

BANK OF BOTSWANA

BANKING SUPERVISION DEPARTMENT



GUIDELINES ON RISK MANAGEMENT

Issue Date: May 15, 2018

TABLE OF CONTENTS

1. AUTHORITY, PURPOSE AND SCOPE	3
(a) Authority.....	3
(b) Purpose	3
(c) Scope	3
2. DEFINITIONS	4
3. INTRODUCTION	10
(a) Types of Material Banking Risks	11
(b) Risk Management Process.....	11
(c) Basic Elements of a Sound Risk Management System	12
(d) Risk Management Function.....	15
(e) Risk Disclosures	16
4. STRATEGIC RISK MANAGEMENT	18
(a) Strategic Planning Process	18
(b) Strategic Risk Identification.....	18
(c) Strategic Risk Measurement.....	19
(d) Strategic Risk Mitigation, Monitoring and Control	19
(e) Strategic Risk Reporting	20
5. CREDIT RISK	21
(a) Establishing an Appropriate Credit Risk Environment.....	21
(b) Credit Risk Identification and Measurement.....	23
(c) Credit Risk Monitoring and Control	26
(d) Credit Risk Reporting.....	35
6. MARKET RISK	36
(a) Market Risk Identification.....	36
(b) Market Risk Measurement	36
(c) Market risk Monitoring and Control	37
(d) Market Risk Reporting	38
INTEREST RATE RISK	39
(a) Interest Rate Risk Identification.....	39
(b) Interest Rate Risk Measurement.....	40
(c) Interest Rate Risk Monitoring and Control	42

(e) Interest Rate Risk Reporting	43
FOREIGN EXCHANGE RISK	45
(a) Foreign Exchange Risk Identification	45
(b) Foreign Exchange Risk Measurement.....	46
(d) Foreign Exchange Risk Monitoring and Control	47
(e) Foreign Exchange Risk Reporting	48
7. LIQUIDITY RISK MANAGEMENT	49
(a) Liquidity Risk Identification	49
(b) Measurement and Management of Liquidity Risk	49
(c) Liquidity Risk Monitoring and Control.....	50
(d) Liquidity Risk Reporting.....	52
8. OPERATIONAL RISK MANAGEMENT	54
(a) Operational Risk Culture	54
(b) Operational Risk Identification and Measurement.....	54
(c) Operational Risk Monitoring, Control and Mitigation.....	56
(d) Operational Risk Reporting.....	59
(e) Business Resiliency and Continuity	60
9. COUNTRY AND TRANSFER RISK.....	63
10. COMPLIANCE RISK MANAGEMENT	65
(a) Compliance Risk Identification.....	65
(b) Compliance Risk Measurement.....	65
(c) Compliance Risk Monitoring, Control and Mitigation	66
(d) Compliance Risk Reporting	68
11. REPUTATIONAL RISK MANAGEMENT.....	69
(a) Identification of Reputational Risk	69
(b) Measurement of Reputational Risk	70
(c) Monitoring, Control and Mitigation of Reputational Risk.....	70
(d) Reporting of Reputational Risk	71

1. **AUTHORITY, PURPOSE AND SCOPE**

(a) **Authority**

- 1.1 These Guidelines are issued by the Bank of Botswana (Bank) pursuant to its authority set forth in Section 4(2) of the Bank of Botswana Act (CAP. 55:01).

(b) **Purpose**

- 1.2 The purpose of these Guidelines is to implement the provisions of all relevant sections of the Banking Act (CAP. 46:04) (Act) for the ultimate attainment of the requirements of Section 4(1) of the Bank of Botswana Act, as well as to provide guidance to banks on the management of risks, in line with the Basel Core Principles 15 - 25 and international best practice.

(c) **Scope**

- 1.3 These Guidelines apply to a bank licensed by the Bank under the Act and statutory banks established under separate Acts of Parliament, which fall under the purview of the Bank's supervision in terms of Section 53(2) of the Act and/or their respective statutes.

2. DEFINITIONS

- (a) **Accommodation** - A loan, advance or other credit facility, financial guarantee or other liability granted or incurred by a bank to or on behalf of any person, natural or legal.
- (b) **Act** - The Banking Act (CAP.46:04).
- (c) **Audit Committee** - A committee (or equivalent body) established by a board of directors of a bank for the purpose of overseeing the accounting and financial reporting processes and audits of the financial statements of a bank and ensuring the adequacy and effectiveness of the bank's internal control systems.
- (d) **bank** - A company which is licensed by the Bank, pursuant to the Act, to conduct banking business as defined in Section 3 of the Act.
- (e) **Bank** - The Bank of Botswana established under the Bank of Botswana Act (CAP. 55:01).
- (f) **Banking book** - refers to positions that are not assigned to the trading book.
- (g) **Basel II Directive** - Directive on the Revised International Convergence of Capital Measurement and Capital Standards for Botswana
- (h) **Basis risk**: refers to the impact of relative changes in interest rates for financial instruments that have (i) either similar tenors, but are priced using different interest rate reference curves (reference rate basis risk); or which have (ii) different tenors, but with the same reference curve (tenor basis risk or short-term non-parallel gap risk); or which have (iii) similar tenors and reference curves, but in different currencies (currency basis risk).
- (i) **Board of Directors** - The highest body of authority in a bank responsible for the bank's business and risk strategy, organisational financial soundness and governance. The board also provides effective oversight of senior management.
- (j) **Contagion effects**: the advent of the spread of negative or positive consequences of a financial or economic nature across countries or regions.
- (k) **Contingency Funding Plan** - A compilation of policies, procedures, and action plans for responding to severe disruptions to a bank's ability to fund some or all of its activities in a timely manner and at a reasonable cost.
- (l) **Counterparty risk**: the risk that a party to a transaction or contract will fail to fulfil its contractual obligations.
- (m) **Credit swaps**: contracts where one side pays an ongoing fee in exchange for a guarantee that upon default the insurance will pay the full principal amount due to the contract owner.

- (n) **Enterprise-wide risk management:** is the overall management of risk that an organisation takes and holds to achieve its strategic objectives. It is the sum of the various risks the organisation takes in the various categories and focuses on optimising the balance and interaction of the different types of risks.
- (o) **Expected credit losses (ECL):** is the probability-weighted estimate of credit losses (i.e., the present value of all cash shortfalls) over the expected life of a financial instrument.
- (p) **Exposure** - The amount of a bank's exposure is calculated as follows:
 - (a) The sum of all loans and credit facilities granted, either directly or indirectly, to a person or group of inter-related persons, such as:
 - (i) term loans, overdrafts, credit lines and other credit facilities;
 - (ii) trade bills discounted, invoice discounts and factoring;
 - (iii) credit substitutes, such as guarantees, acceptances, letters of credit and bills, and finance lease receivables;
 - (iv) underwriting of debt and equity securities, and other forms of participations;
 - (v) securitised assets and other transactions with recourse;
 - (vi) credit derivatives, futures and forwards, swaps and option contracts such as credit default swaps and other derivatives; and
 - (vii) contingent liabilities, such as commitments to extend credit, performance bonds and warranties.
 - (b) Less the amount by which the above-listed accommodations are irrevocably secured by:
 - (i) eligible financial collateral meeting all the requirements of the Directive on the Revised International Convergence of Capital Measurement and Capital Standards for Botswana (Basel II Directive) placed with a bank that granted the accommodation; or
 - (ii) an eligible guarantee meeting all the requirements of the Basel II Directive; and
 - (iii) For a guarantee to be considered eligible, the following conditions must be satisfied:

- (a) The credit protection must represent a direct claim on the protection provider;
- (b) The guarantee or credit derivative must be explicitly referenced to specific exposures or a pool of exposures, such that the extent of the credit protection is clearly defined and incontrovertible;
- (c) The credit protection contract must not contain any clause that:
 - (i) allows the protection provider to unilaterally cancel the protection;
 - (ii) increases the effective cost of the protection, as a result of the deteriorating credit quality of the protected exposure;
 - (iii) prevents the protection provider from being obliged to pay out in a timely manner, in the event that the original obligor fails to make any payments due; and
 - (iv) allows the maturity of the credit protection to be reduced by the protection provider.
- (d) It must be legally effective and enforceable in all jurisdictions which are relevant at the time of the conclusion of the credit agreement;
- (e) In addition to the legal certainty requirements for a guarantee to be eligible, the following conditions must also be satisfied:
 - (i) Upon default or non-payment by a counterparty, a bank must have the right to pursue, in a timely manner, the guarantor, for any monies due under the claim, in respect of which the guarantee is provided;
 - (ii) The guarantor must either make a lump sum payment of all monies due under the claim to the bank or assume the payment obligations of the counterparty that was covered by the guarantee;
 - (iii) A bank must have the right to receive any such payments from the guarantor, without first having to take legal action in order to pursue the counterparty for payment;
 - (iv) The guarantee must be an explicitly documented obligation assumed by the guarantor;

- (v) The guarantee must cover all types of payments the underlying obligor is expected to make in respect of the claim; and
 - (vi) Where a guarantee covers payment of the principal only, interest and other amounts not covered by the guarantee must be treated as the uncovered portion.
- (q) **Foreign exchange settlement risks:** is the risk of loss when a bank in a foreign exchange transaction pays the currency it sold, but does not receive the currency it bought.
- (r) **Funding Liquidity Risk** - The risk that the bank will not be able to efficiently meet both the expected and unexpected current and future cash flows and collateral needs without affecting either daily operations and/or the financial condition of the bank.
- (s) **Interest rate sensitivity gap:** measures the responsiveness of the asset and liability portfolio to changes in interest rates.
- (t) **Interest rate swaps:** is an agreement to exchange one stream of interest payments for another.
- (u) **Liquid Assets** - Freely transferable assets, unencumbered by any charge or lien whatsoever, located in Botswana and are central bank eligible, including:
 - (i) Treasury bills, Bank of Botswana Certificates, and other securities issued by the Botswana government or the Bank and maturing within 370 days;
 - (ii) Negotiable instruments of such types as the Bank may approve and payable within a period of 184 days; and
 - (iii) Such other assets as the Bank may from time to time, approve, provided that they: (1) have distinct denominations of at least P1 000; (2) are listed and actively traded by an exchange in Botswana, if instruments of public issue; (3) disclose the earliest possible date that a borrower may pre-pay; (4) are rated no less than AA- by an external credit assessment institution acceptable to the Bank; and (5) are otherwise acceptable to the Bank in accordance with the requirements for the Secured Lending Facility.
- (v) **Liquidity** - The ability of a bank to fund asset growth and/or meet contractual obligations as they fall due, including obligations to fund loan and investment commitments, deposit withdrawals and other maturing liabilities, without incurring unacceptable capital losses.
- (w) **Liquidity Risk** - The risk of loss to a bank resulting from inability to meet actual needs for cash or inadequate liquidity levels, which must be covered by funds obtained at excessive cost.

- (x) **Liquidity-Risk Management** - The process of ensuring that the bank's needs for funds, including maintaining the required level of liquidity and meeting expected and contingent cash needs can be regularly met at a reasonable cost.
- (y) **Management-action-trigger limits:** represents the management's tolerance for accepting the market risk related losses on a daily and cumulative month-to-date basis, especially on the trading portfolio.
- (z) **Management information system (MIS):** A computer system consisting of hardware and software that serves as the backbone of an organisation's operations.
- (aa) **Mark-to-market:** is a measure of the fair value of accounts that can change over time, such as assets and liabilities.
- (bb) **Net Funding Requirements** - The liquid assets necessary to fund a bank's cash obligations and commitments in future, determined by performing a cash flow analysis in which all cash inflows are measured against all cash outflows to identify potential net shortfalls.
- (cc) **Open Position** - the difference between a bank's total of its foreign currency-denominated assets and liabilities, both spot and forward, in Pula currency (equivalent) balances.
- (dd) **Optionality risk:** refers to the risk that arises from price movements in instruments that are either automatic or behavioral to changes in interest rates.
- (ee) **Related Person** - Includes all of the following without limitations: (1) Significant shareholder; (2) member of a board of directors or audit committee; (3) principal officer and senior management officials, (4) guarantor of a trust; (5) A person who maintains a trust on behalf of a bank or its affiliate; (6) Any person who is related to such significant shareholder, member of a board of directors or audit committee, principal officer or family member or business interest; (7) subsidiary of a bank; (8) company or undertaking in which at least a 5 percent interest is held by a bank; (9) parent company of a bank; (10) company that is under common control with a bank; and (11) A company that holds at least a 5 percent interest of another company in which a bank holds at least a 5 percent interest.
- (ff) **Risk transfer:** risk transfer is a risk management and control strategy that involves the contractual shifting of a pure risk from one party to another.
- (gg) **Senior Management Official** - Any person who is an officer of a bank, including those holding positions of managing director or chief executive officer (and deputies), chief financial or operations officer, chief lending officer, chief internal auditor, chief treasury officer (or their equivalents), and other heads of department (core banking functions) and/or others who are in a policy-making position.
- (hh) **Stop loss:** an advance order to sell an asset when it reaches a particular price point. It is used to limit loss or gain in a trade.

- (ii) **Stress testing** - is a generic term often used to describe various techniques and procedures employed by banks to gauge their potential vulnerability to exceptional but plausible events. Stress testing alerts bank management to adverse unexpected outcomes related to a variety of risks and provides an indication of how much capital might be needed to absorb losses should large shocks occur.
- (jj) **Swap**: is a derivative contract through which two parties exchange financial instruments.
- (kk) **Syndicated loans** - credits granted by a group of banks to a borrower.
- (ll) **Trade financing**: is the financing and facilitation of trade of goods and services, locally and internationally.
- (mm) **Trading book** - a trading book consists of positions in financial instruments or commodities held either with a trading intent or in order to hedge other elements of the trading book.
- (nn) **Unencumbered** - Not pledged either explicitly or implicitly as security, collateral, guarantee and/or other credit-enhancement for any transaction.
- (oo) **Unexpected losses**: Losses above expected levels.
- (pp) **Value at risk (VaR)**: is a method of calculating financial risk based on a defined probability level. It indicates the potential loss of a position/asset over a period of time with a given level of confidence.
- (qq) **Yield curve risk**: is a risk that arises when unanticipated shifts of the yield curve have adverse effects on a bank's income or underlying economic value.

3. INTRODUCTION

- 3.1 Risk-taking is inherent in banking business. Excessive and poorly managed risk can, however, lead to losses and thus pose a threat to the safety and soundness of a bank. Therefore, the Bank places emphasis on the adequacy of a bank's management of risk and issues these Guidelines for the purpose of providing guidance to all banks on minimum standards and requirements for sound and effective management procedures and systems to be in place at every bank.
- 3.2 For the purpose of these Guidelines, risk in a bank refers to the possibility that the outcome of an action or event could bring adverse impact on solvency, earnings, cash or, in general, sustainability of a bank's operations. Such outcomes could result in either direct diminution of a bank's earnings, or erosion of capital, loss of cash, or cash flow, or the imposition of constraints on a bank's ability to meet business objectives. These constraints could hinder a bank's capability to conduct business in a safe and sound manner, including the ability to effectively take advantage of opportunities that could enhance performance. As such, the board of directors (board) and senior management officials (Management) of a bank are expected to ensure that the risk a bank is taking is understandable, measurable, controllable and within a bank's capacity to readily withstand adverse effects.
- 3.3 Effective risk management is core to the success of every bank and encompasses all activities that affect a bank's risk profile. The board and Management of a bank should put in place appropriate systems and infrastructure to identify, measure, monitor, control and report overall risks that a bank may assume.
- 3.4 These Guidelines are aligned to the Basel Core Principles for Effective Banking Supervision. Core Principle 15 on 'risk management processes' requires banks and banking groups to have comprehensive risk management processes (including effective board and senior management oversight) to identify, evaluate, monitor and control or mitigate all material risks, and to assess a bank's overall capital adequacy in relation to the risk profile. Risk-taking should be commensurate with the nature, size and complexity of a bank and the degree of a bank's risk appetite and tolerance level. The risks a bank may be exposed to depend on factors such as business activities, nature and type of products, business cycle, economic sectors, geographic location, business model and, in general, operating strategy.
- 3.5 These Guidelines are not intended to prescribe a uniform set of risk-management strategies for all banks. The sophistication of processes, systems and internal controls for risk management is determined by the nature, size and complexity of the business activities of a bank.
- 3.6 The guidance expressed in these Guidelines is not exhaustive; other relevant regulatory requirements and applicable industry standards should also be taken into account as appropriate.

(a) Types of Material Banking Risks

3.7 The Bank assesses inherent risks using the expected impact on the supervised bank's earnings, liquidity, capital, and, more broadly, set goals/objectives. Quantitative and qualitative factors are applied in the process of risk assessment. These Guidelines highlight some of the risks inherent in banking business as follows:

- (i) Strategic Risk;
- (ii) Credit Risk;
- (iii) Market Risk;
 - (a) Interest Rate Risk;
 - (b) Foreign Exchange Risk;
- (iv) Liquidity Risk;
- (v) Operational Risk;
- (vi) Country and Transfer Risk;
- (vii) Compliance Risk; and
- (viii) Reputational Risk.

3.8 These risks are intertwined; hence they should be managed in an integrated manner (enterprise-wide risk management).

(b) Risk Management Process

3.9 Each bank must prepare a comprehensive risk-management programme (RMP) tailored to its needs and circumstances. The RMP should be reviewed at least annually. The RMP should, at the minimum, include the following elements:

(i) Risk Identification

3.10 In order to properly manage risk, a bank must recognise and understand risks that may arise from both existing and new business initiatives (interest rate processes, products, delivery channels, etc.). For example, risks inherent in a lending activity include credit, liquidity, interest rate and operational risks. Risk identification should be a continuing process, and should be understood at both transactional and portfolio levels.

(ii) Risk Measurement

3.11 Risk should be measured accurately and timely in order to determine the impact on the bank's profitability and capital. Risk measurement tools should be tested periodically for accuracy. Good risk-measurement systems assess the risks of both individual transactions and portfolios.

3.12 Where a bank uses models to measure components of risk, such a bank should ensure that the board and Management understand the limitations and uncertainties relating to the output of the models and the risks inherent in their use. In addition, the output of such models should be a reasonable reflection of the risks assumed. A bank should perform regular and independent validation; and testing of the models used.

For example, an internal credit risk-rating system and/or modelling should be validated using well-established external rating system/methodology.

(iii) Risk Monitoring

- 3.13 A bank should put in place an effective management information system (MIS) to monitor risk levels and facilitate the timely review of risk positions and exceptions. Monitoring reports should be frequent, timely, accurate and informative. Such reports should be distributed to appropriate individuals for implementation, to be specifically identified in the bank's procedures.

(iv) Risk Mitigation and Control

- 3.14 A bank should establish and communicate risk limits through policies, standards, and procedures which define responsibility and authority. These limits should serve as a means to control exposure to various risks associated with the bank's activities; they should have a process to authorise and document exceptions or changes to risk limits when warranted. A bank may also apply various mitigating tools in minimising exposure to various risks.

(c) Basic Elements of a Sound Risk Management System

- 3.15 A sound risk-management system should, at a minimum, have the following key elements:
- Risk governance framework, including, active board and senior management oversight (BMO) ;
 - Adequate policies, procedures and limits (PPL);
 - Adequate risk measurement, monitoring and management information system (MIS); and
 - Adequate internal controls (ICs).

(i) Active Board and Senior Management Oversight

- 3.16 The board provides effective oversight on Management's actions to ensure that the actions of the latter are consistent with the risk strategy, risk appetite framework and policies of a bank. The board should approve the overall business strategies and significant policies of the bank, including those related to taking and managing risks, and should also ensure that Management have skills, expertise and competence commensurate with the nature, scale and complexity of the bank's business. The board should comprise individuals with diversified skills and work experience. Within the board, there should be a member or members designated or assigned specific responsibilities for risk-management oversight activities.
- 3.17 Board members should continually enhance their skills so that they are able to understand the types of risks to which banks are exposed. The board should demand to be furnished with periodic reports by a bank, for it to identify, in a timely manner, the nature and significance of the risks a bank is exposed to. The board should use

this information to provide clear guidance regarding the level of exposures suitable to a bank and have the responsibility to ensure that Management implements the procedures and controls necessary to comply with adopted policies.

- 3.18 Management is responsible for ensuring that the day-to-day activities of a bank are consistent with the bank's risk strategy. This includes risk appetite and policies approved by the board; establishing and communicating a strong awareness of an effective internal control environment and high ethical standards; as well as establishing clear guidance regarding the business and risk strategy such as risk limits, in order to ensure that activities undertaken by a bank are within the risk appetite prescribed by the board of the bank.

(ii) Adequate Policies, Procedures, and Limits

- 3.19 The board and Management of a bank should tailor the risk-management policies and procedures to the types of risks that arise from the activities of the bank. The bank's policies and procedures should provide detailed guidance for the day-to-day implementation of broad business strategies and, generally, include limits designed to shield the bank from excessive and imprudent risks. Senior management is expected to modify these tools when necessary to respond to changes in a bank's activities or business conditions.

- 3.20 Every bank should ensure that:

- policies, procedures and limits provide for the adequate identification, measurement, monitoring and control of the risks posed by a bank's significant activities;
- established limits are understood by, and regularly communicated to, relevant staff;
- policies clearly delineate accountability and lines of authority across the bank's activities;
- risk-management strategic policies, processes and limits are properly documented, regularly reviewed and appropriately adjusted to reflect changing risk appetites, risk profile, market and macroeconomic conditions; and communicated within the bank; and
- policies provide for the review of activities which are new to the bank in order to ensure that the infrastructure necessary to identify, measure, monitor and control risks associated with the activity are in place before the activity is adopted.

(iii) Adequate Risk Measurement, Monitoring and Management Information Systems

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

- a bank's risk monitoring practices and reports should address all the material risks;
- key assumptions, data sources and procedures used in monitoring risk should be appropriate, adequately documented and tested for reliability on an ongoing basis;
- reports and other forms of communication should be consistent with a bank's activities, structured to monitor exposures and compliance with established limits, goals, objectives; and, as appropriate, compare actual versus expected performance;
- reports to the bank's board and Management should be accurate and timely and contain sufficient information for decision makers to identify any adverse trends and to evaluate adequately the level of risk faced by a bank;
- risk monitoring activities must be supported by an information system that provides the board and Management with timely reports on the financial condition, operating performance and risk exposure of a bank, as well as with regular and sufficiently detailed reports for line managers engaged in the day-to-day management of the bank's activities. The sophistication of the bank's information system must keep pace with developments in the bank's risk profile, increased business complexity and new products or business lines; and
- the board and Management must put in place a reporting format, which clearly delineates the likely occurrence (frequency) and impact, to be signed at regular intervals by relevant senior management officers and Board members.

(iv) Adequate Internal Controls

3.22 A bank's audit and risk management committees should review the adequacy and effectiveness of internal control systems and means through which risk exposures are managed. A sound internal control process consists of the following interrelated elements: management oversight and control culture; risk recognition and assessment; control activities and segregation of duties; information and communication; and monitoring activities and correcting deficiencies.

3.23 A bank should establish and maintain an effective system of controls, including the enforcement of official lines of authority and appropriate separation of duties, such as trading, custody and back-office.

3.24 Failure to implement and maintain an adequate separation of duties can lead to serious losses, compromise the financial integrity of a bank and may warrant formal enforcement action by the Bank.

3.25 Ideally, internal controls should be tested by an independent internal auditor, who reports directly either to a bank's board or its audit committee.

3.26 In order to ensure the adequacy of a bank's internal controls and audit procedures, the following should be observed:

- the system of internal controls should be appropriate to the type and level of risks posed by the nature and scope of a bank's activities;
- The bank's organisational structure should establish clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits;
- reporting lines should provide sufficient independence of the control areas from the business lines and adequate separation of critical functions throughout the bank, such as those relating to trading, custodial and back-office activities¹;
- official bank structures should reflect actual operating practices;
- financial, operational and regulatory reports should be reliable, accurate and timely; wherever applicable, exceptions should be noted and promptly investigated;
- adequate procedures for ensuring compliance with applicable laws and regulations should be in place;
- internal audit or other control review practices should provide for independence and objectivity;
- internal controls and information systems should be adequately tested and reviewed; the coverage, procedures, findings and responses to audits and review tests should be adequately documented; identified material weaknesses should be given appropriate and timely high level attention; and Management's actions to address material weaknesses should be objectively verified and reviewed; and
- the bank's audit committee or board of directors should review the effectiveness of internal audits and other control review activities on a regular basis.

(d) Risk Management Function

3.27 Every bank should establish a risk management function (function) headed by a senior management official (executive level), which oversees risk-management strategies employed by a bank. The function should be independent of those that take or accept risks on behalf of a bank and should report directly, functionally to the board or relevant sub-committee of the board.

¹ For example: business origination, payments, reconciliation, risk management, accounting, audit and compliance.

3.28 The risk management function should ensure that effective processes are put in place for:

- (i) identifying current and emerging risks;
- (ii) developing risk assessment and measurement systems;
- (iii) establishing policies, practices and other control mechanisms to manage risks;
- (iv) developing risk-tolerance limits for senior management and board approval;
- (v) monitoring positions against approved risk-tolerance limits; and
- (vi) reporting results of risk monitoring to senior management and the Board.

(e) Risk Disclosures

3.29 A bank should make sufficient public disclosures that would allow stakeholders to determine whether it identifies, assesses, monitors and controls/mitigates risks effectively. The amount and type of disclosures should correspond with the size, risk profile and complexity of the bank's operations, and evolving industry practices. The disclosures must include, at least, the following elements:

- (i) A formal disclosure policy approved by the board of directors, which addresses the bank's approach to determining what risk disclosures it will make and the internal controls over the disclosure process;
- (ii) Implement a process for assessing the appropriateness of the bank's disclosures, including the verification and the frequency of the disclosures. The disclosures should be consistent with how senior management and the board assess and manage the risk of the bank; and
- (iii) The public relations function of the bank or its designate should manage the communication of information to the market, so that it either builds reputation or minimises the impact of adverse reputation risk events. It should also be responsible for monitoring a bank's reputation within the market place. Depending on the nature, size and complexity, and the risk profile of a bank, the specifics of the governance structure of the public relations function may vary.

3.30 These risk-management disclosures must, at a minimum, meet the requirements under Pillar III of Basel II.

(f) Risk Capital

3.31 Consistent with the Basel II Directive, a bank must hold Basel II compliant capital to cushion all risks.

3.32 In addition, a bank must ensure that well-defined processes are in place to assess its capital adequacy in relation to its risk profile. Based on the material risks identified, a bank should assess its overall capital adequacy, and develop a strategy for maintaining capital levels consistent with its risk profile and business plans. This

should be reflected in a bank's capital planning process and the setting of internal capital targets. The capital planning process must be dynamic and forward-looking in relation to a bank's risk profile. In addition, a bank should have a robust system for the continuous monitoring and reporting of risk exposures, and assess how its changing risk profile affects its capital.

- 3.33 For risks that are not easily quantifiable or related to capital, focus should be directed at ensuring the effectiveness of their management and mitigation. Adequate systems and processes for managing these risks should be put in place and implemented effectively, with consideration for providing appropriate capital for any residual risks that cannot be reduced to satisfactory levels.

(g) Supervisory Expectations

- 3.34 In the discharge of their functions, supervisors shall apply a risk-based supervisory approach to assess risk in a broader context than that reflected by the balance sheets of individual banks. That is, the supervisory "risk perimeter" shall extend beyond accounting consolidation concepts. In this regard, when compiling a bank's risk profile, the supervisor should consider risks arising from within an individual bank (solo perspective), from its associated entities (banking group and group-wide basis) or from the prevailing macroeconomic environment. This is in line with the requirements of Principle 8 of the Basel Core Principles for Effective Banking Supervision, that requires the supervisor to develop and maintain a forward-looking assessment of the risk profile of individual banks and banking groups, proportionate to their systemic importance; as well as to identify, assess and address risks emanating from banks.
- 3.35 Consistent with the Basel II Directive, the supervisor shall ensure that banks periodically disclose to the market their risk-management practices to promote and maintain public confidence. Such risk disclosure and transparency will allow market participants to understand more fully a bank's risk profile and thereby reduce market uncertainties about the bank's financial strength.

(h) External Auditors

- 3.36 Consistent with the requirements of the Banking Act, relevant accounting standards and international best practice and Guidelines on banks' audit committees, annual independent external audit and publication of audited financial statements, a bank's external auditor should monitor its compliance with the requirements of these guidelines. Where there is a breach or non-compliance, such auditor must notify the Bank as soon as practical. Furthermore, the auditor should always communicate in writing to those charged with governance all significant audit findings and reportable matters, including poor risk management practices.

4. STRATEGIC RISK MANAGEMENT

4.1 Strategic risk is a possible source of loss that might arise from the pursuit of an unsuccessful business plan. For example, strategic risk might arise from making poor business decisions, from the substandard execution of decisions, from inadequate resource allocation, or from failure to respond adequately to changes in the business environment.

4.2 Strategic risk can arise from either internal or external risk factors. Internal factors are under the control of the bank and can affect or deter the implementation of the strategic plan. Such factors include the organisational structure; culture, work processes and procedures; personnel; and information and technology. External risk factors are factors which the bank has minimal or no control over and can also affect or deter the realisation of the goals determined in the strategic plan. Such factors may include competition; change of target customers; technological changes; economic factors and regulations.

(a) Strategic Planning Process

4.3 A bank should put in place a strategic plan, which should be supported by a realistic budget. A strategic plan clarifies a bank's overall purpose, defines goals and priorities and determines practical approaches for achieving targeted priorities. Therefore, it should encompass the following:

- (i) support or participation of the board, delegated committees, senior management and staff from various departments;
- (ii) adequacy of information in developing assumptions in relation to economic factors, technological changes, changes in law, position of the bank compared to competitors, current competitive position, future market trends and customer needs, among others;
- (iii) consistency of the operational plans with the overall objective of a bank;
- (iv) assessment of actual performance against strategic plans; and
- (v) a bank should periodically evaluate actual performance against the strategic plan in order to monitor and adjust its plans appropriately. The evaluation should be measurable, and with adequate frequency.

(b) Strategic Risk Identification

4.4 Identification and measurement of strategic risk can be determined through strategic planning and the preparatory process of a strategic plan. Both the strategic plan and the operational plan, as well as the budget, should be consistent with the business scope, complexity, external environment and internal factors of the bank, including the size and resources.

4.5 The strategic risk management policy should provide general guidelines to strategic risk management. The policy should contain at least the following: definition of strategic risk; sources of strategic risk; risk mitigation factors and a bank's accepted tolerance for strategic risk exposure.

4.6 Management should fully participate and carefully decide on the basis of information that business and strategic plans are feasible and appropriate. Management should ensure good communication and cooperation between all employees and departments involved in the strategic planning process.

(c) Strategic Risk Measurement

4.7 A bank should establish and maintain a management information system (MIS) which enables the board to identify and measure the risks associated with the bank's strategic plan. The level of sophistication of the system should depend on the nature, scale and complexity of the business segments within the business plan of a bank. The MIS should enable Management to monitor:

- (i) current and forecast economic conditions;
- (ii) current and forecast industry and market conditions;
- (iii) exposure to different sectors and associated sector risks; and
- (iv) mechanisms that are in place to identify exceptions to limits and guidelines, and corrective action required.

(d) Strategic Risk Mitigation, Monitoring and Control

4.8 A bank needs strong internal control systems to ensure that it is not unduly exposed to strategic risks. Hence, a bank should adopt and implement robust strategic risk mitigation measures and techniques to enhance the achievement of strategic objectives. These include engaging requisitely qualified and experienced board and Management, formulation of strategic and operational plans, high quality personnel and proper training, comprehensive risk-management systems and adequate access to information, as well as timely and efficient introduction of new products or services. Internal controls should ensure that:

- (i) a bank's structure establishes clear lines of authority;
- (ii) a bank's systems and structures provide for business continuity planning; and
- (iii) the process of setting up and reviewing strategic and business plans are comprehensive and carefully adhered to.

4.9 Internal and external audits are integral to the implementation of a risk-management process to control risk associated with a bank's business strategy. To carry out their function effectively, Internal Auditors should have appropriate skills, knowledge and authority as well as independence within a bank to ensure that senior management reacts to and acts upon their recommendations.

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

(e) Strategic Risk Reporting

4.11 The reporting of strategic risk should be entrusted to an independent functional unit within a bank. Reporting could be in the form of performance reporting, on-going monitoring and/or appraisal to the board.

4.12 In order to enable effective risk reporting, the board and senior management should ensure the availability of information systems which can identify and measure strategic risk in an accurate, reliable and regular manner. The information systems should be able to provide information required to support implementation of a bank's strategic plans. Therefore, the information systems should be able to collect financial, accounting and other data, such as data on economic conditions, competition, technology and regulatory requirements. Furthermore, to remain effective, a bank should review its MIS regularly and subject it to regular upgrades and modification.

4.13 Reporting should be done, at least once a year; in order to provide timely and adequate information to judge the changing nature of the bank's strategic risk profile and evaluate compliance with the stated policy objectives and constraints. This notwithstanding, any material changes of information on a bank's strategic risk profile or other items of the strategic plan prone to rapid change must be reported in the interim.

5. CREDIT RISK²

- 5.1 This section provides guidance on sound practices in credit risk management. While the principles contained in this section are, in the main, applicable to the business of lending, should be applied to all activities where credit risk is present.
- 5.2 Credit risk is defined as the risk that a counterparty will fail to perform fully its financial obligations, or the potential that a bank borrower or counterparty will fail to meet its obligations in accordance with agreed terms. It could arise from multiple activities, such as default of loan or bond obligation, or from the guarantor, credit enhancement provider or derivative counterparty failing to meet its obligations. Credit risk also includes credit concentration risk and insider lending.
- 5.3 The goal of credit risk management is to maximise a bank's risk-adjusted rate of return by maintaining credit risk exposures within acceptable parameters. A bank needs to manage the credit risk inherent in the entire portfolio, as well as the risk in individual credits or transactions. The effective management of credit risk is a critical component of a comprehensive approach to risk management and is essential to the long-term success of any banking organisation.
- 5.4 For most banks, loans are the largest and most obvious source of credit risk. However, other sources of credit risk exist throughout the activities of a bank, including in the banking book and trading book, and both on and off-balance sheet items. For example banks face credit risk (or counterparty risk) in various financial transactions other than loans, including on inter-bank transactions, trade financing, foreign exchange transactions, financial futures, swaps, bonds, equities, options, and in the extension of commitments and guarantees, and the settlement of transactions.
- 5.5 The sound practices for the effective management of credit risk set out in this section addresses the following areas:
- (a) Credit risk management, policies and procedures;
 - (b) Credit risk identification and measurement;
 - (c) Credit risk monitoring and control; and
 - (d) Credit risk reporting.
- (a) Establishing an Appropriate Credit Risk Environment
- 5.6 A bank should formulate and implement a structured credit risk management strategy, which will include credit-risk policies and related processes. The strategy should be approved and reviewed regularly (at least annually) by the board of directors. The strategy and policies should cover the various activities of the bank

² Reference Documents: Guidelines on the Revised International Convergence of Capital Measurement and Capital Standards for Botswana (Basel II) (September 8, 2015); Basel Core Principles for Effective Banking Supervision (September 2012) (Principles 17, 18, 19, 20 and 21); Principles for the Management of Credit Risk (September 2000).

in which credit exposure is a significant risk and should reflect the bank's risk appetite, risk profile and capital strength.

- 5.7 The credit-risk strategy should establish the objectives for assuming, identifying, measuring, monitoring, reporting and controlling or mitigating credit risk.
- 5.8 Sound credit risk management involves managing the risk and reward relationship and controlling and minimising credit risk across a wide spectrum, such as exposure type, economic sector, geographical location, currency, maturity, target markets, desired portfolio mix and anticipated profitability. This might also include identification of target markets and other desirable outcomes such as levels of diversification and concentration tolerance.
- 5.9 A bank's comprehensive credit risk management programme should:
- (a) identify existing or potential credit risks to which the bank is exposed in conducting its business activities and developing and implementing sound and prudent credit policies to effectively manage and control these risks;
 - (b) develop and implement effective credit granting, documentation and collection processes; and
 - (c) develop and implement comprehensive procedures to effectively monitor and control the nature, character and quality of the credit portfolio.
- 5.10 The Management of a bank should implement the credit strategy approved by the board of directors. The board should ensure that senior management is fully capable of managing the credit activities conducted by the bank and that such activities are effected based on the risk strategy, policies and tolerance levels approved by the board.
- 5.11 The senior management of a bank should develop policies and procedures for identifying, measuring, monitoring and controlling credit risk. The policies should be designed and implemented in the context of internal and external factors such as the bank's level of capital, management and staff capabilities, credit needs in the bank's market area, anticipated future growth and technology.
- 5.12 Policies and procedures that are properly developed and implemented should enable the bank to:
- (a) maintain sound credit-granting standards;
 - (b) identify, measure, monitor and control credit risk at both individual and portfolio levels;
 - (c) properly evaluate new business opportunities; and
 - (d) identify and administer problem credits.
- 5.13 For a bank's credit policy to be considered adequate, it should, at a minimum, address the following:

- (i) types of credit offered by the bank, by exposure type (commercial, consumer, real estate, etc.), economic sector, geographic location, currency, maturity, target markets and desired portfolio mix;
 - (ii) guidelines which, at a minimum, address the goals for portfolio mix and risk diversification, and the bank's plans for monitoring and taking appropriate corrective action, if deemed necessary, on any concentrations that may exist;
 - (iii) detail the structure of the credit approval authority and process, approval limits and approval lending authority of each loan officer, management or board credit committee, including procedures for granting exceptions;
 - (iv) responsibility of the board of directors in reviewing, ratifying or approving loans;
 - (v) indicate acceptable collateral and terms and conditions under which unsecured loans would be granted;
 - (vi) terms and conditions for both price and non-price related items, including maturity and payment structure, interest rate, fees and collateral;
 - (vii) limitations on the maximum volume of credits, individually and by exposure type;
 - (viii) credit documentation, monitoring and classification;
 - (ix) appropriate and adequate collection procedures, including, but not limited to, actions to be taken against borrowers who default; and
 - (x) reporting and internal communication of exceptions.
- 5.14 A bank should provide a system to conduct credit risk management under Directive on the Revised International Convergence of Capital Measurement and Capital Standards for Botswana (Basel II) in a manner suited to the risk management approach it has adopted.
- (b) Credit Risk Identification and Measurement
- 5.15 A bank should have methodologies that enable it to quantify the risk involved in exposures to individual borrowers or counterparties. A bank should use measurement techniques that are appropriate to the complexity and level of the risks involved in its activities, based on robust data, and subject to periodic validation (e.g., externally validated internal rating model).

- 5.16 A bank should have objective and precise statistical techniques, such as value at risk, for the measurement of credit risk quantity. A bank should also be able to analyse credit risk at the product and portfolio level, in order to identify any particular sensitivities or concentrations.
- 5.17 A bank should have a management information systems (MIS) and analytical techniques that enable Management to measure the credit risk inherent in all on and off-balance sheet activities. The MIS should provide adequate information on the composition of the credit portfolio, including identification of any concentrations of risk.
- 5.18 The bank's information system should be able to aggregate credit exposures to individual borrowers and counterparties by type, economic sectors, country, geographical area and currency.
- 5.19 The bank's MIS should monitor actual exposures against established limits and all exposures should be included in a risk-limit measurement system. The exposures approaching risk limits should be brought to the attention of senior management. Exceptions to credit-risk limits should be reported to senior management, on a meaningful and timely basis.
- 5.20 The measurement of credit risk should take into account:
- (i) the specific nature of the credit (loan, derivative, overdraft, etc.) and its contractual and financial conditions (maturity, reference rate, etc.);
 - (ii) the exposure profile until maturity in relation to potential market movements;
 - (iii) the existence of credit risk mitigants, such as collateral or guarantees; and
 - (iv) the potential for default based on the internal credit risk rating.
- 5.21 A bank should periodically employ stress testing and back testing in evaluating the quality of its credit risk-assessment models and establish internal tolerance limits for differences between expected and actual outcomes; and have processes for updating limits, as conditions warrant. The validation of internal credit risk assessment models should be subject to periodic review by qualified, independent individuals (e.g., internal, external auditors and bank supervisors):
- 5.22 Stress testing of the credit portfolio should involve identifying possible events or future changes in economic conditions that could have unfavourable effects on a bank's credit exposures and assessing the bank's ability to withstand such changes. Three areas that a bank could usefully examine are:

- (a) economic or industry downturns (both in the whole economy and in particular sectors);
 - (b) market risk events (interest rate risk and foreign exchange risk); credit-risk events higher than expected levels of delinquencies and defaults; and
 - (c) liquidity conditions.
- 5.23 Stress testing could range from relatively simple alterations in assumptions about one or more financial, structural or economic variables to the use of highly sophisticated financial models.
- 5.24 The output of the tests should be reviewed periodically by senior management and appropriate action taken in cases where the results exceed agreed tolerances. Stress-test analyses should include contingency plans regarding actions management might take given certain scenarios. The output should also be incorporated into the process for assigning and updating policies and limits.

Credit Granting Processes

- 5.25 A bank should operate within sound, well-defined credit-granting criteria. These criteria should include a clear indication of the bank's target market and a thorough understanding of the borrower or counterparty as well as the purpose and structure of the credit and its source of repayment.
- 5.26 A bank's credit-granting approval process should establish accountability for decisions taken and designate who has the absolute authority to approve credits or changes in credit terms. Approval authorities should be commensurate with the expertise of the individuals involved.
- 5.27 Each bank should develop a clear understanding of the credit risk involved in more complex credit-granting activities. For example, loans to certain industry sectors, asset securitisation, customer-written options, credit derivatives (e.g., credit swaps, interest rate swaps) and credit-linked notes.
- 5.28 All extensions of credit should be made free of conflict of interest and on an arm's-length basis. Extensions of credit should be made subject to the criteria and processes described in the bank's credit granting process.
- 5.29 Material transactions³ with related parties should be subject to the approval of the board (excluding board members with conflict of interest), and in certain circumstances (e.g., a large loan to a major shareholder) reported to the Bank.

³ Refer to Section 17 of the Banking Act Cap. 46:04 and Banking Regulation 9 for material transactions. Also refer to Guidelines on Transactions with Related Parties and Guidelines on Large Exposures

5.30 A bank that participates in loan syndications or other such loan consortia should not place undue reliance on the credit risk analysis done by the lead underwriter or on external commercial loan credit ratings. All syndicate participants should perform their own due diligence, including independent credit risk analysis and review of syndicate terms prior to committing to the syndication. Each bank should analyse the risk and return on syndicated loans in the same manner as directly sourced loans.

5.31 A bank could utilise techniques to mitigate credit risk consistent with the standardised approach for credit risk as outlined in Annexure 3 of the Basel II Directive. Transactions should, however, be entered into primarily on the strength of the borrower's credit worthiness and ability to repay the facility in accordance with the agreed terms. Collateral should neither be a substitute for a comprehensive assessment of the borrower or counterparty nor should it compensate for insufficient information. A bank should have policies covering the acceptability of various forms of collateral, procedures for the ongoing valuation of such collateral and a process to ensure that collateral is, and continues to be, enforceable and realisable. With regard to guarantees, a bank should evaluate the level of coverage being provided in relation to the credit quality and legal capacity of the guarantor.

(c) Credit Risk Monitoring and Control

5.32 A bank should develop appropriate credit limits, consistent with the bank's risk appetite, risk profile and capital strength which are understood by, and regularly communicated to all relevant staff. Limits should be defined in line with the existing Guidelines on Large Exposures and a bank must ensure that it complies with these guidelines.

5.33 A bank should have procedures to identify situations where, in considering credits, it is appropriate to classify a group of obligors as connected counterparties and, thus, as a single borrower. This would include aggregating exposures to a group of accounts exhibiting financial interdependence, including corporate or non-corporate, where they are under common ownership or control or with strong connecting links. A bank should have procedures for aggregating exposures to individual clients across business activities.

5.34 A bank should establish overall credit limits at the level of individual borrowers and counterparties, and groups of connected counterparties that aggregate in a comparable and meaningful manner, the different types of exposures, both in the banking and trading book and on and-off-balance sheet. The limits should also be established for particular industries or economic sectors, countries, geographic regions and specific products. The limits established should comply with those stipulated in the Banking Act, Regulations and/or Guidelines, where necessary.

5.35 A bank may manage credit concentrations and other portfolio issues using such mechanisms as loan sales, credit derivatives, securitisation programmes and other secondary loan markets, provided that it has policies and procedures, as well as adequate controls, in place for these mechanisms.

- 5.36 A bank is encouraged to develop and utilise an internal credit risk rating system in managing and monitoring credit risk. The rating system should be consistent with the nature, size and complexity of a bank's activities. Large loans, as determined by the board, must be individually assessed and rated using the internal credit grading (rating) system. Other smaller loans or groups of smaller loans (i.e., schemes), may be classified on the basis of either a credit risk grading system, payment delinquency status or credit scoring system.
- 5.37 Where internal ratings are assigned to an individual borrower or counterparty at the time the credit is granted, such rating should be reviewed on a periodic basis and be assigned a new rating when conditions either improve or deteriorate. It is also important that the consistency and accuracy of ratings is examined periodically by a function such as an independent credit review group.
- 5.38 A bank must validate internally generated credit ratings/scoring by mapping such ratings to the ratings of the recognised external credit rating agencies outlined in the Revised Directive on the International Convergence of Capital Measurement and Capital Standards for Botswana.
- 5.39 Exposures with credit risk grades for individually assessed loans that are either large, complex, high risk, deteriorating ratings or problem credits should be subject to additional oversight and monitoring; for example, through more frequent visits from credit officers and inclusion on a watch list that is regularly reviewed by the board and senior management. The internal credit risk ratings could be used by line management in different departments to track the current characteristics of the credit portfolio and help determine necessary changes to the credit strategy of the bank.
- 5.40 A bank should maintain proper documentation for each credit accommodation. Credit documentation requirements for each type of credit accommodation offered by the bank should be listed in its credit granting standards.
- 5.41 The credit files should include all the information necessary to ascertain the current financial condition of the borrower or counterparty, as well as sufficient information to enable decision making. Credit files should, at a minimum, include credit application, current financial statements, financial analysis, record of all credit reviews, reference letters, appraisal, record of all guarantees and securities, record of terms and conditions of the facility and internal credit ratings.

Asset/Credit Classification

- 5.42 At the minimum, a bank should classify its assets into the following regulatory credit classification categories:

(a) Standard or Pass

5.43 A credit is in the “pass/standard category if there are no:

- (i) Material or significant performance problems (the credit is current and the borrower is complying, and is expected to continue to comply, with all terms of the contract); or
- (ii) Technical and/or legal documentation deficiencies.

(b) Special Mention or Watch

5.44 A credit should be in the “special mention” or watch category if it is currently protected, but potentially weak. That is, assets with potential weaknesses that may, if not checked or corrected, weaken the asset as a whole or potentially jeopardise a borrower’s repayment capacity in the future. This would, for example, include credit given through inadequate loan agreement or covenants, a lack of control over collateral, or incomplete or inadequate documentation, as well as adverse trends which are not yet serious enough for a classification of Substandard.

(c) Substandard

5.45 A credit should be classified as “sub-standard” if it has one or more well-defined weaknesses that make the full collection of principal and interest questionable. This would include, for example, (i) deterioration of the borrower’s financial condition, including net worth and/or repayment capacity; (ii) the pledged collateral (if any) is undocumented, insufficient, or deteriorating; (iii) the borrower’s financial information is absent or unsatisfactory; (iv) other adverse factors exist, which cause concern regarding the ability of the borrower to repay the credit in accordance with the existing repayment terms, such as delinquency of 90 days, significant deviation from original source of repayment or carryover debt; and/or (v) an actual breach of the contract has occurred.

5.46 All accommodations that are three (3) months in arrears should be, at a minimum, be classified as “Substandard”.

(d) Doubtful

5.47 A credit shall be classified as “doubtful” when weaknesses exist which make collection or repayment in full, highly questionable and improbable based upon currently existing circumstances, conditions and the estimated recoverable amount of the pledged collateral (if any). Such credits generally display high levels of delinquency and the possibility of loss is very high. However, because of certain important and reasonably specific pending factors, which may work to the advantage and strengthening of the credit, classification of the credit as “loss” is deferred until its more exact status is determined. Pending factors may include a merger/acquisition and capital injection. .

5.48 All accommodations that are four (4) to six (6) months in arrears should be, at a minimum, be classified as “doubtful”.

(e) Loss

5.49 At the time of classification, the credit is deemed uncollectable and of such little value that it should not continue to be included on the accounts and financial statements of the bank. The classification of credit as loss does not mean that the credit has no recovery or salvage value, but that the bank should not defer writing it off even though at least part of the value could be recovered in the future. Such classification does not cancel the borrower’s obligation to repay, nor does it mean that the bank should not continue to exercise its full legal right to collection or payment. Loans classified as loss may have severe delinquency, unsecured and/or not well secured and not in the process of collection. Overdrafts considered loss may be hardcore, stagnant for a long period of time and unsecured or not well secured.

5.50 All accommodations that are more than six (6) months in arrears should be considered for classification as “Loss”,

Performing and Non-Performing Status of Credit Exposures

5.51 For regulatory reporting and disclosure purposes, credit exposures shall be broadly categorised as “performing” and “non-performing”; where performing exposures shall consist of “standard” exposures and “special mention” exposures (subject to such exposures not having significant credit risk as per the prevailing accounting standards). Non-performing exposures shall consist of all “special mention” exposures with significant credit risk as per applicable accounting standards, sub-standard, doubtful and loss, as well as all credit exposures that meet the definition of non-performing loans outlined in paragraphs 5.54-5.57 below.

Mapping Regulatory Non-performing Assets (NPA) Frameworks with the Accounting Concept of Impaired Assets – Interim Approach

5.52 A bank should map the five regulatory categories of credit exposures onto the accounting concept of impaired assets (IFRS 9) as detailed below. Pass credit exposures shall map onto Stage 1. Stage 3 shall consist of sub-standard, doubtful and loss exposures, while the special-mention exposures shall be disaggregated into performing and non-performing (as per paragraph 5.51) and the performing portion would form part of Stage 1, while the non-performing portion will map onto Stage 2.

	Regulatory Credit Exposure Categorisation				
	Standard/ Pass	Special Mention/Watch	Sub- Standard	Doubtful	Loss
	Performing		Non-performing		
IFRS 9 Categorisation	Stage 1	Stage 2	Stage 2	Stage 3	

Frequency of asset classification

- 5.53 Asset reclassification should be done on a monthly basis. However, if between these reviews the bank gains knowledge of a significant deterioration in the quality of an individual credit or in part of the bank's portfolio, the bank should reclassify such credit exposures to reflect their true status.

Identification of non-performing exposures

- 5.54 Non-performing exposures should always be categorised for the whole exposure, including when non-performance relates to only a part of the exposure, for instance, unpaid interest. For off-balance sheet exposures, such as loan commitments or financial guarantees, the whole exposure is the entire cancellable nominal amount.
- 5.55 The following exposures shall be considered as non-performing:
- (a) all exposures that are "defaulted" under the Basel II framework;
 - (b) all exposures that are credit-impaired (having experienced a downward adjustment to their valuation due to deterioration of their creditworthiness) according to the applicable accounting framework;
 - (c) all other exposures that are not defaulted or impaired but nevertheless:
 - (i) are material exposures that are more than 90 days past due; or
 - (ii) where there is evidence that full repayment based on the contractual terms, original or, when applicable, modified (e.g., repayment of principal and interest) is unlikely without the bank's realisation of collateral, whether or not the exposure is current and regardless of the number of days the exposure is past due.
 - (d) forborne exposures⁴ should be identified as non-performing when they meet the specific criteria provided for in this definition.
- 5.56 Collateralisation or received guarantees should have no direct influence on the categorisation of an exposure as non-performing. That is, the collateralisation or guarantee status does not influence the past-due status, including the counting of past-due days and the determination of the exposure as nonperforming, once the materiality and overdue days threshold have been met. When the relevant criteria are met, an exposure should be categorised as non-performing even if the collateral value exceeds the amount of the past-due exposure.

⁴ See paragraph 5.59

Re-categorisation of non-performing exposures as performing

5.57 An exposure ceases to be non-performing and can be re-categorised as performing when all the following criteria are simultaneously met:

- (a) the counterparty does not have any material exposure more than 90 days past due;
- (b) repayments have been made when due over a period of at least three continuous months as specified by the supervisor. A longer repayment period shall be required for non-performing forborne exposures as detailed in paragraphs 5.58 – 5.64;
- (c) the counterparty's situation has improved to the extent that the full repayment of the exposure is likely, according to the original or, when applicable, modified conditions; and
- (d) the exposure is not "defaulted" according to the Basel II standard or "impaired" according to the applicable accounting framework.

5.58 The following situations will not lead to the re-categorisation of a non-performing exposure as performing:

- (a) partial write-off of an existing non-performing exposure, (i.e., when a bank writes off part of a non-performing exposure that it deems to be uncollectible);
- (b) repossession of collateral on a non-performing exposure, until the collateral is actually disposed of and the bank realises the proceeds (when the exposure is kept on balance sheet, it is deemed non-performing); or
- (c) extension or granting of forbearance measures to an exposure that is already identified as non-performing subject to the relevant exit criteria for non-performing exposures. The re-categorisation of a non-performing exposure as performing should be made at the same level (i.e., at counterparty or transaction level) as when the exposure was originally categorised as non-performing.

Identification of forbearance

5.59 Forbearance includes concessions that are granted due to the counterparty's financial difficulty on any exposure in the form of a loan, a debt security or an off-balance sheet item (e.g., loan commitments or financial guarantees) regardless of the measurement method for accounting purposes.

5.60 The identification of an exposure as forborne does not affect its categorisation as impaired for accounting purposes or as defaulted in accordance with the regulatory framework.

- 5.61 Refinancing an existing exposure with a new contract due to the financial difficulty of a counterparty could qualify as a concession, even if the terms of the new contract are no more favourable for the counterparty than those of the existing transaction.
- 5.62 A forbore exposure will be identified as such until it meets both of the following exit criteria:
- (a) When all payments, as per the revised contractual terms, have been made in a timely manner over a continuous repayment period not less than one year (probation period for reporting). The starting date of the probation period should be the scheduled start of payments under the revised terms, regardless of the performing or non-performing status of the exposure at the time that forbearance was granted; and
 - (b) The counterparty has resolved its financial difficulty.
- 5.63 Forbearance may be granted on performing or non-performing exposures. When forbearance is applied to a non-performing exposure, the exposure should remain non-performing. When forbearance is applied to a performing exposure, the bank then needs to assess whether the exposure meets the non-performing criteria, even if the forbearance resulted in a new exposure. When the original exposure would have been categorised as non-performing at the time of granting forbearance, had the forbearance not been granted, the new exposure should be categorised as non-performing.
- 5.64 When a forbore exposure under the probation period is granted new forbearance, this should trigger a re-start of the probation period, and banks should consider whether the exposure should be categorised as non-performing. Similarly, when a forbore exposure becomes non-performing during the 12-month probation period, the probation period starts again.
- 5.65 A bank must not use forbearance practices to avoid categorising loans as non-performing. Therefore, the definition prohibits the upgrading of a non-performing exposure by granting forbearance measures and requires a separate categorisation for forbearance exposures.

Treatment of Accrued Interest on Impaired Credits

- 5.66 Accrued interest on any loan in arrears exceeding three months should be suspended. Such accrued interest should only be released to income when both the interest and the past due principal amounts have been collected in cash. This principle should be applied to overdrafts in excess of authorised limits and any other credits, investments, etc., which do not perform in accordance with agreed terms for a defined period, in this case 90 days and above.
- 5.67 A bank should cease to accrue interest on a credit as soon as it is identified as impaired. At a minimum, the following credits should be placed on non-accrual status:

- (i) All adversely classified credits
- (ii) Credits 90 days or more past due. (A bank may determine in its own credit policy that certain types of credits should be subject to non-accrual when delinquent for less than 90 days).

Capital Requirements for Impaired Credits (non-performing for more than 90 days)

- 5.68 A bank should hold capital for any unsecured portion of any loan that is past due for more than 90 days, net of specific provisions (including partial write-offs), as prescribed in the Basel II Directive.

Credit Impairment Provisions

- 5.69 A bank must compute credit impairment provisions in terms of the relevant accounting standards and such provisions shall be accordingly mapped onto the corresponding prudential credit exposure categorisation.

Loan-Loss Provisioning Policy

- 5.70 A bank should develop and implement comprehensive procedures and information systems to monitor the quality of its loan portfolio. These procedures should define criteria for identifying and reporting potential problem credits and other transactions to ensure that they are subject to more frequent monitoring, as well as possible corrective action, classification and/or provisioning.
- 5.71 A loan should be identified as a problem asset when there is reason to believe that all amounts due, including principal and interest, will not be collected in accordance with the contractual terms of the loan agreement. A loan should be re-classified as performing when all arrears have been cleared and the loan has been brought fully to current status; repayments have been made in a timely manner over a continuous period (with evidence of continued collection), in accordance with the agreed contractual terms.
- 5.72 A loan shall be classified as impaired if the bank considers that the obligor is unlikely to pay its credit obligations to the bank in full, without recourse by the bank to the legal actions allowed under the agreement and law, such as realising security (if held); and/or the obligor is past due for more than 90 days on any material credit obligation to the bank. Overdraft facilities will be considered as being impaired once the customer has breached an advised limit.
- 5.73 A bank's provisioning policy should clearly set out how the bank will manage problem credits. Responsibility for such credits may be assigned to the originating business function, a specialised workout section, or a combination of the two, depending upon the size and nature of the credit and the reason for its problems.

- 5.74 Loan accounting policies and practices should be selected and applied in a consistent way that reasonably ensures that the loan and loan loss provisioning information is reliable and verifiable.
- 5.75 The provisioning policy and processes should ensure that the bank maintains adequate provisions for identified and expected losses in accordance with the prevailing applicable accounting standards. In addition, a bank must provision for expected credit losses (ECL) from the time a loan is originated, rather than awaiting “trigger events” signaling imminent losses. Such provisioning should be forward looking (based on reasonable and supportable information that includes historical, current and forecast information). Furthermore, a bank must hold adequate capital to absorb unexpected losses. The bank’s policies and process for grading and classifying its loans and provisioning should take into account off-balance sheet exposures as well.
- 5.76 A bank is required to ensure that valuation, classification and provisioning for significant exposures are conducted on an individual item basis. A bank should set an appropriate threshold for the purpose of identifying significant exposures and to regularly review set thresholds. The remainder of the portfolio should be segmented into groups of loans with similar credit risk characteristics for evaluation and analysis on a collective basis. A bank may use different methods on group loans for the purpose of assessing credit risk and valuation. For example, loans may be grouped on the basis of one or more of the following characteristics: estimated default probabilities or credit risk grades, loan type, product type, market segment, geographical location, collateral type or past-due status.
- 5.77 A bank should be able to demonstrate, for individually assessed loans that are, or likely to be impaired, how the amount of any impairment is determined and measured. This includes proof of existence of procedures describing the impairment measurement techniques available and steps performed to determine which technique is most appropriate in a given situation. If a bank determines that observable data does not indicate that impairment exists for an individually assessed loan, the bank should include the loan in a group of loans with similar credit risk characteristics for collective impairment evaluation.
- 5.78 For groups of loans that are collectively assessed for impairment, estimated credit losses should reflect consideration of the bank's historical net charge-off rate of the groups, adjusted upward or downward for changes in trends, conditions and other relevant factors that affect repayment of the loans in these groups as of the evaluation date.
- 5.79 In estimating probability of defaults, loss given defaults and loan losses, a bank may determine either a single amount or a range of possible amounts. In the latter case, a bank should recognise an impairment loss equal to the best estimate within the range after considering all relevant information about conditions existing at the measurement date that is available before it completes its prudential reports or financial statements.

- 5.80 Provisions or loan loss reserves held for future or presently unidentified losses which are freely available to meet losses which subsequently materialise, qualify for inclusion within tier II capital. However, provisions ascribed to identified deterioration of particular assets or known liabilities, whether individual or grouped, do not qualify for inclusion as part of tier II capital.

(d) Credit Risk Reporting

- 5.81 A bank should establish a system of independent, on-going assessment of its credit risk management processes and the results of such reviews should be communicated directly to senior management and the board of directors.
- 5.82 A bank should have an efficient internal credit review and reporting system in order to manage effectively the bank's various portfolios. Internal audits of the credit risk processes should be conducted on a periodic basis and it should assess compliance with the bank's credit policies and procedures.

6. MARKET RISK⁵

6.1 Market risk emanates from movements in market prices, in particular, changes in interest rates yields, foreign exchange rates, equity and commodity prices.

6.2 Principle 22 of the Basel Core Principles for Effective Banking Supervision states that a bank must have adequate market risk management processes, which take into account its risk appetite, risk profile, systemic importance and capital strength, by taking into account market and macroeconomic conditions and the risk of a significant deterioration in market liquidity. Prudent policies and processes, as well as roles and responsibilities for the identification, measuring, monitoring and control of market risk, must be clearly articulated.

(a) Market Risk Identification

6.3 A bank should establish a sound and comprehensive process for the identification of market risk, which should, among other things, include the following:

- (i) a framework to identify market risk;
- (ii) an appropriately detailed structure of risk limits, guidelines and other parameters used to govern market risk taking;
- (iii) an appropriate management information system (MIS) for measuring, monitoring and controlling market risk, including transactions between and with related parties; and
- (iv) accounting policies on the treatment of market risk.

6.4 A bank should incorporate a market risk management process into its overall risk management system, to enable it to understand and manage its consolidated risk exposure more effectively. Where a bank is part of a financial services group, the risk management process should also be integrated with that of the group, where practical.

6.5 The market-risk management system should be commensurate with the scope, size and complexity of a bank's trading and other financial activities and the market risks assumed. It should also enable the various market risk exposures to be accurately and adequately measured, monitored and controlled.

(b) Market Risk Measurement

6.6 A bank's risk management system should be able to quantify risk exposures and monitor changes in market risk factors (e.g., changes in interest rates, foreign exchange rates and equity prices) and other market conditions on a daily basis. The

⁵ Reference Documents: Guidelines on Capital Measurements and Capital Standards for Botswana (September 8, 2015); Basel Core Principles for Effective Banking Supervision (September 2012); Principle 22 for the Management of Market Risk (2011) (Principle 22).

risk management system should, wherever feasible, be able to assess the probability of future losses.

- 6.7 A bank must perform stress tests to identify potential vulnerability to exceptional but plausible events or changes in economic conditions on a bank's market risk exposures and assess its ability to withstand such changes. Stress-testing should alert bank management to any adverse unexpected outcomes related to market risk and provide an indication of how much capital might be needed to absorb losses, should large shocks occur.
- 6.8 A bank should ensure that its treasury and financial derivative valuation processes are robust and independent of its trading function. Models and supporting statistical analyses used in valuations and stress tests should be appropriate, consistently applied and have reasonable assumptions. These should be validated before deployment. Staff involved in the validation process should be adequately qualified and independent of the trading and model development functions. Models and analyses should be periodically reviewed to ascertain the position data, the accuracy of volatility, valuation and risk factor calculations, as well as the reasonableness of the correlation and stress test assumptions. More frequent reviews may be necessary if there are changes in models or in the assumptions resulting from developments in market conditions.
- 6.9 The market risk management process should, where appropriate, include regular scenario analysis and stress tests. Scenario analysis and stress tests should be both quantitative and qualitative.
- 6.10 Scenario analysis and stress testing should, as far as possible, be conducted on a bank-wide basis, taking into account the effects of unusual changes in market and non-market risk factors. Such factors include prices, volatilities, market liquidity, historical correlations and assumptions in stressed market conditions, the bank's vulnerability to worst case scenarios or the default of a large counterparty and maximum cash inflow and outflow assumptions.

(c) Market risk Monitoring and Control

- 6.11 A bank should have a business unit dedicated to the management of market risks. Typically, monitoring of market risk is also the responsibility of the asset-liability management committee (ALCO). The ALCO should meet on a frequency that is commensurate with the bank's business activities. The terms of reference, composition, quorum and frequency of meetings should also be formalised and clearly documented.
- 6.12 The board and senior management should regularly review the results of scenario analyses and stress testing for market risk, including the major assumptions that underpin them.

(d) Market Risk Reporting

6.13 Reports detailing the market risk exposure of the bank should be produced using a reliable management information system and reviewed by the board on a regular basis. These reports should, at a minimum, include the following:

- (i) summaries of the bank's aggregate market risk exposures by product, market, currency and duration (e.g., interest rate and foreign exchange exposures and/or any other types of market risk the bank may be exposed to); results of stress tests for market risk, including those assessing breakdowns in key assumptions and parameters;
- (ii) summaries of the findings of reviews of market risk policies, procedures, and the adequacy of the market-risk measurement systems, including any findings of internal and external auditors or any other independent reviewer;
- (iii) reports demonstrating compliance with internal policies and prudential limits on market risk, including exceptions; and

INTEREST RATE RISK⁶

- 6.14 Interest rate risk is the exposure of a bank's on-and off-balance sheet positions to adverse movements in interest rates, resulting in a loss to earnings and, consequently, possible erosion of capital.
- 6.15 The changes in interest rates affect a bank's earnings by altering interest sensitive income and expenses. Interest rate changes also affect the underlying value of a bank'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).
- 6.16 While interest rate risk is assumed by banks as part of normal financial intermediation, excessive interest rate risk poses a significant threat to a bank'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 adverse movements in interest rates.
- 6.17 Principle 23 of Core Principles for Effective Banking Supervision stipulates that banks are required to have an appropriate interest rate-risk strategy and interest rate-risk management framework that provides a comprehensive bank-wide view of interest rate risk. This includes policies and processes to identify, measure, evaluate, monitor, report and control or mitigate material sources of interest rate risk.
- 6.18 An interest rate-risk management process encompasses risk identification, measurement, monitoring and control.
- (a) Interest Rate-Risk Identification
- 6.19 The primary sources of interest rate risk include:
- (i) **re-pricing risk**, which arises from timing differences in the maturity (fixed rate) and re-pricing (floating rate) 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 re-pricing 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 that are either explicit or imbedded in many bank assets, liabilities and off-balance sheet portfolios. If not adequately managed, the asymmetrical pay-off characteristics of instruments with optionality features can pose significant risk, particularly to

⁶ Basel Committee on Banking Supervision (Principle 23) Principles for the Management and Supervision of Interest Rate Risk (2004).

those who sell them, since the options held, either explicit or embedded, are generally exercised to the advantage of the holder, and the disadvantage of the seller.

(b) Interest Rate-Risk Measurement

- 6.20 A bank 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 its activities. The assumptions underlying the risk measurement system should be clearly understood by the board and senior management, who should have an integrated view of interest rate risk across products and business lines.
- 6.21 Interest rate-risk measurement systems should assess the effects of rate changes on both earnings and economic value. In addition, a bank should ensure that all material positions stemming from both on and off-balance sheet positions are incorporated into the measurement system on a timely basis.
- 6.22 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.
- 6.23 The techniques that can be used to measure market risks (i.e., interest rate risk, foreign exchange/currency risk) include gap analysis (maturity/repricing schedule), duration, simulation and value at risk (VaR).

Gap analysis

- 6.24 To evaluate earnings exposure, interest rate-sensitive liabilities in each maturity 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. Therefore, the size of the gap for a given time band gives an indication of the bank’s repricing risk exposure.
- 6.25 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.
- 6.26 A bank should adopt the time bands as specified in the Directive on the Revised International Convergence of Capital Measurement and Capital Standards for Botswana (Basel II).

Duration

- 6.27 Duration is the weighted-average term to maturity of assets/liabilities or the percentage change in the economic value of a position that will occur given a small change in the level of interest rates.
- 6.28 Duration-based weights can be used in combination with the maturity/re-pricing 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. In some cases, different weights should be used for differences in the coupon rates and maturities (for instance, one weight for assets and another for liabilities);
- 6.29 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; and
- 6.30 **A bank should adopt the time bands as specified in the Basel II Directive**

Simulation Approaches

- 6.31 A bank with a complex risk profile or which uses complex financial instruments, should employ more sophisticated interest rate-risk measurement systems than those based on simple maturity/re-pricing 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. The following simulation approaches are recommended:
- (i) Static simulation
 - (ii) Dynamic simulation
 - (iii) Value at risk (i.e., probable loss in a portfolio over a specified period) by using the parametric method or variance/covariance approach, historical simulation; or Monte Carlo method.
- 6.32 A bank using VaR models should carry out back tests.
- 6.33 VaR is not unique to market risk as it can also be used to measure other types of risk, namely, credit and operational risks.

Stress-Testing

- 6.34 A bank must perform stress testing to identify potential vulnerability to exceptional but plausible events on financial risks in general and interest risk exposures, in particular, to assess the bank's ability to withstand such changes or shocks. Stress testing should alert bank management to any adverse unexpected outcomes related

to, say, interest rate risk and provide an indication of how much capital might be needed to absorb losses, should large shocks occur.

- 6.35 The following are typical factors that must be considered when stress-testing for interest rate risk: all likely sources of interest rate risk, including re-pricing risk; basis risk; yield curve risk and optionality risk.
- 6.36 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), for example, an increase 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 the 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 bank's risk profile.
- 6.37 Management and the board should periodically review both the design and results of such stress tests, and ensure that appropriate contingency plans are in place.
- (c) Interest Rate-Risk Monitoring and Control
- 6.38 Interest rate risk management policies and procedures should be clearly defined and consistent with the nature and complexity of a bank's activities.
- 6.39 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 bank procedures for acquiring specific instruments, managing portfolios and controlling a bank's aggregate interest rate risk exposure; and
- (v) clearly define approvals necessary for exceptions to policies, limits and authorisations.

6.40 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 a bank'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) review and approval by the board, at least on an annual basis, of new instruments or new strategies.

6.41 At a minimum, a bank should have limits in the following categories:

- (i) change in the 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.

6.42 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 a bank.

(e) Interest Rate-Risk Reporting

6.43 The board should review interest rate risk reports on a regular basis to assess whether such risk exposures are detailed and, at a minimum, include the following:

- (i) summaries of a bank's aggregate exposures;
 - (ii) a 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.
- 6.44 Reports produced by the bank and external auditors or other outside parties on interest rate risk exposures, should be made available to the supervisory authority.

FOREIGN EXCHANGE RISK⁷

- 6.45 Foreign exchange risk is the potential adverse impact on earnings and economic value due to exchange rate movements. This involves settlement risk, which arises when a bank incurs financial loss due to foreign exchange positions taken in both the trading and banking books. Foreign exchange positions arise from the following activities:
- (i) trading in foreign currencies through spot, forward and option transactions as market maker or position taker, including the unhedged positions arising from customer-driven foreign exchange transactions;
 - (i) holding foreign currency positions in the banking book (e.g., in the form of loans, bonds, deposits or cross-border investments); or
 - (ii) engaging in derivative transactions (e.g., structured notes, synthetic investments and structured deposits) that are denominated in foreign currency for trading or hedging purposes.
- 6.46 There are various forms of risks that can emanate from a foreign exchange transaction, 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.
- 6.47 A bank should, therefore, have a comprehensive risk management framework for all material risks inherent to the lifecycle of a foreign exchange transaction.
- (a) Foreign Exchange-Risk Identification
- 6.48 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;

⁷ Basel Committee on Banking Supervision (Principle 22), Supervisory Guidance for Managing Risk Associated with the Settlement of Foreign Exchange Transactions (2013).

- (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 a bank's expected future cash flows, as a result of an unexpected change in exchange rates or exploded exchange rates.
- (b) Foreign Exchange-Risk Measurement
- 6.49 A bank 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 bank. 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) use a short-hand method where the overall position is computed by taking, in absolute terms, the greater of either net foreign currency liabilities or net foreign currency assets exposures.
 - (iii) employ accepted financial models or methods for measuring risk of foreign exchange options;
 - (iv) be able to calculate comprehensive risk-factor sensitivities for the purpose of capturing the non-linearity nature of price risk of foreign exchange positions;
 - (v) have accurate and timely data;
 - (vi) incorporate daily mark-to-market of trading positions; and
 - (vii) enable banks to monitor their foreign exchange settlement risks in real time, in order to ensure that settlement limits will not be exceeded.
- (c) Stress-Testing on Foreign Exchange Positions
- 6.50 A bank should conduct stress tests on its foreign currency positions. The stress tests assess the impact of changes in exchange rates on the profitability and economic value of a bank's equity. Stress-testing results should be incorporated in the review of business strategies, policies and limits on foreign exchange risk. The assumptions used in the stress-testing model should be clearly documented and reviewed from time to time to reflect changes in the operating environment.

(d) Foreign Exchange-Risk Monitoring and Control

6.51 Foreign exchange-risk monitoring processes should be established to evaluate the performance of a bank's risk strategies/policies and procedures in achieving its overall goals. The monitoring function should be independent of business units taking risk and should report directly to senior management/board. Ordinarily, the middle office, which is responsible for verification of transactions, should perform the risk review function in relation to day-to-day activities. Being a highly specialised function, it should be staffed with people who have relevant expertise and knowledge. The unit should also prepare reports for the information of senior management, as well as the bank's ALCO.

6.52 The middle office should regularly reconcile positions of traders to ensure that they are within assigned limits. Internal reports comparing actual positions against internal limits should be routinely prepared for management. A bank should have management information systems that provide accurate and timely information. Periodic and frequent revaluations at current market rates should permit the monitoring of a bank's profits or losses on its foreign exchange book.

6.53 A comprehensive framework of limits to control foreign exchange-risk exposures should be established for different levels of reporting. The foreign currency exposure thresholds are set at 5 percent for minor currencies, 15 percent for major (i.e., vehicle currencies) and 30 percent for a composite, comprising both minor and major currencies, as a percentage of audited unimpaired capital. At a minimum, a bank should have the following limits for foreign exchange operations:

- (i) open position limits for individual currencies to which a bank has 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.

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

(d) Internal Controls and Independent Audits

6.55 A bank should conduct periodic reviews of its internal control and risk management process for foreign exchange risk to ensure its integrity, accuracy and reasonableness. Such reviews should be conducted by parties independent to the function being reviewed. The reviews should, among others, ensure:

- (i) accuracy and completeness of recording of all foreign exchange transactions;
 - (ii) effective segregation of duties between foreign exchange trading, settlement and accounting functions; and
 - (iii) effectiveness and accuracy of reporting of excesses of limits and other exceptions.
- 6.56 Particular attention should be drawn to irregularities in profit and loss, abnormal foreign exchange 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 foreign exchange trading area should be appropriately and timely elevated to senior management.
- 6.57 A bank 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.
- 6.58 Internal auditors and other risk control functions should be adequately staffed and have sufficient expertise and authority for reviewing the foreign exchange trading business.
- (e) Foreign Exchange-Risk Reporting
- 6.59 The types of reports vary depending upon the overall foreign exchange risk profile of a bank. 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.
- 6.60 A bank is required to report foreign currency positions weekly, as specified in the Foreign Currency Exposure Directive, BOBA 1/04. The Directive prescribes the maximum amount which any bank may hold or the amount of debt which it may incur in foreign currencies, generally or in any specified currency or currencies. The prudential limits are set for exposure per currency and for the overall foreign currency risk exposure in the Directive.

7. LIQUIDITY RISK MANAGEMENT⁸

- 7.1 Liquidity is the ability of a bank to fund increases in assets and/or meet obligations as they become due, without incurring unacceptable capital (or principal amount) losses. The fundamental role of banks in the maturity transformation of short-term deposits into long-term loans makes banks inherently vulnerable to liquidity risk, both of a bank-specific nature and that which affects markets as a whole (market liquidity). Virtually every financial transaction or commitment has implications for a bank's liquidity. Effective liquidity risk management enhances a bank's ability to meet cash flow obligations, which are uncertain, as they are affected by external events and other agents' behaviour. Liquidity-risk management is critical because a liquidity shortfall at a single bank can have system-wide repercussions.
- (a) Liquidity-Risk Identification
- 7.2 A bank should define and identify the liquidity risks to which it is exposed for all legal entities, branches and subsidiaries in the jurisdiction in which it is active.
- 7.3 A bank should evaluate each major on- and off-balance sheet position, including the effect of embedded options and other contingent exposures that may affect the bank's sources and uses of funds, and determine how it can affect liquidity risk.
- 7.4 A bank should consider the interactions between exposures to funding liquidity risk and market liquidity risk. For example, market illiquidity may make it difficult for a bank to raise funds by selling assets and thus increase the need for funding liquidity. Also, this interaction may lead to illiquidity spirals, with banks stock-piling liquidity and not on-lending in the interbank market because of pessimistic assumptions about future market conditions.
- 7.5 A bank should fully factor into its risk management the consideration that asset values may deteriorate under market stress, and take this into account in assessing the feasibility and impact of asset sales during stress on its liquidity position.
- 7.6 A bank should recognise and consider the strong interaction between liquidity risk and other types of risks to which it is exposed. Among others, interest rate, credit, operational and reputational risks, may influence a bank's liquidity profile.
- (b) Measurement and Management of Liquidity Risk
- 7.7 A bank should have a sound process for identifying, measuring, monitoring and controlling liquidity risk. This process should include a robust framework for comprehensively projecting a bank's cash inflows against its outflows, and the liquidity value of its assets to identify the potential for future net funding shortfalls. A bank should measure and forecast its prospective cash flows for assets, liabilities, off-balance sheet commitments and derivatives over an appropriate set of time

⁸ Basel Committee on Banking Supervision (Principle 24), Principles for Sound Liquidity Risk Management and Supervision (2008)

horizons, under normal and stressed conditions and a range of stress scenarios, including scenarios of severe stress.

- 7.8 Regarding the time horizons over which to identify, measure, monitor and control liquidity risk, a bank should ensure that its liquidity risk management practices integrate and consider vulnerabilities to changes in liquidity needs and funding capacity on an intraday basis; day-to-day liquidity needs and funding capacity over short and medium-term horizons up to one year; longer-term liquidity needs over one year; and vulnerabilities to events, activities and strategies that can put a significant strain on internal cash generation capability.
- 7.9 A bank should identify, measure, monitor and control a bank's liquidity risk positions for:
- (i) future cash flows of assets and liabilities;
 - (ii) sources of contingent liquidity demand (financial derivatives; guarantees and commitments) and related triggers associated with off-balance sheet positions;
 - (iii) currencies in which a bank is active; and
 - (iv) correspondent, custody and settlement activities.
- (c) Liquidity-Risk Monitoring and Control
- 7.10 A bank should actively manage its intra-day liquidity positions and risks to meet payment and settlement obligations on a timely basis under both normal and stressed conditions and thus contribute to the smooth functioning of payment and settlement systems.
- 7.11 A bank's liquidity risk governance structure must be led by the ALCO. The committee must have a thorough understanding of the interrelationship between liquidity and other market and credit risk exposures on the balance sheet. The ALCO should also oversee the pricing of liquidity and the review of loan default reports and stress tests results.
- 7.12 A bank should have a reliable management information system (MIS) designed to provide the board of directors, senior management and other appropriate personnel with timely and forward-looking information on the liquidity position of the bank. The MIS should have the ability to calculate liquidity positions in all of the currencies in which the bank conducts business – both on a subsidiary/branch basis in all jurisdictions in which the bank is active and on an aggregate group basis. It should capture all sources of liquidity risk, including contingent risks and the related triggers and those arising from new activities, and have the ability to deliver more granular and time sensitive information during stress events.

- 7.13 To effectively manage and monitor its net funding requirements, a bank should have the ability to calculate liquidity positions on an intra-day basis, on a day-to-day basis for the shorter time horizons, and over a series of more distant time periods thereafter. The MIS should be used in day-to-day liquidity-risk management to monitor compliance with the bank's established policies, procedures and limits.
- 7.14 A bank should set limits to control its liquidity risk exposure and vulnerabilities. Such limits should be relevant to the business in terms of its location, complexity of activity, nature of products, currencies and markets served. Limits should be used for managing day-to-day liquidity within and across lines of business and legal entities under "normal" conditions.
- 7.15 While management and staff have the responsibility to utilise good judgement to identify and manage underlying risk factors, a bank should also design a set of early warning indicators to identify the emergence of increased risk or vulnerabilities in its liquidity risk position or potential funding needs. Early warning indicators can be qualitative or quantitative in nature and should also be able to signal whether embedded triggers in certain products (e.g., callable public debt, OTC derivative transactions) are about to be breached or whether contingent risks are likely to crystallise, which would cause the bank to provide additional liquidity support for the product or bring assets on-balance sheet.
- 7.16 A bank should actively monitor and control liquidity risk, exposures and funding needs at the level of individual legal entities, foreign branches and subsidiaries, and the group as a whole, incorporating processes that aggregate data across multiple systems in order to develop a group-wide view of liquidity risk exposures and identify constraints on the transfer of liquidity within the group.
- 7.17 A bank should establish a funding strategy that provides effective diversification in the sources and tenor of funding. It should maintain an on-going presence in its chosen funding markets and strong relationships with funds providers to promote effective diversification of funding sources. A bank should regularly gauge its capacity to raise funds quickly from each source. It should identify the main factors that affect its ability to raise funds and monitor those factors closely to ensure that estimates of fund raising capacity remain valid.
- 7.18 As a general liquidity management practice, banks should limit concentration in any one particular funding source or tenor. Some banks are increasingly reliant on wholesale funding, which tends to be more volatile than retail funding. Consequently, these banks should ensure that wholesale funding sources are sufficiently diversified to maintain timely availability of funds at the right maturities and at reasonable costs. Furthermore, banks reliant on wholesale funding should maintain a relatively higher proportion of unencumbered, highly liquid assets than banks that rely primarily on retail funding. For banks active in multiple currencies, access to diverse sources of liquidity in each currency is required, since banks are not always able to swap liquidity easily from one currency to another.

- 7.19 An essential component of ensuring funding diversity is maintaining market access. Market access is critical for effective liquidity-risk management, as it affects both the ability to raise new funds and to liquidate assets. Senior management should ensure that market access is being actively managed, monitored and tested.
- 7.20 A bank should actively manage its collateral positions, differentiating between encumbered and unencumbered assets and should monitor the legal entity and physical location where collateral is held and how it may be mobilised in a timely manner.
- 7.21 A bank should conduct stress tests on a regular basis for a variety of short-term and protracted bank-specific and market-wide stress scenarios to identify sources of potential liquidity strain and to ensure that current exposures remain in accordance with a bank's established liquidity-risk tolerance. A bank should use stress test outcomes to adjust its liquidity-risk management strategies, policies, and positions and to develop effective contingency plans.
- 7.22 A bank should have a formal contingency funding plan (CFP) that clearly sets out the strategies for addressing liquidity shortfalls in emergency situations. A CFP should outline policies to manage a range of stress environments, establish clear lines of responsibility, include clear invocation and escalation procedures and be regularly tested and updated to ensure that it is operationally robust.
- 7.23 A bank should maintain a cushion of unencumbered, high-quality liquid assets to be held as insurance against a range of liquidity-stress scenarios, including those that involve the loss or impairment of unsecured and typically available secured funding sources. There should be no legal, regulatory or operational impediment to using these assets to obtain funding.
- (d) Liquidity Risk Reporting
- 7.24 A bank should establish and maintain an MIS that provides senior management officials, the risk management committee and the board of directors with adequate and timely information to:
- (i) monitor a bank's liquidity positions, including trends, in all currencies in which the bank has material activity;
 - (ii) project a bank's liquidity position and future cash flows over different time periods, including daily and longer term, minimum three months, ideally six months, and under alternative scenarios, including stress scenarios;
 - (iii) review liquidity risk exposures on a timely basis;
 - (iii) compare current liquidity exposures with limits established by the board of directors; frustration

- (v) determine compliance with a bank's board-approved policies, procedures and limits and the Bank's liquidity requirements, as prescribed in the Act and Banking Regulations 1995;
- (vi) ensure that the information system enables management to evaluate the level and trends of the bank's aggregate liquidity exposure; and
- (vii) report compliance with prudential regulatory requirements for liquidity.

8. OPERATIONAL RISK MANAGEMENT⁹

- 8.1 Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Therefore, operational-risk management seeks to identify why a loss occurred and at the broadest level includes the breakdown into four causes: people, processes, systems and external factors.
- 8.2 Every bank should establish a comprehensive system, which will enable it to identify, assess, monitor and control or mitigate operational risk. This includes, codifying all policies and procedures for risk management controls, designing the operational-risk assessment methodology and establishing a risk-reporting system for operational risk.
- (a) Operational Risk Culture
- 8.3 A bank with a strong culture of risk management and ethical business practices is less likely to experience potentially damaging operational risk events and it is better placed to deal effectively with those events when they occur.
- 8.4 The board should establish a code of conduct, which sets clear expectations for the integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts. Clear expectations and accountabilities ensure that bank officers understand their roles and responsibilities for risk, as well as their authority to act.
- 8.5 Compensation policies should be aligned to the bank's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They should also appropriately balance risk and reward.
- 8.6 The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume.
- 8.7 Senior management should ensure that all staff members of the bank are accorded training on operational risk. The training should reflect the seniority, role and responsibilities of the individuals for whom it is intended.
- (b) Operational-Risk Identification and Measurement
- 8.8 Senior management should identify and assess the operational risk inherent in all material products, activities, processes and systems to make sure that the inherent risks and incentives are well understood.

⁹ Reference Documents: Guidelines on the Revised International Convergence of Capital Measurement and Capital Standards for Botswana (Basel II) (September 8, 2015); Basel Core Principles for Effective Banking Supervision (Principle 25), and Principles for the Sound Management of Operational Risk (2011)

- 8.9 Effective risk identification considers both internal and external factors. Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively.
- 8.10 The following are some of the tools, which may be used for identifying, measuring and assessing operational risk:
- (i) **Audit Findings:** While audit findings primarily focus on control weaknesses and vulnerabilities, can also provide insight into the inherent risk, due to internal or external factors;
 - (ii) **External Data Collection and Analysis:** External data elements consist of gross operational loss amounts, dates and recoveries. Relevant causal information for operational loss events occurring at organisations other than the bank could be compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures;
 - (iii) **Business Process Mapping:** identifies the key risk points in the overall business process. Process maps can reveal individual risks, risk inter-dependencies and areas of control or risk management weakness;
 - (iv) **Risk and Performance Indicators:** Key performance indicators (KPIs) provide insight into the main drivers of exposure associated with key risks and the status of operational processes, which may, in turn, provide insight into operational weaknesses, failures and potential loss. Risk and performance indicators are often paired, with escalation triggers to warn when risk levels approach or exceed thresholds/limits and/or prompt mitigation measures;
 - (v) **Scenario Analysis:** Scenario analysis involves obtaining expert opinion of business line managers and risk managers to identify potential operational risk events and assess their potential outcome. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process.
 - (vi) **Internal Loss Data Collection and Analysis:** Internal operational-loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. The bank may also find it useful to capture and monitor operational risk contributions to credit and market-risk related losses in order to obtain a more complete view of its operational risk exposure;
 - (vii) **Risk Assessments:** In a risk assessment/risk self-assessment, a bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact. A similar approach, risk control self-assessments (RCSA), evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and

residual risk (the risk exposure after controls are considered). Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment;

- (viii) **Measurement:** Larger banks may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational-risk exposure.
- (ix) **Comparative Analysis:** Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of a bank's operational risk profile.

8.11 A bank should ensure that the internal pricing and performance measurement mechanisms appropriately take into account operational risk. Where operational risk is not considered, risk-taking incentives might not be appropriately aligned with the risk appetite and tolerance.

8.12 A bank should systematically track and record the frequency, severity and other information on individual loss events. Such data could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate or control that risk.

(c) Operational-Risk Monitoring, Control and Mitigation

8.13 The board and senior management should implement a process to regularly monitor operational-risk profiles and material exposures to losses.

8.14 A bank should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies. Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations; safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations. A sound internal control programme should, at the minimum, comprise the following components, which are integral to the risk management process:

- (i) Management oversight of the risk control practices;
- (ii) Risk recognition and assessments;
- (iii) Control activities and segregation of duties;
- (iv) Information and communication; and
- (v) Monitoring activities and correction of deficiencies.

8.15 Control processes and procedures should include a system for ensuring compliance with policies. Examples of principal elements of a policy compliance assessment include:

- (i) top-level reviews of progress towards stated objectives;
 - (ii) verifying compliance with management controls;
 - (iii) review of the treatment and resolution of instances of non-compliance;
 - (iv) evaluation of the required approvals and authorisations to ensure accountability to an appropriate level of management;
 - (v) tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy; and
 - (vi) ensuring the adequacy and effectiveness of controls.
- 8.16 The bank should institute segregation of duties. Assignments that establish conflicting duties for individuals or a team without dual controls or other risk - mitigation measures may enable concealment of losses, errors or other inappropriate actions. Therefore, areas of potential conflict of interest should be identified, minimised and be subject to careful independent monitoring and review.
- 8.17 A bank should also ensure that internal controls are adequate and effective for each function, process or products. Examples of these controls include:
- (i) clearly established authorities and/or processes for approval;
 - (ii) close monitoring of adherence to assigned risk thresholds or limits;
 - (iii) safeguards for access to, and use of, bank assets and records;
 - (iv) appropriate staffing level and training, to ensure competence in the discharge of the responsibilities;
 - (v) on-going processes to identify business lines or products where returns appear to be out of line with targets or expected outcomes;
 - (vi) regular verification and reconciliation of transactions and accounts; and
 - (vii) Staff leave policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks at least once a year.
- 8.18 Effective use and sound implementation of technology can contribute to an effective control environment. However, automated processes introduce risks that must be addressed through sound technology governance and infrastructure risk management programmes.

- 8.19 The use of technological products, activities, processes and delivery channels exposes a bank to strategic, operational and reputational risks, and the possibility of material financial loss. Therefore, a bank should have an integrated approach to identifying, measuring, monitoring, controlling and managing technology risks. The integrated approach should encompass the following key aspects:
- (i) governance and oversight controls that ensure that technology and outsourcing arrangements are aligned with and supportive of a bank's business objectives;
 - (ii) policies and procedures that facilitate identification and assessment of risk;
 - (iii) establishment of a risk appetite and tolerance statement, as well as performance expectations, to assist in controlling and managing risk;
 - (iv) implementation of an effective control environment and the use of risk-transfer strategies that mitigate risk; and
 - (v) monitoring processes that test for compliance with policy thresholds or limits.
- 8.20 Management should ensure that a bank has a sound technology infrastructure, which meets current and long-term business requirements by providing sufficient capacity for normal activity levels, as well as peaks during periods of market stress; ensuring data and system integrity, security and availability; and supporting integrated and comprehensive risk management.
- 8.21 Mergers and acquisitions (M/As) resulting in fragmented and disconnected-technology infrastructure, cost-cutting measures or inadequate investment, can undermine a bank's ability to aggregate and analyse information across risk dimensions or the consolidated enterprise, particularly during periods of high growth. Management should make appropriate capital investment or otherwise provide for a robust infrastructure, particularly before M/As are consummated, high-growth strategies are initiated, or new products are introduced.
- 8.22 Outsourcing is another business strategy that can expose a bank to strategic, operational and reputational risks and the possibility of material financial loss. Therefore, the board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk-management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass, among others, the following:
- (i) procedures for determining whether and how activities can be outsourced;
 - (ii) processes for conducting due diligence in the selection of potential service providers;

- (iii) sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;
 - (iv) programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;
 - (v) establishment of an effective control environment within a bank and the service provider;
 - (vi) development of viable contingency plans; and
 - (vii) execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.
- 8.23 In circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, Management can complement controls by seeking to transfer the risk to another party, such as through third party insurance. The board should determine the maximum loss exposure a bank is willing to take and has the financial capacity to absorb, and should perform an annual review of a bank's risk and insurance management programme. While the specific insurance or risk-transfer needs of a bank should be determined on an individual basis, many jurisdictions have regulatory requirements that must be taken into consideration.
- 8.24 Consistent with the requirement of Section 14(2)(b) of the Banking Act (CAP. 46:04), a bank must either buy a "banker's bond" policy to cover operational risk relating to professional negligence or create a reserve out of its income, specifically for professional negligence and related risks.
- 8.25 Risk transfer is an imperfect substitute for sound controls and risk-management programmes. Therefore, a bank should view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational-risk control. Having mechanisms in place to quickly identify, recognise and rectify distinct operational risk errors can greatly reduce exposures. Careful consideration should be given to the extent to which risk-mitigation tools, such as insurance, truly reduce risk, transfer the risk to another business sector or area, or create a new risk (e.g., counterparty risk).
- (d) Operational-Risk Reporting
- 8.26 Operational-risk reports may contain internal financial, operational and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making. Operational-risk reports should include:

- (i) breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits;
 - (ii) details of recent significant internal operational risk events and losses; and
 - (iii) relevant external events and any potential impact on the bank and operational risk capital.
- 8.27 Data capture and risk-reporting processes should be analysed periodically with a view to continuously enhancing risk management performance, as well as advancing risk-management policies, procedures and practices.
- 8.28 Appropriate reporting mechanisms should be in place at the board, senior management and business line levels that support proactive management of operational risk.
- 8.29 A bank should continuously improve the quality of operational-risk reporting by ensuring that its reports are comprehensive, accurate, consistent and actionable across business lines and products. Risk reports should be manageable in scope and volume because effective decision-making can be impeded by deficient or excessive amounts of data.
- 8.30 Reporting should be timely and a bank should be able to produce reports in both normal and stressed-market conditions. The frequency of reporting should reflect the risks involved and the pace and nature of changes in the operating environment.
- 8.31 Reports generated by (and/or for) supervisory authorities should also be reported internally to senior management and the board, where appropriate.
- (e) Business Resiliency and Continuity
- 8.32 A bank should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.
- 8.33 A bank can be exposed to disruptive events, some of which may be severe and result in inability to fulfil some or all of its business obligations. To provide resiliency against this risk, a bank should establish business continuity plans commensurate with the nature, size and complexity of its operations. Such plans should take into account different types of likely or plausible scenarios to which the bank may be vulnerable.
- 8.34 Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programmes, communication and crisis-management programmes. A bank should identify critical business operations, key internal and external dependencies and appropriate resilience levels. Plausible disruptive scenarios should be assessed for their financial, operational and reputational impact, and the resulting risk assessment should be the foundation for

recovery priorities and objectives. Continuity plans should establish contingency strategies, recovery and resumption procedures and communication plans for informing management, employees, regulatory authorities, customers, suppliers, and, where appropriate, civil authorities.

- 8.35 A bank should periodically review its continuity plans to ensure that contingency strategies remain consistent with current operations, risks, threats, resiliency requirements and recovery priorities. Training and awareness programmes should be implemented to ensure that staff can effectively execute contingency plans. Plans should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in disaster recovery and business continuity testing with key service providers. Results of formal testing activity should be reported to senior management and the board.
- 8.36 The bank is required to conduct regular stress-test scenarios. The stress tests should be rigorous, forward looking and capable of identifying possible events or changes in market conditions that could adversely impact the bank's business operations and assess the bank's ability to withstand such changes. Such stress testing should alert bank management to any adverse unexpected outcomes related to operational risk and provide an indication of how much capital might be needed to absorb losses should large shocks occur.
- 8.37 A bank must hold adequate capital to absorb operational-risk losses. Computation of such capital must be consistent with the banks determination of the regulatory capital charge for operational risk under the Revised International Convergence of Capital Measurement and Capital Standards for Botswana (Basel II).
Money Laundering and Financial Crime Risks
- 8.38 All banks must ensure full compliance with the Financial Action Task Force (FATF) Recommendations and all applicable legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of weapons of mass destruction, and other related threats to the integrity of the Botswana financial system.
- 8.39 Consistent with the requirements of the FATF Recommendations and the Financial Intelligence (FIA) Act (CAP 08:07), all reporting banks must undertake preventative measures to prevent their banks from being used as conduits for money laundering and terrorism-financing activities. Such preventive measures, should, at a minimum, include customer due diligence, record keeping and additional measures for specific customers and activities, such as politically exposed persons (PEPs), correspondent banking, money or value transfer services, wire transfers, etc.
- 8.40 A bank should identify applicable risks and develop policies for the effective management of AML/CFT risks.

- 8.41 Every bank should adopt a risk-based approach (RBA) in the management of AML/CFT risks in order to target their resources more effectively and apply preventive measures that are commensurate with the nature of risks. In implementing a RBA, banks should have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. Where there are elevated risks, banks should take enhanced measures to manage and mitigate those risks.
- 8.42 All banks must ensure full compliance with the sanction laws and/or requirements related to terrorist financing as issued by the FIA and/or the United Nations Security Council (UNSC). In addition to the UNSC sanction lists, a bank may comply with sanction lists issued by jurisdictions in which the bank has correspondent banking relationships, to minimise the risk of being de-risked.

9. COUNTRY AND TRANSFER RISK¹⁰

- 9.1 When a bank engages in granting credit internationally, it assumes in addition to standard credit risk, risk associated with conditions in the home country of a foreign borrower or counterparty (country and transfer risk). Country or sovereign risk encompasses the entire spectrum of risks arising from the economic, political and social environments of a foreign country that may have potential consequences for foreigners' debt and equity investments in that country. Transfer risk focuses more specifically on a borrower's capacity to obtain the foreign exchange necessary to service its cross-border debt and other contractual obligations. In all instances of international transactions, a bank needs to understand the integration of financial markets and the potential for spill-over effects from one country to another or contagion effects for an entire region.
- 9.2 A bank that engages in granting credit outside Botswana should, therefore, have adequate policies and procedures, approved by the bank's board of directors, that identify, measure, evaluate, monitor, report and control country and transfer risk in their international lending and investment activities. The processes should be consistent with the risk profile, systemic importance and risk appetite of the bank. It should take into account market and macroeconomic conditions and provide a comprehensive bank-wide view of country and transfer-risk exposure.
- 9.3 Country exposures (including intra-group exposures) should be identified, monitored and managed on a regional and individual country basis, and the bank should ensure adherence to established limits. Banks are required to monitor and evaluate developments in country and transfer risk and apply appropriate counter measures. The monitoring of country and transfer risk factors should incorporate:
- (i) the potential default of foreign private sector counterparties arising from country-specific economic factors; and
 - (ii) the enforceability of loan agreements and timing and ability to realise collateral under national legal frameworks.
- 9.4 A bank should have information systems, risk-management systems and internal control systems that accurately aggregate, monitor and report country exposures (including intra-group exposures) on a timely basis, and ensure adherence to established country-exposure limits.
- 9.5 A bank is required to include appropriate scenarios into its stress-testing programme to reflect country and transfer-risk analysis for risk-management purposes. Such stress tests should be performed to identify potential vulnerability to exceptional but plausible events on a bank's exposure to country and transfer risks and assess the bank's ability to withstand such changes. The results of stress testing should alert

¹⁰ Basel Committee on Banking Supervision, Core Principles for Effective Banking Supervision (2012) (Principle 21); Research Paper on "Management of Banks' International Lending (Country Risk Analysis and Country Exposure Measurement and Control)" (March 1982).

bank management to any adverse unexpected outcomes and provide an indication of how much capital might be needed to absorb losses should large shocks occur.

- 9.6 A bank should regularly submit sufficient information, on a timely basis, on country and transfer risk for review by the Bank.

10. COMPLIANCE RISK MANAGEMENT¹¹

10.1 Compliance risk is the risk of legal or regulatory sanctions, material financial loss, or loss of reputation, which a bank may suffer, as a result of its failure to comply with laws, regulations, prudential guidelines, supervisory actions and directives, rules, internal policies and procedural guidelines, and codes of conduct applicable to its banking activities.

10.2 Compliance risk arises from failure by a bank to conduct its business in accordance with the business and contractual legal principles applicable in each of the jurisdictions where the bank conducts its business; this could result in unenforceable contracts, litigation, or other adverse consequences. Compliance risk can lead to the revocation of a licence, fines and penalties, payment of damages, deteriorating position in the market, reduced expansion potential, lack of contract enforceability, as well as reputational risk.

(a) Compliance-Risk Identification

10.3 Common sources of compliance risk are:

- (i) violations or non-compliance with laws and regulations and prescribed standards;
- (ii) lack of or inadequate compliance with contractual obligations and other legal documentation;
- (iii) inadequate identification of rights and responsibilities between the bank and its customers;
- (iv) complaints by customers and other counterparties;
- (v) harming the interest of third parties; and
- (vi) litigation procedures, potential exposure and nature of pending or threatened litigation.

(b) Compliance-Risk Measurement

10.4 Compliance risk is not easy to measure. A bank needs to define the appropriate approach to assessing each identified source of risk.

There are various tools used for identifying and assessing compliance risk, such as:

- (i) **self-assessment** - this is where a bank conducts a qualitative assessment of its operations against a list of potential risk vulnerabilities;

¹¹ Basel Committee on Banking Supervision, *Compliance and the Compliance Function in Banks* (2005); and Basel Committee on Banking Supervision, *Corporate Governance Principles for Banks* (2014)

- (ii) **risk indicators** - these are statistics or matrices that can provide insight into a bank's risk position; and
 - (iii) **risk mapping** - in this process, various departments or units are outlined by risk types and levels in order to enable effective development of procedures and mitigation measures for the risks identified.
- 10.5 Compliance risk can also be measured by regular legal reviews of the bank's different products and services, and their relevant documentation in order to ensure that all contracts comply with laws and regulations. This review may take place on each transaction individually or may cover the legal adequacy of standardised documentation and procedures.
- (c) Compliance-Risk Monitoring, Control and Mitigation
- 10.6 Compliance-risk mitigation factors would include putting in place appropriate compliance-risk management processes and an effective compliance function in the bank.
- 10.7 In collaboration with the compliance function, senior management should:
- (i) implement the compliance-risk management system approved by the board;
 - (ii) implement an effective organisational structure for compliance-risk management, and be in regular contact with employees that are directly responsible for conducting compliance-risk management (bank's compliance staff and lawyers);
 - (iii) ensure that all employees are working in order to protect the bank's reputation;
 - (iv) ensure that sufficient human and technical resources are devoted for compliance-risk management; and
 - (v) ensure that there is on-going compliance-risk management training.
- 10.8 The size of the bank and complexity of its business activities dictate the scope of the compliance function and its staffing requirements (number and competencies). Compliance responsibilities may be discharged by staff in different departments or all compliance responsibilities may be conducted by the compliance unit/department.
- 10.9 The compliance function should be independent, with sufficient resources and clearly specified activities. The compliance staff, especially the head of compliance, should not be in a position where conflict of interest between his/her compliance responsibilities may arise.

- 10.10 The head of the compliance function should be a member of senior management and should not have direct business line responsibilities.
- 10.11 Compliance risk should be included in the risk-assessment methodology of the bank. An audit programme that covers the adequacy and effectiveness of a bank's compliance function should be established, including testing of controls commensurate with the perceived level of risk. This principle implies that the compliance function and the internal audit function should be separate to ensure that the activities of the compliance function are subject to independent review. The audit function should, however keep the head of compliance informed of any audit findings related to compliance risk management.

Policies and Procedures

- 10.12 Compliance-risk management policies and procedures should be clearly defined and consistent with the nature and complexity of a bank's activities. The compliance policy should address the following issues:
- (i) define responsibilities and ultimately ensure that the board and senior management are fully acquainted with 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) express its right to obtain access to information necessary to carry out its responsibilities and the corresponding duty of bank staff to cooperate in supplying this information;
 - (v) its right to conduct investigation of possible breaches of the compliance policy;
 - (vi) its right to freely express and disclose its findings to senior management; and
 - (vii) its right of direct access to the board of directors or a sub-committee of the board.

Internal Controls

- 10.13 The audit with respect to compliance risk should be incorporated into the annual plan of the bank's internal audit function.
- 10.14 The internal audit function should, within its scope of operations, cover the following aspects of compliance-risk management:

- (i) verify that compliance-risk management policies and procedures have been implemented effectively across the bank;
 - (ii) assess the effectiveness of controls for mitigating fraud and risks to reputation;
 - (iii) determine that senior management takes appropriate corrective actions when compliance failures are identified;
 - (iv) ensure that the scope and frequency of the audit plan/programme is appropriate to the compliance-risk exposures;
 - (v) determine the level of senior management compliance with the Bank's directives; and
 - (vi) analyse the timeliness and accuracy of compliance risk reports to senior management and the board of directors.
- (d) Compliance-Risk Reporting
- 10.15 A bank is responsible for monitoring its compliance-risk profiles on an ongoing basis by reviewing defined compliance-risk indicators in order to provide management with early warning. The results of these monitoring activities should be included in the bank's periodic reports.
- 10.16 A robust MIS should enable the bank to generate data and reports for use by the board and management.
- 10.17 A bank should establish a database which should contain, among others, the type of legal documents (contracts, memorandum of understanding, etc.), period of document validation, and responsible department/unit for document enforcement.

11. REPUTATIONAL RISK MANAGEMENT¹²

- 11.1 Reputational risk is the potential that negative publicity regarding a bank's business practices, whether true or not, will cause a decline in market share, revenue, credibility and lead to costly litigation. Reputational risk may result from a bank's failure to effectively manage any or all of the other risk types. This risk is real, but not easy to measure.
- 11.2 Reputational risk can emerge at all business levels and has the following key components:
- (i) **corporate** reputation risk: this relates to a bank's performance, strategy, execution and delivery of its services; and
 - (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, resulting in loss of business and/or disproportionate decrease in the value of the bank.
- (a) Identification of Reputational Risk
- 11.3 A bank should conduct a risk-diagnostic review to identify potential reputational risk areas. The board should require 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 review critical control points within the bank.
- 11.4 This process should assist the bank to uncover the key risk factors with high likelihood to give rise to reputational risk. A bank should ensure that the analysis methodology used is highly sensitive to the bank's particular needs and requirements as well as risk issues emanating from the industry. The review process should be objective.
- 11.5 Reputational risk could be inherent in the type of business embarked on, or emanate from environmental and/or governance factors. Therefore, the risk-management methodologies employed must be broad enough to reach all risks in each category.
- (i) Inherent Reputational Risk
- 11.6 This risk can arise from the intrinsic feature of products and/or services or mode of their delivery, which negatively impacts on market and customer satisfaction. Therefore, inherent risks mainly derive from challenges in operational risk, quality assurance and customer satisfaction.

¹² Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking (2001).

(ii) Environmental Risk

- 11.7 This risk arises from the environment within which business is conducted (e.g., geographic, industrial, political and societal). Although these aspects are not related to the quality of the products or services, they can negatively impact market and customer brand acceptance.

(iii) Governance and Control Risk

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

(b) Measurement of Reputational Risk

- 11.9 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 bank. The reputational-risk template should conform directly to the risk definition and should include risk-tolerance levels, with special emphasis on potentially high-risk areas. Controls and metrics should address the categories of reputational risk from a qualitative perspective.

- 11.10 Further to the risk templates, both subjective and objective risk standards should be incorporated in the template. Particular attention should be given to risks whose consequences are capable of causing adverse events in other divisions of a bank (domino risks). A bank should also note that some risks interact with and affect one another (collide), hence actions taken or not taken in one area will have material consequences on the whole bank.

(c) Monitoring, Control and Mitigation of Reputational Risk

- 11.11 Risk monitoring/control should at the least encompass the following:

- (i) establishment of strong enterprise risk-management policies and procedures throughout the organisation, including an effective anti-fraud programme;
- (ii) reinforcement of a risk-management culture by creating awareness at all staff levels;
- (iii) instilling ethics throughout the organisation by enforcing a code of conduct for the board, management and staff;
- (iv) development of a comprehensive system of internal controls and practices, including those related to computer systems and transactional websites;

- (v) compliance with current laws and regulations and enforcing existing policies and procedures;
- (vi) implementation of independent testing and transactional testing on a regular basis;
- (vii) responding promptly and accurately to bank regulators, oversight professionals (such as internal and external auditors), and law enforcement officers, media; and
- (viii) establishment of a crisis-management team in the event there is a significant action that may trigger a negative impact on the organisation.

11.12 Reputational-risk management should be an ongoing activity. A bank should develop a reputational-risk database and identify key controls and tracking reports. As part of an ongoing management of the risk, the board should require staff-awareness training at all levels of the bank, with special training regarding potential high-risk areas. Finally, all aspects of reputational-risk management should be subject to an internal audit review.

(d) Reporting of Reputational Risk

11.13 Preserving a strong reputation revolves around effectively communicating and building solid relationships. Communication between a bank and its stakeholders can be a foundation for a high reputation. Timely and accurate financial reports, informative newsletters and excellent customer service are important tools for reinforcing a bank's credibility and entrenching the trust of its stakeholders.

11.14 Reputational risk is managed through strong corporate governance, the tone of which should be set from the top; a bank's board of directors and senior management should actively support reputational-risk awareness by demanding accurate and timely management information.

11.15 A bank should consider the following key elements for managing reputational risk:

- (i) maintaining timely and efficient communications among shareholders, customers, the board of directors and employees;
- (ii) positive information about a bank should also be communicated appropriately to the market place; and
- (iii) 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 office. A bank should also ensure that there is no general release of information to the public or press without approval from senior management.

- 11.16 Reputational-risk reports should be timely and accurate. Communication related to reputational risk, both in-house and with external parties, should be managed by a bank's public relations/communications office.

Issued this 15th day of May 2018



DIRECTOR
BANKING SUPERVISION DEPARTMENT