay and not on the adequacy of collateral.

3.3.5 Management of problem credits

a) A banking institution's credit policy should establish the procedures for dealing with problem credit facilities. 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 credit facilities 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

a) 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.

3.4 Measuring and Monitoring Credit Risk

3.4.1 Measuring credit risk

a) Every bank should have procedures for measuring its overall exposure to credit risk including exposure to related parties, products, customers, market segments and industries for appropriate risk management decisions to be made.

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

c) An institution should have robust management information systems 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 banking 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 bank:
   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 borrower's 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 rescheduled or otherwise altered 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 rolled over; 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) Banking 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

a) A bank should stress 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 bank's ability to withstand the changes.

b) Banking 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, banking institutions may use their internal systems and/or the provisioning levels prescribed in the Banking Regulations, Statutory Instrument 205 of 2000;
   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 interbank 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 banking 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, banking 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) A bank must be in a position to analyse 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 management with sufficient frequency, currency and, should be reliable with appropriate disaggregation.

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

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 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) Banking 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. Banking institutions' balance sheets are such that long-term assets (loans and advances) are funded by short-term liabilities such as demand and time deposits. Inadequate liquidity risk management can have a negative impact on earnings and capital and, in a worst case scenario, cause the collapse of an otherwise solvent institution.

c) The importance of liquidity transcends the individual banking institution, since a liquidity shortfall at a single institution can have system-wide repercussions. The analysis of liquidity requires management not only to measure the liquidity position of the banking institution on an ongoing basis but also to examine how funding requirements are likely to evolve under various scenarios, including adverse conditions.

d) The formality and sophistication of a banking institution's liquidity risk management processes should reflect the nature, size and complexity of an institution's activities. Institutions should have a thorough understanding of the factors that could give rise to liquidity risk and put in place mitigating controls.

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

f) Banking institutions should understand how its exposures to other risks may affect liquidity and put in place mitigating controls.

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 realisation 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 cashflows 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 a bank's liquidity risk management process. Sound liquidity risk management requires an informed board, capable management and appropriate staffing.

Board Oversight …

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

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

i. approving significant policies that govern or influence the bank's liquidity risk;
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; and
vi. reviewing adequacy of the contingency plans of the banking institution.

Senior Management Oversight …

d) A bank should have an appropriate senior management structure to oversee the day-to-day and long-term management of liquidity risk in line with the board approved strategy, policies and procedures.

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

f) The management structure should ensure that the liquidity strategy approved by the board can be effectively implemented.

g) Senior management should ensure that there is effective coordination between treasury and other functional areas.

h) Among other responsibilities, senior management should:

i. establish a schedule of liquidity reviews with appropriate frequency and depth;
ii. translate the board's approved strategy, objectives and risk tolerances into operational standards;
iii. implement management information systems that facilitate effective liquidity management through adequate identification, measurement, monitoring and control of liquidity risk;
iv. institute effective internal controls over the liquidity risk management process; and
v. promptly communicate any material changes in the banking institution's current or prospective liquidity position to the board of directors.

Asset and Liability Management Committee (ALCO) …

i) The board of directors may delegate the responsibility for managing the overall liquidity of an institution to the Asset and Liability Management Committee. ALCO should comprise senior management from each functional section of the institution that assumes and/or manages liquidity risk.

j) ALCO meetings should be held at least monthly.

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

i. reviewing previous results;
ii. assessing current balance sheet position;
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 strategy;
vii. setting measurable targets;
viii. communicating the targets to appropriate managers and staff; and
ix. monitoring actions regularly and reviewing performance.

4.3.2 Liquidity Strategy, Policies, Procedures and Limits

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

Strategy …

b) 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. composition of assets and liabilities;
ii. approach to managing liquidity in different currencies;
iii. managing access to interbank and other wholesale markets;
iv. diversification and stability of liabilities; and
v. management of intra-group liquidity.

c) The strategy should also define the banking institution's liquidity approach to meeting potential funding needs in the short and long-term and the risk tolerance levels.

Policies…

d) Every banking institution should have a set of liquidity policies regardless of whether liquidity is managed on a consolidated global basis at head office level, in the case of regional and international banking groups. This is because 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.

e) 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. **liquidity risk management in individual currencies**; and
v. **contingency plan** - strategy for handling liquidity crises.

f) 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.

Procedure Manuals …

g) 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.

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

Ratios and Limits…

i) 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.

j) Every banking 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.

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

l) 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 limit 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.

m) Liquidity ratios are useful for quantifying liquidity risk. Limits can be set on these ratios. However, liquidity ratios should always be used in conjunction with more qualitative information such as funding capacity to reveal material liquidity trends.

n) Ratios and limits that banking institutions should use to monitor liquidity risk may be categorized as follows:

i. **Cashflow Ratios and Limits** - liquidity risk may arise from a bank's failure to roll-over maturing liabilities or realise anticipated cashflows from assets. Cashflow 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 a bank 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** – banking institutions should use the following ratios: total loans/total deposits, total loans/total equity capital, borrowed funds/total assets among other ratios to monitor current and potential funding levels.

4.3.3 Liquidity Risk Measurement and Monitoring

a) Every banking institution should establish a risk measurement system to ensure that liquidity requirements are identified and managed on an on-going basis. The measurement system and associated procedures should be applicable under both normal and stressed liquidity conditions. A number of techniques can be used for measuring liquidity risk, ranging from simple gap calculations to sophisticated modeling.

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

Management Information Systems …

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

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

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

ii. analysing cashflows and maturity mismatch positions in all currencies in which a banking 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 exception reports; and

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

e) 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.

Cashflow Analysis and Maturity Profile …

f) Maturity mismatch analysis is a useful means for comparing cash inflows and outflows both on a day-to-day basis and over specified time periods. This approach measures an institution's liquidity by identifying cashflows from on- and off-balance sheet items.

g) Cashflow and maturity mismatch analysis enables banking institutions to assess their ability to meet immediate liquidity requirements, and identify their medium to long-term liquidity profile.

h) All cashflows (including those arising from off-balance sheet transactions) should be captured in the maturity profile. Where certain cashflows are considered to be immaterial, the decision to exclude them from the maturity profile should be approved by senior management/ALCO.

i) The following should be incorporated when constructing a maturity profile for maturity mismatch analysis:

Time Bands…

i. 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.
ii. Wider time bands may be used to manage long-term liquidity.

Behavioural Assumptions…

i. 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 its assets, liabilities and off-balance sheet items.
ii. 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 cashflow patterns and derive behavioural assumptions applicable to the cashflows.

iii. An institution should also examine the potential for significant cashflows from its off-balance sheet activities. The contingent nature of most off-balance sheet instruments increases the complexity of managing the associated cashflows. Every banking institution should therefore ascertain a "normal" level of net cashflows arising from off-balance sheet activities on an on-going basis.

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

Granularity…

i. A maturity profile should be constructed with appropriate granularity to reflect the institution's nature of business.

ii. An appropriate breakdown of the maturity profile by account type (e.g. a breakdown of deposits by type) allows for a more effective analysis to be carried out.

Limits on Net Cumulative Funding Mismatch…

i. A banking institution should specify acceptable limits for the size of the cumulative funding mismatch position for the short-term time bands.

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

Cashflows Denominated in Individual Currencies…

i. Every banking institution should perform maturity mismatch analysis of all its cashflows denominated in the local currency. For foreign currencies, which represent a significant portion of the institution's total funding and/or are not considered to be easily convertible, separate maturity mismatch analysis for such currencies should be performed.

Management Reports…

a) Liquidity management reports should include the following at a minimum:

i. a cash flow analysis highlighting short-term liquidity needs;
ii. structure, level and trend of assets and liabilities;
iii. level and trend of liquidity ratios;
iv. undrawn commitments;
v. limit breaches;
vi. computation of cost of funds and yield on assets;
vii. maturity gap analysis;

viii. levels of liquidity compared to established targets and resultant variance analysis; and

ix. alternative funding sources and funds available, including lines of credit and stand-by facilities, and associated costs.

4.4 Funding Capacity

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

b) For retail markets, an institution should consider its market share, competitive pressures, economic conditions, and other factors when estimating their 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 Intra-group Liquidity

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

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

4.6 Stress Testing

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

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

i. institution-specific crisis scenario; and
ii. general market crisis scenario.

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

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

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

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

h) The key assumption underlying an institution-specific crisis scenario should be that many of the institution's liabilities cannot be rolled-over or replaced, resulting in required repayment at maturity such that the institution would have to wind down its books to some degree.

i) 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. banks 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;
iv. senior management should ensure that key assumptions are evaluated at least annually for reasonableness.

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

k) 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.

l) 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 utilised in managing cashflows under the various crisis scenarios on a periodic basis. These assumptions are to be approved by senior management/ALCO.

m) Banking 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.

4.7 Contingency Plan

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

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

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 Reserve 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;

ii. 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 cashflow 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.

4.8 Media Relationship and Public Disclosure

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

b) Banking institutions 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.

4.9 Internal Controls

a) Each bank 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 a banking 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 individuals 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) The changes in interest rates affect a banking institution's earnings by altering interest-sensitive income and expenses. Interest rate changes also affect the underlying value of an institution's assets, liabilities, and off-balance sheet instruments through changes in the present value of future cash flows (and, in some cases, the cash flows themselves).

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 banking institutions are exposed include:

i. **repricing risk** which arises from timing differences in the maturity and repricing of bank assets, liabilities and off balance sheet positions;

ii. **basis risk** which arises from imperfect correlation in the adjustment of the rates earned and paid on different instruments with otherwise similar repricing characteristics;

iii. **yield curve risk** which arises when unanticipated shifts of the yield curve have adverse effects on a bank's income or underlying economic value; and

iv. **optionality risk** which arises from the options imbedded in many bank assets, liabilities and off balance sheet 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.

5.3.1 Board Oversight of Interest Rate Risk

a) Effective board oversight of a banking institution's exposure to interest rate risk is the cornerstone of an effective interest rate risk management process. The board should understand the nature and level of interest rate risk assumed by the banking institution and how this risk profile fits within the overall business strategies.

b) The responsibilities of the board of directors include the following:

i. reviewing the overall objectives of the banking institution with respect to interest rate risk and ensuring the provision of clear guidance regarding the level of interest rate risk acceptable to the bank;
ii. approving broad business strategies of the bank with respect to interest rate risk and ensuring that management takes the steps necessary to identify, measure, monitor, and control interest rate risk;
iii. approving policies that identify lines of authority and responsibility for managing interest rate risk exposures; and
iv. delegating responsibility for establishing interest rate risk policies to the Asset and Liability Committee (ALCO) or other designated committee.

Senior management oversight …

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.

5.3.2 Risk management policies and procedures

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

b) Interest rate risk management policies and procedures should:

i. specify limits for all types of instruments, portfolios, and activities;

ii. delineate lines of responsibility and accountability over interest rate risk management decisions;

iii. clearly define authorised instruments, either specifically or by their characteristics, hedging strategies, and position taking opportunities;

iv. delineate a clear set of institutional procedures for acquiring specific instruments, managing portfolios, and controlling the bank's aggregate interest rate risk exposure; and

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

c) 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.

5.3.3 Interest Rate Risk Management Process

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

Measurement…

b) Banks should have interest rate risk measurement systems that capture all sources of interest rate risk and that assess the effect of interest rate changes in ways that are consistent with the scope of their activities. The assumptions underlying the risk measurement system should be clearly understood by the board and senior management.

c) Interest rate risk measurement systems should assess the effects of rate changes on both earnings and economic value.

i. **Earning perspective** focuses on the impact of variation in interest rates on accrual or reported earnings. This approach to interest rate risk assessment is obtained by measuring the changes in the net interest income or net interest margin i.e. the difference between the total interest income and the total interest expense.

ii. **Economic Value Perspective** reflects the impact of fluctuation in the interest rates on the economic value of a banking institution measured by the present value of future cash flows. In this respect, economic value is affected both by changes in future cash flows and discount rate used for determining present value. This perspective also considers the potential longer-term impact of interest rates on an institution.

d) 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.

e) 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.

f) 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 time band 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. 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 backtests.

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.

g) 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.

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

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

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

k) 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.

Monitoring …

a) Banking 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.

5.3.4 Stress Testing

a) The risk measurement system should support a meaningful evaluation of the effect of stressful market conditions on the banking institution. Stress testing should provide information on the kinds of conditions under which the bank's strategies and/or positions would be most vulnerable, and be tailored to the risk characteristics of the bank.

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;
   ii. **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);

iii. **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

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

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) 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.

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

5.3.5 Reporting

a) Reporting of risk measures should be done regularly and must clearly compare current exposure to policy limits.

b) Past forecasts or risk estimates should be compared with actual results to identify any modeling shortcomings.

c) The board should review reports detailing the interest rate risk exposure of the bank on a regular basis. The reports prepared for the board and for various levels of management should at a minimum include the following:

i. summaries of the bank's aggregate exposures;
ii. bank's compliance with policies and limits;
iii. key assumptions, such as non-maturity deposit behaviour and prepayment information;
iv. results of stress tests, including those assessing breakdowns in key assumptions and parameters;
v. adequacy of internal controls; and
vi. 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.

d) Reports written by external auditors or other outside parties should be available to the supervisory authority.

5.4 Internal controls

a) Banking institutions should have adequate internal controls to ensure the integrity of their interest rate risk management process.

b) An effective system of internal controls for interest rate risk should include:
i. a strong control environment;
ii. an adequate process for identifying and evaluating risk;
iii. the establishment of control activities such as policies, procedures, and methodologies;
iv. adequate management information systems; and
v. continual review of adherence to established policies and procedures.

c) A bank's internal control systems must meet the following criteria:
i. all material interest rate risk associated with a bank's assets, liabilities, and off-balance sheet positions in the banking book must be assessed;
ii. it must accurately incorporate all of a bank's interest rate sensitive on and off- balance sheet holdings;
iii. it must utilise generally accepted financial concepts and risk measurement techniques;
iv. it must be capable of measuring risk using both an earnings and economic value approach;
v. data inputs should be adequately specified with regard to rates, maturities, re-pricing, embedded options, and other details;
vi. assumptions used to transform positions into cash flows should be reasonable, properly documented, and stable over time;
vii. material changes to assumptions should be documented, justified, and approved by management; and
viii. must be integrated into the bank's daily risk management practices.

d) A bank should pay attention to appropriate approval processes, exposure limits, reconciliations and reviews.

e) Senior management should ensure that reviews and evaluations of policies and procedures address significant changes that may impact the effectiveness of controls.

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

g) If the measurement system for interest rate risk incorporates one or more subsidiary systems or processes, the review should include testing aimed at ensuring that the subsidiary systems are well-integrated and consistent with each other in all critical respects. The results of this review, along with any recommendations for improvement, should be reported to senior management and/or the board and acted upon in a timely manner.

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. 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.

6.2.1 Board and Senior Management Oversight

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

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 place;

iii. monitoring significant foreign exchange exposures;

iv. ensuring that foreign exchange operations within the banking institution are in compliance with foreign exchange control regulations;

v. ensuring that foreign exchange operations are supported by adequate management information systems which complement the risk management strategy; and

vi. reviewing policies, procedures and currency limits regularly in line with changes in the economic environment.

6.2.2 Policies and Procedures

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, making foreign exchange risk management decisions, and conducting oversight;

ii. identify authorized types of financial instruments and hedging strategies;

iii. describe a set of strategies for controlling the institution's aggregate foreign exchange rate risk exposure;

iv. 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

v. define procedures and conditions for dealing with exceptions to policies, limits, and authorizations.

6.2.3 Risk Identification, Measurement and Control

Risk identification …

a) Foreign exchange risk exposures fall into structural and trading categories. Foreign exchange risk can be split into:

i. **translation exposure,** which arises from accounting based changes in consolidated financial statements caused by changes in exchange rates;

ii. **transaction exposure,** which occurs when exchange rates change between the time that an obligation is incurred and the time it is settled, thus affecting actual cash flows; and

iii. **economic exposure,** which reflects the change in the present value of the firm's expected future cash flows as a result of an unexpected change in exchange rates.

Risk Measurement …

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

c) The measurement systems should:

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.

Risk Limits…

d) A comprehensive framework of limits to control foreign exchange risk exposures should be established for different levels of reporting.

e) At a minimum, banking institutions should have the following limits for foreign exchange operations:

i. open position limits for individual currencies to which banks 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 bank operates;
iv. stop loss and/or management-action-trigger limits; and
v. limits for settlement risk of all counterparties.

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

6.2.4 Stress Tests

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

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.

6.2.5 Risk Monitoring and Control

a) Foreign exchange risk monitoring processes should be established to evaluate the performance of a banking institution's risk strategies/policies and procedures in achieving its overall goals.

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

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 bank's ALCO.

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

e) Banking institutions should have management information systems that provide accurate and timely information.

f) Periodic and frequent revaluations at current market rates should permit the monitoring of the bank's profits or losses on its foreign exchange book.

6.2.6 Risk Reporting

a) The types of reports vary depending upon overall foreign exchange risk profile of the banking institution. At a minimum the reports should contain:
   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 including any findings of internal/external auditors.

6.3 Internal Controls and Independent Audits

a) Banking institutions should conduct periodic reviews of their internal control and risk management process for foreign exchange risk to ensure its integrity, accuracy and reasonableness. Such reviews should be conducted by parties independent to the function being reviewed.

b) The reviews should, among others, ensure:
   i. accuracy and completeness of recording of all transactions;
   ii. effective segregation of duties between trading, settlement and accounting functions; and
   iii. effectiveness and accuracy of reporting of excesses of limits and other exceptions.

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

d) Banking institutions should promptly respond to findings regarding any violations of established procedures and ensure that there are adequate procedures for addressing weaknesses or irregularities noted by risk control functions, internal or external auditors and supervisory authorities.

e) Internal auditors and other risk control functions should be adequately staffed and have sufficient expertise and authority for reviewing the trading business.

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. This definition includes legal risk, but excludes strategic and reputational risk.

b) Developments such as deregulation and globalisation of financial markets, the growing sophistication of financial technology, the growth of e-commerce, mergers and acquisitions, viability of integrated financial systems and the increased prevalence of outsourcing are making the activities of banking institutions more diverse and complex leading to high levels of operational risk.

c) Banking 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 bank's risk/return profile and expose the bank to significant losses.

7.2 Operational Risk Management Framework

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

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. adequate management information systems; and
iv. sound internal controls and reviews.

7.2.1 Board and Senior Management Oversight

Board of directors …

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

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

iii. approve and periodically review a written bank-wide operational risk management framework;
iv. approve the operational risk policies developed by senior management;
v. review periodic high-level reports on the institution's overall operational risk profile, which identify material risks and strategic implications for the institution;
vi. 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;
vii. ensure that senior management is taking necessary steps to implement appropriate policies, processes and procedures as approved by the board;
viii. ensure that the operational risk management framework is subject to independent review by internal audit or other oversight functions; and
ix. ensure compliance with regulatory disclosure requirements on operational risk.

Senior management responsibilities…

b) Senior management should develop the operational risk management framework for approval by the board of directors.

c) Senior management should:
i. define the institution's organisational structure and clearly assign authority, responsibility and reporting relationships to encourage accountability;
ii. implement the board approved operational risk management policy;
iii. ensure that the banking 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;
iv. ensure that the bank's operational risk management policy has been clearly communicated to staff at all levels;
v. pay particular attention to the quality of documentation controls and to transaction-handling practices;
vi. put in place clear reporting systems of operational risk failures and provide for their subsequent resolution; and
vii. ensure that the operational risk management framework is subjected to independent reviews, which will provide assurance that the framework is adequate.

7.2.2 Policies and Procedures

a) A banking institution should have well-documented policies and procedures for managing operational risk. The policies 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 responsibility for defining the operational risk management strategy, and for ensuring that it is aligned with the overall business objectives, should rest with the board. In doing so, the board should provide clear guidance on the bank's risk appetite or tolerance.

c) Operational risk management policies, processes, and procedures should be documented and communicated to staff at all levels.

d) 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.

e) 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.

7.2.3 Operational Risk Management Process

Risk identification and assessment…

a) Management should establish a process that identifies the nature and types of operational risk, its causes and impact on the banking institution. Effective

operational risk identification and assessment processes are vital for a bank 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 bank's structure, the nature of the bank's activities, the quality of personnel, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

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

i. **Self Risk Assessment**: Every business unit of a banking institution 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**: Banks should have structures in place to map various business units, organisational 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. A banking institution must have key risk indicators to give an insight into its risk position. These indicators should be reviewed on a quarterly basis to alert management to changes that may be indicative of risk concerns.

iv. **Scorecards:** A banking institution must have techniques for:
- translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures;
- allocating economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk; and
- addressing factor inherent risks, as well as the controls to mitigate them.

v. **Thresholds/limits:** The bank'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.

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. The documentation should demonstrate that the analytical framework is comprehensive and internally consistent;

ii. quantitative and qualitative assumptions embedded in the methodology and provide explanation for the choice of these assumptions;

iii. 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;

iv. 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);

v. all changes to assumptions, and provide explanations for such changes; and

vi. the results of an independent verification of the analytical framework.

7.2.4 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.

7.2.5 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.

7.3 Contingency and Business Continuity Plans

a) A banking institution should have documented contingency and business continuity plans to ensure its ability to operate as a going concern and minimise losses in the event of severe business disruption.

b) The business resumption and contingency plans should take into account different types of scenarios to which the bank may be vulnerable and should be commensurate with the size and complexity of the bank's operations.

c) Management should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential.

d) For critical business processes, the banking institution should:

i. identify alternative mechanisms for resuming service in the event of an outage;

ii. pay particular attention to the ability to restore electronic or physical records that are necessary for business resumption;

iii. ensure that back-up records are at an off-site facility, and that where a bank's operations must be relocated to a new site, care is taken to ensure that the site is at an adequate distance from the affected operations.

e) The business resumption and contingency plans should be reviewed periodically so that they are consistent with the bank's current operations and business strategies. Further, the plans should be tested periodically to ensure that the bank will be able to execute the plans in the unlikely event of a severe business disruption.

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, self regulatory organization standards and codes of conduct applicable to its activities.

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

8.2 Compliance Risk Management

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

Board Oversight…

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

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

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

Senior management oversight …

a) Senior management is responsible for the effective management of a banking institution's compliance risk. As such, the bank's senior management is responsible

for establishing a written compliance policy the contains the basic principles to be followed by management and staff and explains the main processes by which compliance risks are to be identified and managed at all levels of the organisation.

b) Senior management should, with the assistance of the compliance function:
   i. Identify and assess the main compliance risk issues facing the bank and the plans to manage any shortfalls as well as the need for any additional policies or procedures to deal with new compliance risks;
   ii. ensure that the banking institution's compliance risk management framework has clear lines of authority, reporting and communication;
   iii. periodically report to the board of directors or a committee of the board on the bank's management of compliance risk;
   iv. report promptly to the board of directors or a committee of the board on any material compliance failures (e.g. failures that may attract a significant risk of legal or regulatory sanctions, material financial loss or loss to reputation);
   v. ensure that there is sufficient depth and skill in staff resources to manage legal and compliance risk; and
   vi. provide reasonable assurance, through the audit function, that all activities and all aspects of legal and compliance risk are covered by a banking institution's risk management process;
   vii. at least once a year conduct a compliance risk assessment
   viii. periodically reviewing the organisation's compliance risk management framework to ensure that it remains appropriate and sound.

Policies and procedures…

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

b) The compliance policy should address the following issues with respect to the compliance function:
   i. delineate responsibilities and ultimately ensure that the board and senior management are fully apprised of material compliance events;
   ii. its relationship with other risk management functions within the bank and with the internal audit function;
   iii. in cases where compliance responsibilities are carried out by staff in different departments, how these responsibilities are to be allocated among the departments;
   iv. its right to obtain access to information necessary to carry out its responsibilities and the corresponding duty of bank staff to co-operate in supplying this information;
   v. its right to conduct investigations of possible breaches of the compliance policy;

vi. its right to be able freely to express and disclose its findings to senior management; and

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

8.3 Compliance Risk Analysis

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

Self assessment…

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

Risk maps and process flows…

c) 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.

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

Key indicators…

e) Senior management should develop risk indicators to assess the level of compliance risk by different business functions in the bank. The compliance indicators should reflect the nature and characteristics of each of the strategic business units. The bank 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.

Escalation triggers…

f) 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.

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

Breach logs and near miss logs…

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

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

Internal audit reports…

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

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

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

Front-line prevention controls…

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

i. Clarity of roles and responsibilities;
ii. access to accurate, timely and clear management information; and
iii. establishing processes with minimal manual interfaces and intervention.

8.4 Compliance Monitoring and Reporting

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

b) The monitoring function should:

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

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

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

8.5 Tools to Manage the Compliance Process

Compliance Programme…

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

Education, training and communication…

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

c) Compliance training is needed for those whose jobs contain specific compliance tasks or responsibilities. Compliance staff should receive specific training in the type of monitoring techniques used by internal audit. They may need training in matters such as scheduling compliance activities, effective communication, some specifics of the law and effective people and management skills. Conflict resolution will also often be useful training. Others also need compliance training to the extent appropriate to their duties.

Effective monitoring…

d) Effective monitoring aims to check that people are doing what they ought to be doing and that the system is operating satisfactorily.

e) An important part of monitoring is to identify the main potential danger areas and pay special attention to those areas on a regular basis. Other purposes of monitoring are to:

i. ensure that the required procedures are being followed properly;
ii. help resolve difficulties at an early stage; and
iii. serve as an early-warning device.

An effective complaint system…

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

8.6 Certifications

a) Certifications involve requiring the compliance function to approve certain processes and business activities in order to minimize compliance risk.

b) Certifications have a number of advantages including the following:
i. draw attention to possible problem areas in a way that otherwise might not happen in a busy operating environment;
ii. can give maximum coverage and protection in areas where it is not practical to make independent checks regularly;
iii. having to issue a certificate directs minds to compliance with organizational standards and/or regulatory requirements; and
iv. if the compliance system ever has to be justified to a court, a proper system of certificates can demonstrate an intention to ensure that all areas are covered as well as possible, even if total coverage is not practicable.

8.7 Legal Risk

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

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

c) 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.

Organisational Structure…

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 bank.

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

Policies and Procedures…

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

i. a framework for dealing with legal matters of varying complexity;
ii. maintenance of a central inventory of key documents such as contracts, licences, policy statements and others;
iii. regular review and assessment of legal risk in the banking institution's activities including new products;
iv. adequate documentation on all significant transactions including security administration;
v. record maintenance in line with relevant statutory requirements; and
vi. maintenance of confidentiality provisions.

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 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
v. technology.

9.3 Strategic planning process

a) Setting future business direction is the ultimate responsibility of the board of directors or a delegated committee.

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

c) In this regard, every banking 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 banking 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 banking institution, and
v. assessment of actual performance against strategic plans.

d) The board should formulate the overall strategic plans and set an appropriate budget, while senior management should develop operational plans for each function by month, quarter or year. The operational plans should be consistent with the overall organizational strategy. The banking institution can formulate its plans through either a top down approach or bottom up approach or a mix of the two approaches.

e) The **top-down approach** is a strategic planning process where the board or delegated committees and senior management determine and allocate operating targets to

departments. On the other hand, the **bottom-up approach** is a strategic planning process where operational plans and budget from each department are consolidated into the strategic plan. A bank should adopt an approach which is best aligned to the nature, size and complexity of its operations.

f) A banking institution's strategic plans should complement and be integrated with other important issues such as capital adequacy, liquidity, source and use of funds, level and quality of earnings and management efficiency.

g) An important component of both strategic and operational plans is the budget. Banking institutions should develop budgets that are consistent with their plans. In addition, budgets should be underpinned by realistic assumptions, adequate allocation of resources for management and supporting functions as well as monitoring of actual performance.

9.4 Risk Mitigation Factors

a) Banking institutions should adopt and implement robust strategic risk mitigation measures and techniques to enhance the achievement of strategic objectives. These include enganging 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.

Qualified board and senior management…

b) The board and senior management should comprise of members with diverse and useful knowledge and experience. Further, they should be independent, active and have clear understanding of the market, economic and competitive conditions.

c) The bank's independent non-executive directors should diligently provide a check-and-balance mechanism on the activities of executive management.

Formulation & Implementation of strategic and operational plans…

d) The board and senior management should assess the changes in internal and external factors and continuously assess how these changes may affect the banking institution as well as adjust the plans to minimise the impact of these changes.

e) The board and senior management should also monitor compliance with laws, regulations, and shareholders' resolutions.

f) Further, the banking institution should set timeframes for implementation of different aspects of its strategic plans and establish performance evaluation systems.

Capacity building…

g) Every banking institution should recruit staff members with relevant knowledge, expertise, and experience in all business units. The staff members should have capacity to appreciate market conditions, competition and trend of products offered to target customers in line with the banking institution's strategic and operational plans.

h) In addition, staff should receive adequate training on risk management in order to promote efficient and effective implementation of the strategic and operational plans.

Risk management system…

i) A banking institution should have an enterprise-wide risk management system. All types of related risks must be taken into account during the formulation of strategic and operational plans by setting policies, procedures, and risk limits.

Adequate access to information…

j) Banking institutions should have adequate information on their internal and external environment in order to effectively design and implement strategic plans. As such, every banking institution should invest in systems and approaches that will enable it to access adequate, accurate, and timely information to understand competition, the environment, and customer needs. A bank should use various information sources, such as business experts, consultants and correspondent banking institutions to build its information database.

9.5 Managing Strategic Risk

a) Every banking institution should establish an integrated risk **management** function that is designed to enhance understanding and communication of risk issues internally, to provide clear direction and demonstrate senior management support. To be effective, the risk management system needs to be aligned with an organisation's overall objectives, corporate focus, strategic direction, operating practices and internal culture. A banking institution should integrate risk management within existing governance and decision-making structures both at the operational and strategic levels.

b) Each banking institution should develop risk management systems appropriate to the size, complexity and scope of its business. A system to report detailed progress of implementation of the plans and objectives should be implemented including comparison of actual performance against the operational plan and budget, and the business continuity plan for unusual circumstances to facilitate copying with unexpected changes in the environment.

Risk Identification and measurement…

a) Identification and measurement of strategic risk are the responsibility of management who should ensure that periodic reviews of strategic plans are conducted as circumstances change.

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

c) A banking institution should utilize a range of practical tools to assess its strategic risk. The following are some examples of the techniques:

i. **risk maps:** summary charts and diagrams that help the bank to identify, discuss, understand and address risks by portraying sources and types of risks and functions involved;

ii. **modelling tools:** such as scenario analysis and forecasting models to show the range of possibilities and to build scenarios into contingency plans, and

iii. **qualitative techniques:** such as questionnaires and self-assessment to identify and assess risks.

Risk monitoring and reporting…

a) The development of evaluation and reporting mechanisms for risk management activities provides critical feedback to management with respect to strategy implementation. The monitoring of strategic plan implementation should be allocated to a specific independent function in the bank.

b) Where appropriate, the monitoring and reporting of strategic risk should also fall to functional units responsible for review and audit. Reporting could take place through such management channels such as performance reporting, ongoing monitoring and appraisal.

c) A bank should evaluate the effectiveness of its strategy implementation on a periodic basis and make the necessary adjustments to ensure sustained progress toward the attainment of strategic objectives.

d) Effectiveness of risk monitoring depends on ability to identify and measure all the risks, which must be supported by appropriate, accurate and timely management information systems or model to help with analysis and decision making.

j) Therefore, the board or delegated committees and senior management must develop information systems that can identify and measure the risks in an accurate, reliable

and regular manner commensurate with the complexity and diversity of the banking institution's business.

k) Management information systems (MIS) should provide information necessary to support implementation of the strategic plans. The information systems of banking institutions should be able to collect internal data such as financial data, accounting data, and external data such as economic conditions, competition, technology and regulatory requirements.

l) The bank should review its MIS regularly, as well as set policies and procedures and operational framework on MIS development, maintenance, security, repair or upgrade in order to maintain the standard.

Risk control …

a) The board and management should establish a risk management controlling system in accordance with international best practice. The risk monitoring function should be independent of the risk-taking functions. In addition, the board should receive a variety of reports for risk review and monitoring.

b) A banking institution should control strategic risk through the following approaches, among others:

i. adaptive risk management structure;
ii. policies, procedures, and risk limits;
iii. new product reviews;
iv. comparisons of the actual performance with projections
v. quality and effective independent reviews and internal control systems;
vi. management succession plan and training; and
vii. business continuity planning.

10. REPUTATIONAL RISK

10.1 Introduction

a) Reputational risk arises when a situation, occurrence, business practice or event has the potential to materially influence the public and stakeholder's perceived trust and confidence in a banking institution.

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

i. **Corporate reputation risk**: which relates to a bank's performance, strategy, execution and delivery. This is closely intertwined 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 bank, any of its affiliates or its officials will impair its image with one or more of its stakeholders and this will result in loss of business, and/or disproportionate decrease in the value of a bank.

c) Reputational risk may arise from a variety of sources, such as fraud and noncompliance with statutory or regulatory requirements.

d) Other sources of reputational risk may arise from failing to safeguard nonpublic customer information through outsourcing relationships, a high volume of customer complaints, or public regulatory sanctions.

e) Reputational risks may arise where occurrences in other categories of risk also threaten an organisation's image and stakeholder regard. As such, the task of managing reputation risk represents a critical aspect of risk management.

10.2 Categories of Reputational Risk

a) Banking institutions should pay special attention to three general categories of events or circumstances which give rise to reputational risk. The risk methodologies employed must be broad enough to reach all risks in each category.

Inherent Risk…

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

Environmental Risk…

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

Governance and Control Risk…

d) An institution should protect itself against these risk which arise from losses as a result of inadequate or failed internal processes, people and systems as well as from losses caused by an organisation'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 Policies and Procedures

a) Banks are required to have policies and procedures under which they will:

i. adopt sound risk management practices that include the practice of building reputational capital, and earning the goodwill of key stakeholders;

ii. manage reputational risk through a process of anticipation, risk analysis and planning, and then attempting to manage both internal and external expectations;

iii. measure trends in a bank's reputation as a precursor to remedial action; and

iv. identify risk events as being either specific or systemic as this will determine the course of corrective action.

10.4 Risk management and monitoring

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

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

c) A bank should ensure that it establishes a crisis management procedure to manage the potential impact of reputational events.

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

e) Reputational risk can also arise from many aspects of an institution's operations. For example, the failure to manage properly the other risks could result in a large market or credit loss. Even where no monetary loss is incurred, there could still be reputational damage. Institutions thus have to implement a sound and comprehensive risk management process to identify, monitor, control and report reputation related risks.

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

10.5 Risk Methodology Components

Risk Template…

a) In order to capture reputational 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.

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

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

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

Reputation Risk Analysis Methodology and Process…

e) Every banking institution should conduct a risk diagnostic review to identify potential reputational risk issues. The board's responsibilities should include requiring management to use proven analysis methodologies as well as independent and objective reviews designed to bring out and analyse both quantitative and qualitative risk factors and to review critical control points within the bank.

f) This process should assist the bank to uncover the key risk factors which are most likely to give rise to reputational risk issues. 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.

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

10.6 Roles and responsibilities

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

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

c) The bank's 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 reputational risk events. It should also be responsible for monitoring a bank's reputation within the market place.

NOTES

NOTES

NOTES