National Reserve Bank of Tonga

PRUDENTIAL BANKING STANDARD No. 9

GOVERNANCE AND RISK MANAGEMENT

Contents

Contents

Objectives and key requirements of this Prudential Standard

This Prudential Standard sets out minimum foundations for the governance and risk management of banks. It aims to ensure that banks are managed in a sound and prudent manner by a competent Board of Directors, which make reasonable and impartial business judgements in the best interests of the institution and with due consideration to the impact of its decisions on depositors.

Under this Prudential Standard a bank must have systems for identifying, measuring, evaluating, monitoring, reporting, managing and controlling or mitigating material risks that may affect its ability to meet its obligations to depositors and other stakeholders. These systems, together with the structures, policies, processes and people supporting them, comprise a bank's risk management framework.

The Board of a bank, or the Senior Overseas Officer (where a bank is operating as a branch of a foreign bank, as described later under paragraph 37 of this Prudential Standard), respectively, are ultimately responsible for ensuring there is a risk management framework that is appropriate to the size, business mix and complexity of the bank in Tonga. The bank's strategic objectives and business plan must also be consistent with the Board's Risk Appetite statement and its risk management framework.

Effective corporate governance is critical to the proper functioning of a bank. Governance weaknesses can result in the transmission of problems across the banking sector and the economy as a whole. The primary objective of corporate governance is to safeguard stakeholders' interest in conformity with public interest on a sustainable basis. Among stakeholders, particularly with respect to retail banks, shareholders' interest would be secondary to depositors' interest.

PART I

PRELIMINARY

I. Short title

Governance and Risk Management

II. Authorization

1. This Prudential Standard is issued by the National Reserve Bank of Tonga (Reserve Bank) in accordance with sections 19 (3), 20(3) and 99 of the Banking Act (2020) (the Act) in relation to prudential requirements and measures to be applied to banks.

III. Scope of Application

2. This Prudential Standard is applicable to all banks operating in Tonga including the Foreign Bank Subsidiaries (FBS) and Foreign Bank Branches (FBB). As part of its prudential oversight of FBSs and FBBs, the Reserve Bank may discuss with the Foreign Bank (FB) and home supervisor any governance or risk management issues associated with the foreign bank's Tongan operations. In the cases of Tongan domestic banks and FBSs, Reserve Bank may decide to apply the requirements at consolidated level i.e. at the banking group level covering the bank incorporated in Tonga and its non-bank subsidiaries, if considered necessary.

IV. Definitions

3. This Prudential Standard uses the following terms, which unless otherwise indicated, have the meanings specified below:

a) ***Affiliate*** **-** an entity defined as 'affiliate' under Section 2 of the Banking Act (2020) and having the meaning under the Act.

b) ***Bank –*** an entity defined as 'bank' under Section 2 of the Banking Act (2020) and having the meaning under the Act.

c) ***Capital Base*** – means Tier 1 Capital as defined in Prudential Standard number 6 Capital Adequacy Requirements.

d) ***Conflicts of Interest*** - arises as a result of the various activities and roles of the bank or between the interests of the bank or its customers and those of the bank's Board members or senior managers (e.g. where the bank enters into a business relationship with an entity in which one of the bank's Board members has a

financial interest). Conflicts of interest may also arise when a bank is part of a broader group. For example, where the bank is part of a group, reporting lines and information flows between the bank, its parent company and/or other subsidiaries can lead to the emergence of conflicts of interest**.**[1]

e) ***Duty of Care*** - the duty of Board members to decide and act on an informed and prudent basis with respect to the bank. Often interpreted as requiring Board members to approach the affairs of the bank in the same way that a "prudent person" would approach his or her own affairs.

f) ***Duty of Loyalty*** - the duty of Board members to act in good faith in the interest of the bank. The duty of loyalty should prevent individual Board members from acting in their own interest, or the interest of another individual or group, at the expense of the bank and shareholders.

g) ***Executive Director*** – a director who is a member of management of the bank.

h) ***Foreign Bank (FB)*** - means a body corporate that:

(i) is an overseas company within the meaning of section 2 the Companies Act 1995; and

(ii) is authorised to carry on banking business in a foreign country; and

(iii) has been granted a licence under Part II of the Banking Act (2020) to carry on banking business in Tonga.

i) ***Foreign Bank Subsidiary (FBS):*** A subsidiary of a Foreign Bank incorporated in Tonga as a bank.

j) ***Foreign Bank Branch (FBB):*** Branch of a Foreign Bank operating in Tonga in branch mode and excludes branches of Foreign Bank Subsidiaries.

k) ***Governance*** - is the way an organisation is managed, directed and held accountable for achieving its goals, including the goal of adequately managing risk. It refers to the formal structure(s), processes and practices used to support decision making and oversight across all operations of a bank, and the manner in which the bank's business and affairs is directed by both the Board and senior management. It also refers to a set of relationships between a company's management, its Board, its shareholders and other stakeholders which provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance. It helps define the way authority and responsibility are allocated and how corporate decisions are made. This typically consists of board committees and management committees, delegations, management structures and related reporting, as well as various controls (such as policy constraints) to prevent bad practices from occurring, including to control conflicts of interest from influencing decision making. It is also reflected in the way relationships are established, facilitated and controlled internally between the Board, management and other staff and externally with depositors, shareholders

[1] Definitions taken from BCBS publication, Corporate governance principles for banks (July 2015), Bank for International Settlements (BIS)

and other stakeholders. Corporate governance affects, amongst other things, how the bank:

i. Sets corporate objectives;

ii. Determines its risk tolerance/appetite;

iii. Runs the daily operations of the business;

iv. Protects the interests of depositors;

v. Is accountable to the shareholders;

vi. Takes into account the interests of other stakeholders; and

vii. Operates in a safe and sound manner, with integrity and in compliance with applicable laws and regulations.

l) ***Governance framework*** - includes a bank's Board's own rules, committee structure, nomination, hiring, and compensation processes, organizational structure, the strategy or risk appetite it sets, and the control structure it establishes over risk taking activities. Governance extends broadly to all elements of risk management discussed in this Prudential Banking Standard, and it applies especially to the Board 's ultimate responsibility for supervising senior managers, reviewing policies, approving specific transactions, monitoring high-level reports of the bank's activities and results, overseeing internal audit, and ensuring that the bank complies with laws and regulations.

m) ***Independent Director*** - a non-executive director is one who is free from any business or other association – including those arising out of a substantial shareholding, involvement in past management or as a supplier, customer or adviser - that could materially interfere with the exercise of their independent judgement (apart from directorship fees and any shareholdings in other banks, their subsidiaries and affiliates). Independent directors should have proportionate representation on board committees.

n) ***Internal Audit*** - is one or more employees within the bank who are responsible for providing assurance to the Board and Board Audit Committee of the quality and effectiveness of a bank's internal control, risk management, and governance systems and processes, independent of the banks business and operational units, thereby helping the Board and Board Audit Committee protect the bank and its reputation.

o) Locally Incorporated Banks: Tongan domestic banks and the banks that are Foreign Bank Subsidiaries.

p) ***Manager –*** has the meaning in the Act.

q) ***Material Risks*** – are those that could have a material impact, both financial and nonfinancial, on the bank or on the interests of depositors. Material risks at a minimum, must address:

I. credit risk;

II. market and investment risk (including funding);

III. liquidity risk;

IV. operational risk (including IT risk);

V. strategic risk; and

VI. other risks that, singly or in combination with different risks, may have a material impact on the bank (e.g. legal risk or regulatory risk in certain circumstances, country risk, a failure of governance, climate change, pandemic risk, reputational risk, risks from anti money laundering and terrorist financing etc.).

Further information on these risks is contained at Annexure 1.

r) ***Non-executive Director*** - a director who is not a member of management of the bank. Non-executive directors may include Board members or senior managers of the parent company of a locally incorporated bank or of the parent company's subsidiaries, but not executives of the bank incorporated in Tonga or its subsidiaries.

s) ***Risk management*** - the processes, systems and culture established to ensure that all material risks and associated risk concentrations are identified, measured, limited, controlled, mitigated and reported on a timely and comprehensive basis. It includes the identification, measurement, evaluation, monitoring, reporting, and control or mitigation of all material risks on a timely basis and the assessment of the adequacy of capital and liquidity relative to the bank's risk profile, market conditions, and economic environment. Risk management extends to the development and review of contingency arrangements (including robust and credible contingency and recovery plans where warranted) to consider the specific circumstances of the bank. Risk management processes must

t) ***Risk Management Framework*** – the entirety of the systems, structures, policies, processes and people within a bank that identify, measure, monitor and control material risk.

u) ***Risk Appetite*** – a statement of the aggregate amount and type(s) of risk a financial institution is willing to accept in pursuit of its strategy and business objectives. It is decided in advance and within its risk capacity. A risk appetite is expressed in the form of both high-level qualitative statements and, where appropriate, quantitative measures. It must contain limits or risk tolerances for all material risks.

v) ***Risk Culture*** – are the values and behaviours within a financial institution that shape its risk decisions. It includes norms, attitudes and behaviours related to risk awareness, risk-taking and risk management which shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume.

w) ***Risk Governance*** – is governance, as defined above, in respect to the managing, directing and accountability for risk. Risk governance includes the structures, processes and practices used to support decision making and oversight with respect to risk across all operations of a bank. There is an appropriate balance between

achieving business objectives and managing risk, which will vary from bank to bank. Generally, the dictates of markets mean that as returns rise, so does the risk (i.e. greater returns are required by investors as risk increases). Good risk governance should ensure that risk is well managed within risk boundaries established by a bank and that the business objectives and returns sought by the bank are planned and managed consistently within the risk boundaries set. It is critical to an bank operating in a safe and sound manner that the Board of Directors (Board) a bank take a leading role in risk governance and commit their time and focus, in a balanced manner, towards risk governance, not just business growth and profitability.

x) ***Risk Profile*** - is a point-in-time assessment of a bank's gross risk exposures (i.e. before the application of any mitigants) or, as appropriate, net risk exposures (i.e. after taking into account mitigants) aggregated within and across each relevant risk category based on current or forward-looking assumptions.

y) ***Risk Tolerances*** - the maximum level of risk that the institution is willing to take regarding each type of risk, sometimes expressed as a risk limit[2.] These limits are the basis of the risk appetite statement which is a document the board must "own". Risk tolerance limits are both qualitative and quantitative and are expected to be specific, measurable, frequency-based and reportable.

2 Risk tolerances should be set which are both quantitative and qualitative. However, where possible, at least some of the measures used to articulate the risk tolerances for each key risk indicator should be quantitative measures. This allows the risk tolerances to be referenced directly into policy for each risk type and allow each risk to be more easily measured, evaluated and reported against the appetite/tolerance.

PART II

STATEMENT OF POLICY

I. Purpose

1. The purpose of this Prudential Standard is to protect the safety and soundness of banks by establishing sound governance and risk management within each bank.

II. Summary of Important Requirements

2. This Prudential Standard requires banks to identify, measure, monitor, control and report risks. In order for a bank within its risk management framework. To meet these requirements, the framework must have the following key elements:

- have a Board approved policy with respect to both governance and risk management which requires implementation of prudent measures by the bank with respect to governance and risk management;
- sets minimum responsibilities for the Board and management;
- requires establishment of Board Risk and Audit Committees;
- establishes a requirement for a Senior Officer outside Tonga for foreign bank branches;
- requirement for a remuneration policy;
- minimum requirements for strategy and planning;
- requirements for the risk management framework including having adequate systems and controls to identify, measure, monitor and report material risks in a timely manner as required by the Reserve Bank or this Prudential Standard;
- requirements for the risk appetite statement;
- requirements for the risk management strategy;
- requirements for the risk function within an bank;
- requirements for the risk culture;
- requirements for the compliance function; and
- requirements for the internal audit.

3. This Prudential Standard is intended to safeguard depositors, creditors and other stakeholders through sound governance and effective risk management.

III. Responsibility

4. The Board is ultimately responsible for the oversight of a bank's governance and risk management and adherence to the requirements of this Prudential Standard.

5. It is the responsibility of the Board of each bank to establish an effective risk management system for controlling and monitoring all material risks. In the case of FBSs, this responsibility shall primarily lie with the local board. In the case of FBBs, both the parent bank's board and any local management of a FBB identified/established to oversee the Tongan operations shall be responsible for both the oversight of a bank's governance and risk management and adherence to the requirements of this Prudential Standard.

PART III

IMPLEMENTATION AND SPECIFIC REQUIREMENTS

I. Board of Directors and Senior Management

(i) Overall responsibility

6. The Board is ultimately responsible for the sound and prudent governance and risk management of the institution and its business. The Board is also ultimately responsible for the institution's risk management framework and is responsible for the oversight of the operation of the risk management framework by management.

7. It is the responsibility of the Board and management to assess the risks in the activities, undertakings, business(es), products and services and assets and liabilities that the bank undertakes or acquires and continually monitor and control those risks.

8. The Board must ensure that an adequate and effective system of internal risk controls is established and maintained. The responsibilities of the Board, include but are not limited to:

a. Ensuring that the bank has established and implemented a Corporate Governance Policy, approved by the Board in the case of a locally incorporated institution or Senior Officer outside Tonga[3] in the case of a branch operation;

b. Ensuring that the bank has risk policies covering all material risk areas and has policies which control risks in all aspects of its operations;

c. Establishing risk limits for each material risk area within a risk appetite statement and adjusting and evolving these as appropriate for changes in the internal and external environment. The Board must review and monitor material risk areas particularly credit risk, liquidity and funding. The Board must ensure it receives regular and timely information as needed by it to monitor compliance with its risk appetite statement and identify risks that are trending towards its established risk limits so that corrective action can be implemented; and

d. Being aware of and understand the major risks inherent in the bank and in its operating environment.

9. It is the responsibility of a bank's Board and senior management to ensure that the bank meets prudential and statutory requirements and has management practices to limit risks to prudent levels. The risk management practices must be detailed in management systems

3 Refer paragraph 33 of this Prudential Banking Standard.

descriptions which should be regularly reviewed and updated (at least annually) to take account of changing circumstances.

10. The Board and senior management are also responsible and accountable for establishing and promoting codes of conduct and high ethical standards and ensuring that directors and managers are fit and proper as described in Prudential Standard Number 8: Fit and Proper Requirements.

11. The Board must establish a Code of Conduct which should articulate acceptable behaviour for both directors and staff, including avoiding and managing conflicts of interest, which aligns with the Board 's expectations for compliance with statutory and policy obligations as well as the risk appetite and risk management frameworks.

12. In the case of FBBs, the Reserve Bank will rely on the home regulator's governance framework in relation to the Board's responsibilities for that bank and oversight of the Board's compliance with it, unless the Reserve Bank becomes aware of circumstances which require it to apply the standards set out in this Prudential Standard to the FBB's operations. In this case, this Prudential Standard will only apply in relation to the bank's Tongan business.

13. The Board and senior management must establish strategic objectives that will direct the ongoing activities of the bank, taking into account the interests of all stakeholders, but particularly considering the obligation of the bank to repay depositors as and when deposits are due. These strategic objectives must be incorporated within a strategic plan and the business plan.

14. The Board must have a formal charter that sets out the purpose, roles and responsibilities of the Board. The charter should provide for the composition of the Board, including the range of skills and experience necessary for Board members. This is to ensure that each Director has appropriate skills and experience to make effective contributions to Board deliberations, and to understand the risks, and legal obligations of the bank. The charter should also include periodic review of board composition and succession planning for the Board. The Board must also ensure there are suitable charters for each Board committee.

15. Other matters which the Board also has ultimate responsibility for, but is not limited to, are:

a. Ensuring that capital is adequate to incorporate the nature and level of all material risks that it permits in its risk appetite statement, so as to assure its resilience. It is essential that the Board plans and hold loss-absorbing capital commensurate with the current and planned risk-taking activities. The capital adequacy requirements set by a Board must be prudent and appropriate to the bank's business[4] and reflect the risks undertaken by, and presented by, a bank in the context of the markets and

4 It is the Board's responsibility to understand the business the bank operates and the inherent risks that result from the activities the Board allows the bank to undertake. At a minimum, capital must be adequate to allow the bank to survive a downturn or significant risk event by providing a buffer against losses which will bridge it across a downturn or series of events which extend over a period of time, potentially spanning more than a year or two. While the Reserve Bank sets minimum capital requirements in Prudential Standard No. 6: Capital Adequacy, these are bare minimums, which the Reserve Bank will view very seriously if breached. Since each bank's business is different with a different risk profile it is expected that the Board will set capital requirements suitable for the bank and must not abrogate its own responsibility to all stakeholders to ensure its capital is adequate, by just assuming it will operate at a margin above the minimum set by the Reserve Bank.

macroeconomic conditions in which it operates (including all reasonable and foreseeable circumstances)[5].

b. Set the bank's strategy and objectives and ensure adequate planning is undertaken;

c. Establishing, overseeing, and maintaining a sound corporate governance framework that is appropriate for the bank's risk profile, strategy, and operating environment. It determines a bank's business strategy and risk appetite, including the risk tolerances;

d. Align corporate culture and behavior with the expectation that the bank will operate in a safe and sound manner, with integrity and in compliance with applicable laws and regulations;

e. Reviewing and approving the bank's organisational structure, staffing levels, remuneration arrangements, training and working conditions;

f. Overseeing that all procedures, processes, and policies are clearly communicated through all relevant levels of the bank;

g. It has the ultimate responsibility for the safety and soundness of the bank, understanding the regulatory environment, and ensuring that the bank maintains a close relationship with the Reserve Bank;

h. Ensuring that the bank has the necessary back-ups (e.g. contingency plans) and cross-training) to ensure the bank continues operations unhampered;

i. Where the Board decides to outsource a material business activity, that it follows appropriate procedures;

j. Undertaking the necessary due diligence in appointing their senior managers. The bank must have adequate policies and practices for the selection, approval, renewal, and succession of senior managers;

k. Providing oversight of senior management as part of the bank's checks and balances by monitoring management's actions and setting performance standards;

l. Ensuring the bank's compliance with the applicable laws, regulations and the Reserve Bank's Prudential Banking Standards and other guidelines;

m. Ensuring the bank's internal policies and contractual arrangements do not explicitly or implicitly restrict or discourage auditors and other parties from communicating with the Reserve Bank; and

n. Ensuring that the bank has adequate accounting, management information system (and that there are adequate contingency plans for IT systems in the event of disruption) consistent with the size and scope of its operations; and

o. Protect the interests of depositors, meet shareholder obligations, and take into account the interests of other recognised stakeholders.

16. The Board of a Locally-Incorporated Bank (Tongan domestic banks and FBSs) should, at a minimum, establish the following committees and the whole Board should have full and timely access to all reports (and deliberations) of its committees:

a. Audit Committee; and

5 Including those resulting from severe (but plausible) changes in the environment and from multiple risks escalating and impacting on the bank at the one time.

b. Risk Committee.

In addition, for larger banks, the Board may consider establishing a Remuneration Committee. In the case of FBBs, copies of all reports and deliberations of these committees and the ALCO mentioned below, should be provided to the bank's Senior Overseas Officer and head/regional office for review.

17. The Board must ensure that across its members, it contains the necessary skills and experience to function effectively as the Board of a bank. This does not preclude the Board from supplementing its skills and knowledge through the use of external consultants and experts.

18. The Board, in fulfilling its functions, may delegate authority to management with respect to certain matters. This delegation of authority must be clearly documented. The Board must have mechanisms in place for monitoring the exercise of delegated authority. The Board is not abrogated of its responsibility for functions delegated to management.

19. The Board must ensure that senior management of the bank, collectively, have the full range of skills needed for the effective and prudent operation of the bank. This includes the requirement for management to have the necessary skills, knowledge and experience to understand the risks of the bank, including its legal and prudential obligations, and to ensure that the bank is managed in a way that takes into account these risks. The Board should also ensure there are contingency plans and cross-training for key personnel.

20. The members of the board must exercise a "duty of care" and "duty of loyalty" to the bank.

21. The Board and management must develop and implement an appropriate succession planning framework for key persons, positions and skills and experience within the bank.

22. Senior management of a bank is responsible for ensuring the bank's risk management framework operates effectively, and the risk profile of the institution is at all times in line with the Board set risk appetite.

23. The senior management must ensure there is an effective Asset and Liability Committee (ALCO) which comprises suitably qualified and experienced senior management representatives from across all of the business lines. This committee must include the head of risk for the bank. The ALCO must meet at least weekly or more often when necessary. ALCO is responsible for coordinating the bank's fund raising and lending strategies to meet profitability objectives as market conditions change. The ALCO also has responsibility for ensuring that the bank implements and maintains a liquidity management policy that is appropriate for its operations and ensuring that it has sufficient liquidity to meet its obligations as they fall due. The Board will oversee this senior management responsibility and may require one or more board member(s) to be a member of ALCO (but this is not compulsory).

24. Senior management of the bank with responsibilities relating to the business in Tonga, must be ordinarily residing in Tonga (except for the Senior Overseas Officer – see paragraph 37.

25. The bank must provide the external auditor of the bank with the opportunity to raise matters directly with the Board.

26. The Board and management must promptly notify the Reserve Bank of any concerns that they hold about the safety and soundness of the bank. The corporate constitution and Board policies of the bank should not prevent directors or management from notifying the Reserve Bank at any time about concerns which they hold (either collectively or individually).

27. Where a bank is part of a corporate group, whether that be a subsidiary or branch operation, and the bank utilises group policies or functions, the Board must ensure that these policies and functions give appropriate regard to the bank's business in Tonga and its specific requirements. Where a bank is operating in Tonga as a locally incorporated company and it has subsidiaries, the Board of the bank must ensure that the requirements in this Prudential Standard are applied appropriately throughout the group, including in relation to institutions that are not regulated by the Reserve Bank, so as to ensure risks resulting from intercompany transactions and exposures or risks incurred by its subsidiaries do not impact on the financial safety and soundness of the bank in Tonga. In such cases, the risk management framework must address the risks posed by the subsidiaries to the bank and its depositors.

(ii) Board composition for Locally Incorporated Banks

28. Notwithstanding the requirements of the Companies Act 1995[6], the board of a Locally Incorporated Bank must consist of not fewer than five (5), nor more than nine (9) directors. The size of the Board should be commensurate with the size, scope, nature and complexity of the banks operations to ensure that it operates in a sound and prudent manner. The Board of a Locally-Incorporated Bank should be composed of individuals with an appropriate range of skills and experience to understand its activities so that, as a whole, it is able to control and direct those activities effectively.

29. The Board must have a majority of independent directors and at least two independent non-executive directors who are resident in Tonga[7].

30. A major function of a bank's Board is to bring a perspective that is independent of management to the business in which it engages. To this end, the majority of directors should be non-executives of the bank or any of its subsidiaries or affiliates.

6 Section 149 of the Companies Act 1995 requires that a company shall have at least one director.

7 Foreign owned banks should consult with the Reserve Bank if they believe that they cannot meet this requirement.

31. For a bank that is a subsidiary of another Reserve Bank regulated institution or an overseas equivalent[8], the Board must have a majority of non-executive directors, but these nonexecutive directors need not all be independent[9].

32. The chairperson of the Board must be an independent non-executive director of the bank.

33. A majority of directors' present and eligible to vote at all Board meetings must be non-executive directors.

34. The Board must be available to meet with the Reserve Bank on request, collectively and individually, at the discretion of the Reserve Bank.

35. Where there are large shareholders in a locally incorporated bank, Board representation must avoid the creation of significant influence in terms of the Act and where this is avoided, be reasonably consistent with the locally incorporated bank's shareholding.

36. Boards of locally-incorporated banks should hold at least one regular meeting each calendar quarter. The boards of locally-incorporated 'de novo' banks[10] should hold at least one regular meeting each calendar month unless otherwise advised by the Reserve Bank. At each regular meeting the board should review and approve the minutes of the prior meeting, and review the overall business strategies, risk profile compared to the Boards' Risk Appetite Statement, operations, activities and financial condition of the bank. Each action of the board must be recorded in the minutes of the meeting. If necessary, directors may attend meetings by teleconference provided:

(i) a quorum of the required directors is present including directors attending by teleconference;

(ii) all directors can at all times hear the comments of others;

(iii) copies of all documents intended to be discussed during the meeting are made available at least five (5) calendar days prior to the meeting.

A face-to-face meeting of the Board should occur at least annually, unless Government health restrictions prohibit this.

(iii) Senior Officer Outside Tonga

37. Head Offices of FBBs must nominate a senior officer of the corporate bank entity head office with delegated authority from the Board to be responsible for overseeing the

8 An 'overseas equivalent' is one which is not licensed in Tonga but is authorized and subject to prudential regulation in a foreign country.

9 They can include Board members or senior management of the parent company or its subsidiaries, but not executives of the regulated institution (in Tonga) or its subsidiaries. The Board of these banks must have at least two independent directors, in addition to an independent chairperson.

10 A "de novo bank" for purposes of this Prudential Standard includes any locally-incorporated bank which has been in operation for five (5) years or less.

Tonga branch operation. This "Senior Overseas Officer" may be a senior executive or non-executive director of the corporate bank entity.

(iv) Group relationships

38. Boards of banks should ensure that subsidiaries and affiliates operate in a safe and sound manner and are adequately capitalised for the risks that they undertake.

39. Boards are expected to establish policies on related parties (i.e. subsidiaries, affiliates, directors, senior management, and their families) dealings, which include requirements that any such dealings be on commercial terms and conditions and be subject to prudent limits as well as statutory and prudential requirements.

40. Where a bank distributes the financial products of other group members:

- any staff of the bank involved in the distribution or provision must be appropriately qualified and trained to provide those products or services;
- There must be no confusion created in customers' minds about the respective roles of the bank and the product provider and no impression given that the product is guaranteed or otherwise supported by the bank, unless there is a formal legal agreement in place to this effect which has been approval by the Reserve Bank.
- The identity of the product provider must be prominently displayed in the relevant marketing material and product documentation; and
- The customer must make the purchase decision in his/her own right.

(v) Avoiding potential conflicts of interest

41. Directors of banks, including subsidiaries and branches of foreign incorporated banks should avoid situations that could give rise to a conflict of interest or to perceptions of a conflict of interest. To avoid this, the Board must adopt a formal conflict of interest policy, which includes:

- a requirement that no director should simultaneously serve as a Board member, or in an executive capacity with any other financial institution or a subsidiary or affiliate of a bank in Tonga;
- a requirement that conflicts of interest must be avoided, and that where the conflict cannot be avoided, then it must be appropriately managed;
- a board or committee member's duty to disclose any matter that may result, or has already resulted, in a conflict of interest;
- a board member's responsibility to withdraw from any discussion or decision making process on the matters in which a conflict exists or might be perceived to exist, including that director not receiving Board information on the matter;
- a requirement to maintain a record in the minutes of disclosures of activities that could create conflicts of interest or the appearance of conflicts of interest;

- each director to sign off, at least annually, a conflict of interest declaration;
- review or approval process for directors prior to engagement in activities that may be construed as creating a conflict of interest (such as serving on another Board or as a potential supplier of goods and services to the company) to ensure that any conflict of interest may be avoided or alternatively, managed properly;
- procedures for dealing with conflicts of interest where they exist,
- adequate procedures for transactions with related parties to be made on an arms-length basis; and
- the way in which the board will deal with any non-compliance with the policy.

(vi) Board performance assessment and Board renewal

42. The Board must have procedures for assessing, at least once every two years, its performance relative to its objectives. It must also have in place a procedure for assessing, at least once every two years, the performance of individual directors.

43. The performance assessment is a self-assessment of its effectiveness as well as that of its sub-committees. This may occasionally require assistance of independent advisors.

44. The Board must have in place a formal policy on Board renewal. This policy must provide details of how the Board intends to renew itself to ensure it remains open to new ideas and independent thinking, while retaining adequate expertise.

(vii) Board and senior Development Program

45. The Board of each bank must ensure that potential and new directors and the Chief Executive Officer (CEO) meet the fit and proper standards in Prudential Standard No. 8 and that all directors and the CEO maintain these requirements.[11] In addition, appointees should be provided with adequate initial and ongoing development program which must include, but is not limited to, a familiarisation programme on the bank's business and risk profile, risk management and risk governance practices and internal controls.

46. The Board is also required to undertake professional development program on a regular basis as part of meeting ongoing fit and proper requirements for directors.

(viii) Role of Management

47. Senior management is responsible for directing and overseeing the effective management of the bank's operations. Key responsibilities of senior management include, but are not limited to:

a. Ensuring the bank operates within the Board approved Risk Appetite statement and risk management framework, including implementation of the policies and

11 This provision shall also apply to the CEO of the FBB who is in-charge of Tongan operations.

procedures and ensuring the policies, procedures and limits are communicated to all employees affected;

b. Developing and implementing processes and systems that adequately identify, assess, monitor, measure and manage/mitigate risks in relation to all business activities and operations. This includes being forward looking so that changes in the internal and external environments are recognised early, reported to the Board and/or Board Risk Committee so that the risk management framework and/or Board Risk Appetite statement can be adjusted accordingly in a timely manner. This is a continuous process;

c. In support of the implementation of policies, managers should ensure that the bank's procedures address detailed operational requirements;

d. Developing and implementing Board approved business objectives, strategies, plans, organisational structure, controls and policies. Where senior management develop a subset of Board approved strategies and plans on implementation, it must ensure these sub-plans and strategies are consistent with the Board approved plans and strategies and are also consistent with the Board's Risk Appetite statement;

e. Developing suitable Board reporting, which in consultation with the Board as to their information reporting needs, results in a comprehensive Board reporting framework that will keep the Board regularly and adequately informed about the bank's business, relative to the nature, scale and complexity of the bank's business. The Board reporting must have an emphasis on risk reporting to the Board and Board Risk Committee and achievement of the strategic and business plans. Management should keep the board regularly and adequately informed of critical matters relating to the bank's functioning, including as a minimum:

    (i) the bank's performance and financial position generally, but in particular actual performance of the bank against business strategy targets and against the Board's risk appetite;

    (ii) any breaches of risk limits, delegated powers, Prudential Banking Standards issued by the Reserve Bank, applicable laws, and compliance rules;

    (iii) internal control failures;

    (iv) legal, regulatory and business continuity concerns; and

    (v) issues raised as a result of the bank's whistleblower procedures.

    In the case of foreign bank branches, the requirements set out here shall apply to the Senior Officer outside Tonga.

f. Ensuring the achievement of Board approved business objectives, strategies, plans;

g. Monitoring the progress in achieving strategies and reporting this regularly to the Board;

h. Ensuring the effectiveness of the organisational structure and controls and that staffing levels are adequate both in terms of quantity and quality of human resources available to the bank to carry out the business and strategic objectives and for maintenance of an effective risk management framework;

i. Promoting the safety and soundness of the bank, understanding the regulatory environment, and ensuring that the bank maintains a close and open relationship with the Reserve Bank;

j. Ensuring the bank's compliance with applicable laws, regulations, and the Reserve Bank's Prudential Standards;

k. Ensuring that the Board is kept well informed, including of correspondence with the Reserve Bank and breaches or potential breaches of the Reserve Bank's prudential requirements;

l. Ensuring that the bank's internal policies or contractual arrangements do not explicitly or implicitly restrict or discourage auditors or other parties from communicating with the Reserve Bank; and

m. Ensuring that employees have the appropriate level of training and that the bank has a training development framework.

(ix) Persons not to be constrained from providing information to the Reserve Bank

48. The Board and senior management of a bank must establish and maintain policies and procedures to ensure that no current or former officer, employee or contractor (including a professional service provider) of a bank is constrained or impeded, whether by confidentiality clauses or other means, from disclosing information to the Reserve Bank, that may be relevant to the prudential supervision of the bank.

49. The Board and senior management of a bank must establish and maintain policies and procedures to ensure that such persons are not to be constrained or impeded from providing information to auditors, and others, who have statutory responsibilities in relation to the bank.

50. Banks must ensure that their internal policy and contractual arrangements do not explicitly or implicitly restrict or discourage auditors or other parties from communicating with the Reserve Bank.

51. A Board member must notify the Reserve Bank if they become aware of reliable information regarding another Board member's or senior manager's professional misconduct, criminal conviction, bankruptcy, fraudulent activity, or other action which would disqualify that individual from service as a director or senior manager.

II. Board Committees

(i) Board Risk Committee

52. The Board of a bank (excluding FBBs) must have a Board Risk Committee, which assists the Board by providing an objective non-executive oversight of the implementation and operation of the bank's risk management framework.

53. The Board Risk Committee must be provided with the powers necessary to enable it to perform its functions.

54. The chairperson of the Board Risk Committee must be an independent director of the bank.

55. The chairperson of the Board may be a member of the Board Risk Committee, but may not chair the Committee. The chair of the Board Audit Committee may also chair the Board Risk Committee.

56. The Board Risk Committee must have at least three members. All members of the Committee must be non-executive directors of the bank. A majority of the members of the Committee must be independent.

57. The Board Risk Committee must include members who have knowledge in risk management.

58. The Board Risk Committee must have a written charter that outlines its roles, responsibilities and terms of operation. The responsibilities of the Committee must, at a minimum, include:

a. supervision of all aspects of risk management within the bank. While the Board has the overall responsibility for risk management, the Risk Committee is the primary organ of the Board to carry out this responsibility;
b. advising the Board on the institution's overall current and future risk appetite and risk management strategy;
c. discussion of all risk strategies on both an aggregated basis and by type of risk and make recommendations to the Board on the risk appetite;
d. oversight of an institution-wide view of the institution's current and future risk position relative to its risk appetite and capital strength;
e. ensuring the effectiveness of the bank's risk management framework;
f. reviewing the bank's risk policies at least annually to ensure continued effectiveness and overseeing that management has in place processes to ensure the bank's adherence to the approved risk policies;
g. oversight of senior management's implementation of the risk management strategy;
h. constructive challenge of senior management's proposals and decisions on all aspects of risk management arising from the institution's activities;
i. reviewing the performance and setting the objectives of the bank's head of risk and ensuring this person has unfettered access to the Board and the Committee; and

j. oversight and endorsement of the appointment and removal of the person occupying the position of head of risk[12].

59. Other functions the Risk Committee will be responsible for include, but is not limited to, approving and overseeing the setting of delegation policies and all risk policies and standards. The Risk Committee must also ensure it receives adequate reporting of material risks, including key risk indicators for credit risk, liquidity, trading or market risk, balance sheet risk and operating risks as well as any other risks, possible weaknesses or threats considered relevant or referred by the Board for investigation. In reviewing the reporting on risks which the Risk Committee receives, it must ensure it can fulfil the requirements of paragraph 52 (c). The Risk Committee should also ensure that remuneration policies do not provide incentives for imprudent risk taking. (Annexure 1 of this Statement provides further information on these risks).

60. The Board Risk Committee must have free and unfettered access to senior management, risk and financial control personnel, and other parties (internal and external) in carrying out its duties.

61. The Board Risk Committee must invite the head of the risk function to attend all relevant sections of meetings of the Committee.

(ii) Board Audit Committee

62. A bank must have a Board Audit Committee, which assists the Board by providing an objective non-executive review of the effectiveness of the bank's financial reporting and the appointment, effectiveness and work of the internal and external auditors. in relation to compliance with internal policies and regulatory requirements.

63. The Board Audit Committee must have sufficient powers to enable it to obtain all information necessary for the performance of its functions.

64. Where an FBB is subject to regular audit by Head Office auditors, there is normally no need for it to establish an Audit Committee and this function can be undertaken by the Senior Overseas Officer, providing the internal and external auditors provide a copy of all their reports to the Senior Overseas Officer. However, the Reserve Bank will need to be satisfied as to the adequacy of such arrangements and would expect to meet with the auditors/representatives of Head Office when they visit Tonga to conduct audits and risk reviews of the local operations.

65. The Board Audit Committee must have at least two members. All members of the Committee must be non-executive directors of the bank. A majority of the members of the Committee must be independent.

12 If the head of the risk function is removed from their position, the reasons for removal must be discussed with the Reserve Bank as soon as practicable, and no more than 10 business days, after the Risk Committee's endorsement is agreed upon.

66. The chairperson of the Board Audit Committee must be an independent non-executive director of the bank with relevant experience.

67. The chairperson of the Board can sit on the Board Audit Committee but cannot chair the Committee.

68. The Audit Committee should, where possible, include members who have knowledge of or experience in audit practices, financial reporting and/or accounting.

69. The Board Audit Committee must have a charter that includes a reference to the Committee's responsibility for the oversight of the Reserve Bank's prudential reporting requirements, as well as other financial reporting requirements, professional accounting requirements, internal and external audit, and the appointment of the bank's external auditor.

70. The Board Audit Committee (or Senior Overseas Officer for a branch) must review the external auditor's engagement/appointment at least annually, including assessing whether the auditor meets the necessary Audit Independence standard.

71. The Audit Committee (or Senior Overseas Officer for a branch) is responsible for, amongst other things, ensuring:

- the adequacy and independence of the external and internal auditors;
- that internal and external audit plans cover all material risks and financial reporting requirements of the bank and that these plans are reviewed by the Audit Committee regularly to ensure adequate coverage of all material risks and financial reporting requirements is maintained;
- framing policy on internal audit and financial reporting;
- overseeing the financial reporting process;
- providing oversight of and interacting with the bank's internal and external auditors;
- approving, or recommending to the Board or shareholders for their approval, the appointment, remuneration and dismissal of external auditors;
- reviewing and approving the audit scope and frequency (internal and external) and development and regular review of the internal audit plan each year in conjunction with the head of internal audit;
- receiving key audit reports and ensuring that senior management is taking necessary corrective actions in a timely manner to address control weaknesses, non-compliance with policies, laws and regulations, and other problems identified by auditors and other control functions;
- overseeing the establishment of accounting policies and practices by the bank.

72. The Board Audit Committee (or Senior Overseas Officer for a branch) must hold management to account for process and risk management deficiencies identified in the work of both the internal and external audits. When deficiencies are identified, the Audit

Committee must ensure senior management is taking necessary corrective action in a timely manner to address control weaknesses, noncompliance with policies, laws and regulations and other problems identified by auditors. As such, the Committee or Senior Overseas Officer must have in place a system to track and respond to audit deficiencies and ensure timely corrective action is taken by management.

73. The members of the Board Audit Committee and the Senior Overseas Officer must, at all times, have free and unfettered access to senior management, the internal auditor, the heads of all risk management functions and the bank's external auditor, and vice versa.

74. The Board Audit Committee must establish and maintain policies and procedures for employees of the bank to submit, confidentially, information about accounting, internal control, compliance, audit, and other matters about which the employee has concerns. The Committee should also have a process for ensuring employees are aware of these policies and for dealing with matters raised by employees under these policies.

75. Members of the Board Audit Committee and the Senior Overseas Officer must be available to meet with the Reserve Bank on request.

76. The internal auditor must have a direct reporting line and unfettered access to the Board Audit Committee or Senior Overseas Officer.

III. Remuneration Policy

77. A bank must establish and maintain a documented Remuneration Policy, approved by the Board[13].

78. The Board must establish a Remuneration Committee which must have at least two members. All members of the Committee must be non-executive directors. A majority of the members of the Committee must be independent. The Chair of the Remuneration Committee may not be the Chair of the Board.

79. At a minimum, the Board or Remuneration Committee of the Board must be responsible for:

a. conducting regular reviews of the Remuneration Policy (at least annually);

b. overseeing and monitoring bank wide compliance with the Remuneration Policy;

c. considering on an annual basis compensation for the Chief Executive Officer (CEO), direct reports of the CEO, other persons whose activities may in the Board's opinion affect the financial soundness of the bank;

d. ensuring that remuneration is appropriate and consistent with the bank's culture, business and risk appetite and ensuring that the performance-based remuneration encourages behaviour that supports both the bank's long-term financial soundness and

13 FBSs and FBBs may adopt group wide remuneration policies, provided they comply with this Prudential Standard.

its risk management framework[14]. The Remuneration Committee must work closely with the Board Risk Committee in evaluating the incentives created by the remuneration system; and

e. overseeing the remuneration system's design and operation.

80. The Remuneration Policy must at a minimum:

a. Identify who is covered by the policy, which must include the CEO and direct reports and persons whose primary role is risk management, compliance, internal audit, financial control and any other persons who may have a significant effect on the safety and soundness of the bank;

b. detail the remuneration objectives and the structure of the remuneration arrangements, including but not limited to any performance-based remuneration components;

c. align remuneration with the objectives of the bank; and

d. encourage behaviour that takes into consideration the bank's long-term financial soundness and prudent risk management.

81. The Remuneration Policy must ensure that the structure of the remuneration of risk and financial control personnel, does not compromise the independence of these personnel in carrying out their functions.

I. Strategic and Business Planning

82. The Board and senior management must develop a written strategic plan for the bank, with appropriate measurable benchmarks. The strategic planning process should include the establishment of corporate objectives and the effective oversight of the implementation of these objectives.

83. The Board or Senior Overseas Officer must ensure that the strategic plan is current, feasible and based on sound economic and financial assumptions and is consistent with applicable laws, regulations, guidelines and internal policies.

84. A bank must maintain a written Business Plan that sets out its approach for the implementation of its strategic objectives. The business plan must be a rolling plan of at least three years' duration that is reviewed at least annually, with the results of the review reported to the Board or Senior Overseas Officer[15].

85. A bank must identify and consider the material risks associated with its strategic objectives and business plan, and must explicitly manage these risks through the risk

14 Where performance is not considered adequate, the Board or Senior Overseas Officer must be able to adjust (under the contractual terms of the employment contract or arrangements) the performance component of remuneration down to zero if necessary.

15 The business plan must provide projections for both the revenue statement and balance sheet at a minimum. It should preferably not just be a plan for the year end, but should have monthly and quarterly targets for all major items in both the revenue statement and balance sheet. The Board and senior management should regularly review the actual to budget/plan figures during each year to determine if adequate progress against the plan is occurring. Timely action should be taken where the actual performance lags where it was planned to be on a monthly or quarterly basis, providing assumptions and circumstances have not materially changed, which may call for a changed approach to the altered environment.

management framework, including how changing these plans affects its risk profile. The Business Plan must be consistent with risk management framework and the Board's risk appetite statement.

IV. Risk Management Framework

(i) General requirements

86. A bank must maintain a risk management framework that enables it to appropriately develop and implement strategies, systems, structures, processes, policies, procedures, people and other controls to effectively identify, monitor, measure evaluate, report and manage/mitigate its risks. The strategies, systems, structures, processes, policies, procedures, people and other controls comprising the risk management framework must be integrated and cohesive so that together they provide effective and adequate control of risks.

87. A bank must have policies and procedures that provide the Board of a locally-incorporated bank or Senior Overseas Officer with a comprehensive institution-wide view of its material risks and the controls thereof.

88. In the case of FBBs, various elements of the risk management framework set out in this Standard (Part III, Section V) shall generally apply to the parent bank. This would mean that the Reserve Bank will reply on the risk management framework of the parent bank in relation to the risk management matters pertaining to the FBB operations if that framework is considered equivalent to the one set out in this standard and covers the FBB's operations. However, if the Reserve Bank may require the FBB to apply these requirements locally if the parent bank's risk management framework is considered inadequate to take care of the risk management function of the FBB.

89. The requirements relating to organization of risk management function (Part III, Section V, sub-section (v) in a bank including adherence to the lines of defence principle shall apply to all banks including the FBBs. However, in the case of FBBs, Reserve Bank may consider exemption from or accept alternative arrangements for compliance with these requirements on a case-by-case basis if that is justified by their risk profile, size and complexity of operations and the level of compliance with the various regulatory requirements.

90. A bank's risk management framework must provide a structure for identifying and managing each material risk to ensure the institution is being prudently managed, having regard to the size and complexity of its operations.

91. A bank must ensure that compliance with, and effectiveness of, the risk management framework is subject to review by internal or external audit at least annually. The results of this review must be reported to the Board or Senior Overseas Officer.

92. A bank's risk management framework must, at a minimum, include:

a. a risk appetite statement. It is the Board's responsibility to set the risk parameters and tolerances which it expects management to operate within;

b. a risk management strategy (RMS). It is the Board's responsibility to approve the risk management strategy;

c. policies and procedures supporting clearly defined and documented roles, responsibilities and formal reporting structures for the management of material risks throughout the bank and which are consistent with the RMS and the established risk appetite;

d. a management information system that adequately measures and reports on all material risks, ensuring that appropriate risk management information is reported on a regular basis to management and the Board. The Board must identify and enforce its risk reporting needs in this regard, particularly ensuring it receives regular reports identifying risk levels against the risk limits and tolerances set in its risk appetite statement;

e. a risk management function; and

f. a review process to ensure that the risk management framework is effective in identifying, measuring, monitoring, managing and controlling material risks[16].

93. Depending on the size, business mix, complexity and risks undertaken by a bank, it may be appropriate for a bank to include in its risk management framework forward-looking scenario analysis and stress testing programs, which are based on severe, but plausible assumptions.

94. A bank's management information system must provide the Board and senior management with regular, accurate and timely information in relation to the institution's risk profile, and how the risk profile compares to the risk appetite.

95. A bank's data quality must be adequate for timely and accurate measurement, assessment and reporting on all material risks across the institution and must provide a sound basis for making decisions.

96. Senior management of the bank must monitor and manage all material risks consistent with the strategic objectives, risk appetite statement and policies approved by the Board.

97. A bank is required to provide the Reserve Bank with high level descriptions of its key risk management systems covering all material areas of risks and keep the Reserve Bank informed of all material changes to their risk management systems descriptions as they are made reflecting changing business conditions.

16 Where a material change to the size, business mix, risks faced and/or complexity of the operations is proposed, a bank must assess whether any amendment to, or a review of, the risk management framework is necessary to take account of these developments, at that time.

98. A bank must have and maintain a clear and concise risk appetite statement that addresses its key risks. The Board is responsible for setting the risk appetite of the institution and must approve the risk appetite statement.

(ii) Risk appetite statement

99. A bank's risk appetite statement must, at a minimum, convey:

a. the level of aggregate risk that the Board is willing to assume and manage in the pursuit of the bank's business objectives;

b. for each key risk, the maximum level of risk that the Board is willing to operate within, expressed as a risk tolerance or limit[17];

c. the process for ensuring that risk tolerances are set at an appropriate level, based on an estimate of the impact in the event that a risk tolerance is breached, and the likelihood of each material risk event occurring[18].

d. the process for monitoring compliance with each risk limit and for taking appropriate action in the event that it is breached[19;] and

e. the timing and process for review of the risk appetite[20].

(iii) Risk management and governance policy

100. A bank must have an 'overarching' risk management and governance policy which all other risk policies are consistent with and are connected to. There may be a separate risk management policy to a governance policy, but if so the two policies must be consistent and

17 It is also good practice (but not a requirement) to identify a normal operating range for each material risk or key risk indicator. This will allow easier identification of risks which need closer monitoring when they move outside the normal operating range.

18 Various factors should be taken into account by the Board in setting risk tolerances/limits, but the capital strength must be a core consideration and the primary objective of the limits set must be to keep the bank safe and sound on an ongoing basis. The likelihood of a risk event occurring ranges from very regular or constant e.g. loan defaults, to very occasional, such as a major economic downturn, which tends to be cyclical over a period of years. A convenient way of handling risk is to use a simple matrix, comprising the severity of the impact of a risk on one scale and the frequency of occurrence on the other scale. Risks can be plotted on such a graph and grouped into risk categories e.g. happens often, low impact; happens regularly but not often, medium impact; happens rarely, high impact. Obviously risks which occur often and are of high impact on the bank need much more attention from the Board and management than risks which occur rarely and are low impact. However there is no requirement to handle risk in this way, but there must be an adequate framework established in terms of this Prudential Standard.

19 The Board must not tolerate breaches of its risk tolerances/limits and must, through directions to its management team, actively manage risks. To do so it must receive regular reporting which will indicate if risk tolerances/limits are being approached (which requires regular measurement of the risks). Action must be taken by the Board to avoid a risk rising to the point where it breaches a limit. The action must be commensurate in terms of severity of action and urgency with the likelihood of a risk tolerance or limit being breached.

20 The risk appetite and risk tolerances should be changed when conditions change e.g. loan losses are likely to increase in the event of an economic downturn in the economy, so risk tolerances should be considered early in such a risk event, leading to changes in credit risk policies and the handling of problem loans (more intensive scrutiny). Because of this, Board's, as part of their risk responsibility, need to be examining the environment regularly in a forward looking manner and perusing data which will help them identify possible looming threats or a series of events which when combined, are likely to create a major risk event.

interrelated and whether combined or separate policies exist, the policy(s) must specifically cover risk governance and the Board's role in risk management of the bank.

101. The overarching risk management and governance policy(ies) required under paragraph 66 must, as a minimum, include:

a. Clearly defined authorities and responsibilities for the Board of Directors for locally incorporated institutions;

b. Clearly defined authorities and responsibilities for the Senior Management for locally and foreign incorporated institutions;

c. Requirements for appointment of the external and internal auditors;

d. an adequate, sound and integrated framework within which the whole risk management process will operate[21];

e. how material risks will be identified and assessed;

f. how material and key risks will be measured, including how these measures are validated and used;

g. controls identified for material and key risks, including the process for establishing, implementing and testing mitigation strategies and control mechanisms for material risks;

h. the process for monitoring, communicating and reporting risk issues, including escalation procedures for the reporting of material events and incidents;

i. the process for identifying, monitoring and managing potential and actual conflicts of interest;

j. the mechanisms in place for monitoring and ensuring ongoing compliance with all prudential and legislative requirements;

k. the process for ensuring consistency across the risk management framework, including the components identified under paragraph 82;

l. the process for establishing and maintaining appropriate contingency arrangements (including robust and credible recovery plans where warranted) for the operation of the risk management framework in stressed conditions; and

m. the process for review of the risk management framework.

102. There must be a risk policy for each material risk area and the bank should have policies covering all aspects of its operations. All risk policies must be reviewed at least annually[22] and approved or confirmed by the Board, or in the case of a branch operation by the Senior Overseas Officer.

103. Policies may allow for exceptions to policies with proper approvals, but the policy must provide for how these exceptions will be approved, handled and reported. The types of

[21] The risk management process must be able to identify risks currently impacting the bank as well as being forward looking to anticipate new risks or changes to the environment which will change the level of material or key risks.

[22] A bank must monitor the date when each policy or procedure was last revised, the date that it is next due for review, and who is responsible for the review. For convenience, the reviews may be conducted on a rolling basis throughout the year, policy by policy, or the review of all policies may be conducted at one time.

exceptions allowed and the process for approving them should be clear to employees responsible for implementation, including the approval level/person(s).

104. Before new products or services are introduced, a bank must ensure that there are policies covering these new products and services and in particular the risks associated with new products and activities are subject to adequate management and controls before being introduced or undertaken and must be approved in advance by the Board or its appropriate committee.

105. Policies and procedures typically include limits as part of the risk management and control structure. To be effective, limits established in policy must be monitored and reported and policies must establish how this will be carried out. The policy must also state who will monitor compliance with policies and the extent and timing of reporting at each level to which compliance is to be reported.

(iv) Risk management strategy

106. A bank must maintain a risk management strategy (RMS) that addresses its material and key risks. The RMS must be approved by the Board.

107. At a minimum, an RMS must:

a. describe each of the bank's key risks within its material risk categories and its approach to managing these risks;

b. list the policies and procedures dealing with risk management matters;

c. summarise the role and responsibilities of the risk management function;

d. describe the risk governance relationship between the Board, board committees and senior management with respect to the risk management framework; and

e. outline the approach to ensuring all persons within the bank have awareness of the risk management framework and for instilling an appropriate risk culture across the bank.

(v) Risk management function

108. A bank must have a designated risk management function that, at a minimum:

a. is responsible for assisting the Board, board committees and senior management to develop and maintain the risk management framework;

b. is appropriate to the size, business mix and complexity of the bank;

c. has the necessary operational independence and independent reporting lines to the Board, board committees and senior management to conduct its risk management activities in an effective and independent manner;

d. is resourced with adequate staff, who have clearly defined roles and responsibilities and who possess appropriate experience and qualifications to exercise those responsibilities;

e. can identify and make recommendations to ensure the operational structure of the bank facilitates effective risk management;

f. has access to all aspects of the institution that have the potential to generate material risk, including information technology systems and systems development resources;

g. has a head of the risk management function who is a senior executive at the same level as the heads of business units[23], so that the risk function is able to effectively challenge business units about risk taking, within the management structure (particularly about their decisions and activities which might materially affect the risk profile of the bank);

h. is able to recognise uncertainties, limitations and assumptions attached to the measurement of each material risk and report this to the Board;

i. must be able to identify and monitor material individual, aggregate and emerging risks and measure these risks and assess the current and future impact on the bank of its exposure to these risks;

j. subject to the review and approval of the Board, developing and implementing the enterprise-wide risk governance framework, which includes the bank's risk culture, risk appetite and risk limits;

k. ongoing monitoring of the risk-taking activities and risk exposures in line with the Board approved risk appetite, risk limits and corresponding capital or liquidity needs (i.e. capital planning);

l. establishing an early warning or trigger system for breaches of the bank's risk appetite or limits; and

m. reporting to managers and the Board or Risk Committee on these items, including, but not limited to, proposing appropriate risk-mitigating actions.

n. is required to notify the Board of any significant breach of, or material deviation from, the risk management framework.

109. A bank may engage the services of an external service provider to perform part of the risk management function where the institution can demonstrate to the Reserve Bank that the risk management function meets the requirements in paragraph 82.

[23] Ideally the head of the risk function must be independent from business lines, other revenue generating responsibilities and the finance function. The head of risk, who is often titled Chief Risk Officer (CRO), must not be the Chief Executive Officer (CEO), Chief Financial Officer, or Head of Internal Audit. However, for smaller banks, where this is not considered feasible, the structure must seek to achieve the objectives of this Prudential Standard. The Reserve Bank may intervene and designate an alternative structure if it considers the structure established by a bank is not effectively achieving the objectives of this Prudential Standard. Nevertheless, the head of risk must always have a direct reporting line to the CEO, and have regular and unfettered access to the Board and the Board Risk Committee.

110. Outsourcing any part of the risk management function by a bank must also meet the requirements of the Prudential Standard on Outsourcing.

(vi) Risk culture

111. The Board must form a view of the risk culture in the bank and whether the risk culture meets the Board's requirements. The Board must determine whether that culture supports the ability of the bank to operate consistently within its risk appetite. The Board must also identify any desirable changes to the risk culture and ensure the institution takes steps to address those changes. The Board must address this regularly to ensure there are no signs that the risk culture of the bank has changed over time and if it has, then measures are implemented promptly to bring the risk culture within the Board's desired parameters.

112. The risk culture developed must promote risk awareness and encourage open communication and challenge about risk-taking across the bank, as well as between the Board and managers.

(vii) Risk management declaration and notification requirements

113. The Board or Senior Overseas Officer must make an annual risk management framework declaration to the Reserve Bank within 3 months of the bank's balance date, stating that, to the best of its knowledge and having made appropriate enquiries:

a. the bank has in place systems for ensuring compliance with all prudential requirements;

b. the risk management framework is appropriate and adequate for the size and complexity of the bank and enables it to monitor and manage its risks including, where appropriate, by setting and requiring adherence to a series of prudent limits, and by adequate and timely reporting processes;

c. risk management and internal control systems have been established and these risk management systems are operating effectively and are adequate having regard to the risks they are designed to control;

d. the Board and management have identified the key risks facing the bank;

e. the bank has a RMS and Risk Appetite statement that complies with this Prudential Standard, and the bank has complied with each measure and control described in the RMS and the tolerances in the Risk Appetite statement;

f. the bank is satisfied with the effectiveness and reliability of the processes and systems surrounding the production of financial information at the bank;

g. The risk management systems descriptions held by the Reserve Bank are accurate and current; and

h. the bank in the financial year just completed has complied with the statutory and prudential requirements of the Money Laundering and Proceeds of Crime Act, banking licence conditions, all of the Reserve Bank's Prudential Standards and other prudential requirements.

114. If a bank feels it needs to qualify the declaration prescribed in the previous paragraph, it would need to explain to the Reserve Bank the reasons for the qualifications, as well as provide plans for corrective action.

115. The declaration must be approved by the Board and signed by the chairperson of the Board and the chairperson of the board Risk Committee or Audit Committee; or the Senior Overseas Officer (in the case of a branch); as well as the Chief Executive Officer in all cases.

116. The Board or Senior Overseas Officer must qualify the risk management declaration if there has been any significant breach of the risk management framework. Any qualification must include a description of the cause and circumstances of the breach and steps taken to remedy the problem. Where a corporate group declaration is submitted (which is permitted), the qualification must state whether it relates to the group or bank's risk management framework.

117. A bank must notify the Reserve Bank immediately after it becomes aware:

a. of a significant breach of the risk management framework; or

b. that the risk management framework did not adequately address a key risk.

118. A bank must on adoption, and following any material revisions, submit to the Reserve Bank a copy of the bank's:

a. risk appetite statement;

b. business plan; and

c. RMS

as soon as practicable, and no more than 10 business days, after Board approval.

119. A bank must notify the Reserve Bank as soon as practicable, and no more than 10 business days, after it becomes aware of any material or prospective material changes to the size, business mix and complexity of the bank.

120. In addition, a bank is required to submit to the Reserve Bank on an annual basis the Reserve Bank Return "Certification of Compliance with the Banking Act (2020) (the Act)".

V. Compliance function

121. A bank must have a designated compliance function that assists management in effectively managing compliance risks. Preferably the compliance function should be independent, but if this is considered not to be economically feasible for a small bank, then the proposed compromise must be discussed with the Reserve bank, including how the compromise will deal with and affect the principles contained in this Prudential Banking Standard.

122. The Compliance function is responsible for, amongst other things, ensuring that the bank operates in compliance with all internal policies as well as applicable laws and regulations, including the Prudential Banking Standards.

123. The compliance function must be adequately staffed by appropriately trained and competent persons who have sufficient authority to perform their role effectively, and have a reporting line independent from business lines.

124. The compliance function must routinely monitor compliance with rules, regulations and policies (including all internal policies and procedures) to which the bank is subject and compliance reports must be available to the Board and/or Board Audit Committee.

VI. Internal Audit

125. A bank must have an independent and adequately resourced internal audit function, which is reflective of the size and nature of the bank's business.

126. The objectives of the internal audit function must include evaluation of the adequacy and effectiveness of the financial and risk management framework of the bank.

127. To fulfil its functions, the internal auditor must, at all times, have unfettered access to all the bank's business lines and support functions.

128. The Internal Auditor must be independent from business lines, other revenue-generating responsibilities and the finance function. The Internal Auditor must have a direct line of report to the Board Audit Committee and the Internal Auditor will only report to the management line for administrative purposes, such as terms and conditions of employment.

129. The Internal Auditor will draw up an internal audit plan for the year in conjunction with the Board Audit Committee and take instructions from the Board Audit Committee, including in the coverage of items within the plan that the Board and Board Audit Committee consider requires attention or they need more information or another opinion about. The Internal Audit function is to support the Board Audit Committee in its need to have an independent line of enquiry[24] into risk and related matters, unfettered by management's views and opinions, where needed.

130. A bank must ensure that the scope of the internal audit includes a review of the policies, processes and controls put in place by management to ensure compliance with the Reserve Bank's prudential requirements.

PART IV

24 This is because the members of the Board Audit Committee must be non-executives and therefore at times may need independent investigation, analysis, assurance and verification of matters.

CORRECTIVE MEASURES AND THE RESERVE BANK'S ULTIMATE AUTHORITY

I. Remedial measures and sanctions

131. Non-compliance with the requirements of this Prudential Standard will be subject to corrective actions as provided under section 22 and/or 39 of the Banking Act (2020), depending on the circumstances, and the administrative penalties outlined in Prudential Standard No.3 Administrative Penalties.

132. As well as non-compliance with any provision of this Prudential Standard as per paragraph 117, if a bank fails to comply with the instructions and reporting requirements, or if there is risk that the risk management is inadequate and may cause the capital base to be impaired and result in a condition that threatens the interests of depositors or the general public, the Reserve Bank may pursue appropriate corrective actions and sanctions by imposing or varying requirements, or by imposing conditions on the bank's licence as provided in Part IV of the Act (section 22 and 39). Such requirements or conditions imposed on a bank may include, but are not limited to requiring the bank to take certain steps or to refrain from adopting or pursuing a particular course of action or to restrict the scope of its business in a particular way, including a prohibition from engaging in certain business or activities for a specified period of time. The Reserve Bank might also require, but is not limited to, one or more of the following remedial measures or sanctions:

i Require the bank to improve its risk management in various ways, or take other measures to reduce the banks risks;

ii Require the bank to cease entering into certain types of business or dealing with certain types of customers until further notice and/or (s) offering certain types of products and services;

iii Require the bank to report more frequently to the Reserve Bank and in more detail, particularly regarding improvements to its risk management;

iv Require the bank to maintain higher Minimum Capital Ratios (as per paragraph 19 under the heading 'Minimum Capital Ratio') under the Prudential Standard number 6 Capital Adequacy Requirements;

v Impose limitations or prohibitions on the acceptance of deposits (either generally or from persons who are not already depositors), the borrowing of money, the granting of credit or the making of investments by the bank, or cause the bank to cease undertaking banking business altogether;

vi Prohibit the bank from entering into certain types of transactions or classes of transactions;

vii Suspend access to the credit facilities of the bank; or

viii Suspend or require the removal of any directors or managers.

II. Final Authority

133. The Reserve Bank may vary or waive any provision in this Prudential Standard in relation to one or more specified banks.

134. The Reserve Bank has the final determination or interpretation of any provision within this Prudential Standard, whether or not a provision states it is normally for a bank to determine. The Reserve Bank may always override a bank's interpretation and it will normally consider the particular facts and circumstances of a situation in doing so.

135. Where this Prudential Standard provides for the Reserve Bank to exercise a power or discretion, this power or discretion will be exercised in writing.

136. In this Prudential Standard, unless the contrary intention appears, a reference to an Act, Regulations or Prudential Standard is a reference to the Act, Regulations or Prudential Standard as in force from time to time.

137. A bank must contact the Reserve Bank if it seeks to place reliance, for the purposes of complying with this Prudential Standard, on a previous exemption or other exercise of discretion by the Reserve Bank. In these cases the Reserve Bank will consider whether transition arrangements are appropriate to allow the bank time to become compliant with the provisions of this Prudential Standard. When making such an application, the bank must submit a plan detailing how it intends to become compliant with the requirements of this Prudential Standard and the proposed timeframe for it to achieve full compliance.

PART V

EFFECTIVE DATE

I. Commencement

138. The effective date of this prudential standard shall be XXX.

II. Supercedence

139. This standard supersedes and replaces Prudential Standard 9 - Governance which was revised in 2014.

National Reserve Bank of Tonga

Salote Road
(Private Bag No. 25)
Nuku'alofa
Kingdom of Tonga

ANNEXURE 1

DEFINITIONS OF RISKS

- **Credit risk** is the potential financial loss resulting from the failure of customers to honour fully the terms of a loan, contract or other exposure of the bank. The Reserve Bank has issued Prudential Standards on Asset Quality (Prudential Standard 1) and Credit Risk Grading Systems (Prudential Standard 2).
- **Liquidity risk** is the risk that a bank cannot meet its commitments as and when due. Liquidity conditions in markets can change suddenly and in certain circumstances deposits become far less stable, hence liquidity buffers must be maintained at all times as per Prudential Standard No. 5 Liquidity.
- **Market risk** (or trading risk) and investment risk is the potential risk to earnings resulting from changes in interest rates, currencies and equity and commodity prices. Market risk the potential risk to earnings and capital resulting from changes in interest rates, changes in market and investment prices and the impact of exchange rate fluctuations on foreign currency positions. It includes interest rate risk in the banking book.
- **Operational risk** is the potential inherent risk in day to day business operations. Risks include natural disaster, system failure, fraud and forgery. The Reserve Bank may issue (or amend) Prudential Standards in relation to the management of these risks.
- **Strategic and planning risk** is the risks arising from the strategic objectives and business plans not being met, or circumstances arising which increase the strategic threats faced by a bank (changes in the external environment) or weaknesses of the bank (changes in the internal environment of the bank).
- **Legal, reputational and compliance risk** is:
    - legal and documentation risk (LR) is the risk of some unanticipated legal or documental hindrance that renders transactions incomplete or non-binding. The management of legal and documentation risk involves the consulting of expert legal advisers, consulting with the authorities when appropriate, and the avoidance of transactions where there remains doubt about the legality of the transaction.
    - reputational risk (RR) is the risk of negatively affecting the bank's image, which could prejudice its ability to retain and generate business. RR is a risk faced by all companies, but is particularly crucial in the case of banks. Continuation of business depends on reputation, and any damage to reputation can exacerbate liquidity risk. Bank runs have been caused by damage to reputation.
    - compliance risk (CR) is the risk of non-compliance with Statutory or regulatory requirements of the Government and regulators, as well as regulatory requirements of financial exchange/s and other generally accepted codes, such as the corporate governance codes. Non-compliance may lead to

the withdrawal of licenses to do business, and to the incurring of penalties. This has severe RR fallout.

- **Information security risk** comprises the impacts to an organization and its stakeholders that could occur due to the threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate. This is a risk to organizational operations (including functions, image and reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems.

The Reserve Bank may issue (or amend) Prudential Standards in relation to these risks, which bank's should refer to.

ANNEXURE 2

GUIDANCE: GOVERNANCE AND RISK MANAGEMENT

Introduction

1. This guide provides further information to assist Licensed Financial Institutions (banks) understand the Reserve Bank's expectations regarding compliance with the Prudential Standard on Governance and Risk Management.

2. The objective of this Guidance is to encourage an effective risk governance model that contains checks and balances to support appropriate consideration of risk management throughout a bank.

Risk Governance

3. Risk governance refers to the formal structure used to support risk-based decision making and oversight across all operations of a bank. The risk governance of a bank forms an integral part of its risk management framework.

4. Risk governance typically consists of board committees and management committees, delegations, management structures and related reporting, as well as various controls (such as policy constraints) to prevent bad practices from occurring, including to control conflicts of interest from influencing decision making. Risk governance is an important aspect of corporate governance.

5. Corporate governance is reflected in the way relationships are established, facilitated and controlled internally between the Board, management and other staff and externally with depositors, shareholders and other stakeholders. Corporate governance affects, amongst other things, how a bank:

viii. Sets corporate objectives;

ix. Determines its risk tolerance/appetite;

x. Runs the daily operations of the business;

xi. Protects the interests of depositors;

xii. Is accountable to the shareholders;

xiii. Takes into account the interests of other stakeholders; and

xiv. Operates in a safe and sound manner, with integrity and in compliance with applicable laws and regulations.

6. In considering risk governance, there is an appropriate balance between achieving business objectives and managing risk, which will vary from bank to bank. Generally, the dictates of markets mean that as returns rise, so does the risk (i.e. greater returns are required by investors as risk increases). Good risk governance should ensure that risk is well managed within risk boundaries established by a bank and that the business objectives and returns sought by the bank are planned and managed consistently within the risk boundaries set. If a

bank is to operate in a safe and sound manner, it is critical that the Board of a bank takes a leading role in risk governance and commits its time and focus, in a balanced manner, towards risk governance, not just business growth and profitability.

7. The risk governance structure will be dependent on the size, business mix, complexity and types and extent of risks faced.

8. Sound risk governance at Board, Board Committee and senior management levels is central to risk management because:

i. the conduct and competency at the top establishes the standard and pattern of conduct and culture in the whole of the organisation;

ii. it gives leadership in the development of a safe and sound banking business, establishing the right balance between risk and return i.e. the Board in their role of risk governance, decides the balance between the desire to achieve strategic objectives and the risks which may be inherent in achieving those objectives, or the time within which the objective is to be reached and tailors the strategic plan accordingly in balance with its risk appetite;

iii. it provides direction for the development and implementation and maintenance of the risk management framework. In doing so, it ensures the risk management framework is enterprise wide and well understood throughout the bank;

iv. it establishes and varies risk limits or boundaries and priorities in a timely manner, both in the risk appetite statement and in policies, which it approves or endorses;

v. through the broad background, skills and experience of the directors, as well as their independence from the day to day operations, it provides an objective view of the business undertaken and market niches addressed, so that the risks inherent in that business can be clearly identified and assessed and timely mitigation strategies introduced;

vi. it regularly considers and develops plans to counter any developing gaps between strategic initiatives, day-to-day operational performances and emerging risk management issues, which may all be linked. This is a dynamic process.

9. A fundamental concept for risk governance within a bank is establishing:

i. ‘risk ownership’ within a bank. With risk ownership comes responsibility for the identification, measurement, monitoring and management of risks;

ii. functionally independent review and challenge. Experience shows that good governance of a bank requires there to be a view of risk within a bank which is not confused or compromised by business growth and profitability objectives and incentives. The view provided must be at a sufficiently senior level that effective challenge to high risk objectives is provided, so that risk is appropriately considered and a balance

achieved which is acceptable within the Board's Risk Appetite (see later);

iii. independent assurance. As with the audit of financial records, there must be an independent assurance within an bank that risk is not exceeding the Board's risk appetite. This assurance must be continuous rather than periodic, because changes in the internal and external environment are occurring continuously and risks change with these changes in the environment.

These provide a sound basis for ensuring risks are appropriately identified, assessed and managed.

10. In addition, risk governance and risk management needs to be forward looking as well as focussing on the current position. Risks within the current/existing environment can normally be managed reasonably well by banks that have achieved good risk management. However risks change and the environment within which an bank operates changes continuously. Therefore, the risk management framework should seek to identify potential risks or changes in risk as early as possible so that the Fi is not caught by surprise. The more time a bank has to adjust or plan for changes in risks or the realisation of potential risks, the better prepared and resilient the bank is likely to be.

11. One such model that is widely used and provides an effective framework for risk governance is the three lines of defence risk management and assurance model. This model provides defined risk ownership responsibilities with functionally independent oversight and assurance. banks may choose to use alternatives to the three lines of defence model if similar outcomes can be achieved. Whichever model is chosen, the detail of the implementation of the model will often vary in different banks.

The three lines of defence model

12. A graphical representation of a sample implementation of the three lines of defence model is provided at **Attachment A** of this Guidance.

a. The first line of defence

13. The first line of defence comprises the business management[25] who should have ownership of risks. Accordingly, business management is responsible for day-to-day risk management decision-making involving risk identification, assessment, mitigation, monitoring and management. Making the 'front line' mangers and staff (those interfacing with customers and the public to deliver the banks products and services) responsible for risk as well as business objectives, creates a balanced approach towards customer and the public by managers and staff. The Reserve Bank expects the roles and responsibilities of risk owners to be clearly defined and, where appropriate, incorporated into performance reviews.

[25] Business management typically includes all levels of management responsible for business decision-making. The first line of defence also includes relevant management committees.

14. A key tenet of the three lines of defence model is that business management cannot abrogate its responsibility for risk management. The first line of defence is responsible for:

a) effective implementation of the risk management framework, including reporting and escalation of relevant information to responsible senior management, and to the second line of defence or as far as the board committees or the Board of directors (the Board)[26], as necessary; and

b) managing risk in a way that is consistent and integrated with the risk management framework.

Executive and senior business management would ensure risk ownership is clearly defined and that the risk management framework is effectively implemented and supports decision-making. This would usually include reporting, escalation and monitoring procedures that are appropriate for the management of different risk categories.

b. The second line of defence

15. The second line of defence comprises the specialist risk management function(s) that are functionally independent of the first line of defence. The second line of defence supports the Board and its committees by:

a) developing risk management policies, systems and processes to facilitate a consistent approach to the identification, assessment and management of risks;

b) providing specialist advice and a development program to the Board, board committees and first line of defence on risk-related matters;

c) objective review and challenge of:

i) the consistent and effective implementation of the risk management framework throughout the bank; and

ii) the data and information captured as part of the risk management framework which are used in the decision-making processes within the business, in particular the completeness and appropriateness of the risk identification and analysis, ongoing effectiveness of risk controls, and prioritisation and management of action plans; and

d) oversight of the level of risk in the bank and its relationship to the risk appetite, and any necessary reporting and escalation to the Board or its committees.

16. In order to be effective, risk management functions would have:

a) adequately experienced staff with relevant technical knowledge who facilitate the development, ongoing review and validation of the risk management framework; and

26 For the purposes of this Guidance, a reference to the Board, in the case of a foreign ADI, is a reference to the Senior Officer Outside of Tonga or Compliance Committee (as applicable) as referred to in Prudential Standard on Governance and Risk Management.

b) appropriate seniority and authority, with access to the responsible board committees.

17. Smaller and less complex banks often combine risk management roles with other roles or functions. Where such dual roles exist, the Reserve Bank expects that appropriate care would be taken to ensure that the objectiveness of the risk management function is maintained and that any conflicts of interest are identified and appropriately managed.

c. The third line of defence

18. The third line of defence normally comprises essentially the audit function. In particular the internal audit provides the Board Audit Committee (or Senior Overseas Officer or functional internal audit part of the overseas banking group, (provided that functional unit reports to the head Board Audit Committee without interference from management) in the case of a branch) with the means to assure itself about the conduct of risk management within the bank and that other information it is receiving from management accurately reflects the true position.

19. However, the application of the third line of defence would vary depending on the size, business mix and complexity of a bank. The independent assurance function could, for example, include internal audit, a third-party assurance provider or a combination of the two. A key consideration would be appropriate independence, technical knowledge and experience.

20. The internal audit function therefore reports to the Board Audit Committee and not to any area of management, except for administrative purposes, such as remuneration and setting of employment conditions.

21. The internal (and external audit) must have full and free access to all business lines and information.

22. Findings by the third line of defence would, of course, be made available to management as well as the Board Audit Committee. While findings raised by the third line of defence would typically be utilised by management to increase business efficiency and inform decision-making, these benefits are secondary to the primary assurance objective.

23. The internal auditor in conjunction with the Board Audit Committee should draw up a plan annually which reflects the areas the Board Audit Committee want covered. This would be assessed by the Audit Committee on a risk basis. The internal audit plan should be reviewed throughout the year by the Audit Committee, not only to check progress against plan, but to make adjustments in circumstances where information changes the Audit Committee or Boards' view on what needs to be covered, so adjusting priorities or changed consideration of the urgency of coverage of certain areas.

Role of the Board

24. Under the Prudential Standard on Governance and Risk Management, a bank must at all times have a risk management framework that governs the way the bank manages risks arising in the bank. This Prudential Standard affirms that the Board is ultimately accountable for the risk management framework of the bank and is responsible for the oversight of its

operation by management. Together, the Board Risk Committee and Board Audit Committee assist the Board in its oversight of the operation by management of the overall risk management framework.

25. The Board Audit Committee assists the Board in fulfilling its corporate governance and oversight responsibilities in relation to an entity's financial reporting, internal control system, risk management framework and internal and external audit functions (i.e. independent assurance).

26. In performing its responsibilities, the Board may obtain advice from board committees, external advisers and management and seek their recommendations as the Board considers prudent. Provided the directors approach their role with an enquiring mind and make an independent assessment of the matters for decision, the Board is normally entitled to place reasonable reliance on the recommendations and advice it receives, commensurate with the directors understanding of the skills and experience and previous record of those it consults in decision making.

27. The Board is directly responsible for the broader strategy of the bank and under the Prudential Standard on Governance and Risk Management is required to consider and approve the risk appetite statement, strategic plan, business plan and risk management strategy[27]. There is potential for some of these responsibilities to create an apparent or potential conflict in or clash of objectives. This requires the broad skills and experience of the Board as a whole to properly balance the objectives in achieving the sound and safe operation of the bank. For example, the strategic objective of profit and growth cannot be the overriding objective without creating excessive risk for the bank in the medium to longer term. Hence, the effective design of the documents and related processes the Prudential Standard requires the Board to consider and approve by the bank will facilitate their integration, with each process appropriately supporting the others.

28. The Board approval and oversight responsibilities for the risk management framework are unaffected if risk management and business operations are outsourced to a third party or are performed by another part of a group of companies. That is, the Board are not relieved of any of their responsibilities.

29. The Board is responsible for determining the appropriate level and quality of capital for the bank above the minimum capital requirements set out in Prudential Standard No. 6 on Capital Adequacy having regard to the risk profile and nature of risks faced by the bank. Capital provides the bank with an ability to 'weather' the occurrence of expected or unexpected risks. The consideration of capital must be done in conjunction with the setting of risk tolerances within the Risk Appetite statement, which places boundaries on the risk profile. In turn the internal and external environment within which the Fi operates must be carefully examined periodically by the Board when undertaking these considerations. The frequency and depth of consideration of environmental factors and risks should increase proportionally to the rate and nature of change occurring. The capital adequacy requirements

27 Where a material change to the size, business mix, risks faced and/or complexity of the operations is proposed, a bank must assess whether any amendment to, or a review of, the risk management framework is necessary to take account of these developments, at that time.

set by a Board must be prudent and appropriate to the bank's business[28] and reflect the risks undertaken by, and presented by, a bank in the context of the markets and macroeconomic conditions in which it operates (including all reasonable and foreseeable circumstances)[29].

30. In determining whether the Board has met its responsibilities under the Prudential Standard on Governance and Risk Management, the Reserve Bank will assess the steps taken by the Board to ensure it meets those responsibilities. For example, the Reserve Bank expects senior management to report on the material risks and escalate material risk issues to the Board or the Board Risk Committee level. The Board and/or Board Risk Committee could also obtain independent views and reports as they deem appropriate, as well as consider risk issues escalated from the risk management function. The Reserve Bank expects that the Board would clearly communicate its expectations in respect of the reporting and escalation to be provided by management, the risk management function(s) and internal audit. Where the Board considers that the risk reporting is ineffective or that material risk issues have failed to be escalated, the Reserve Bank expects the Board to adopt all appropriate measures (including directions for management remedial actions and reports) to identify and address the reasons for the failure.

Risk management culture

31. The Prudential Standard on Governance and Risk Management requires a Board to ensure that they form a view of the risk culture in the bank and the extent to which that culture supports the ability of the bank to operate consistently within its risk appetite. The Prudential Standard also requires the Board to identify any desirable changes to the risk culture and ensure the bank takes steps to address those changes. The Reserve Bank's view is that a sound risk culture is a core element of an effective risk management framework. Risk culture refers to 'the norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify, understand, openly discuss and act on the organisation's current and future risk'30 . The Reserve Bank expects that the Board would have a view of the risk culture that is appropriate for ensuring that the bank operates within the risk appetite.

32. A bank's risk culture is strongly influenced by the 'tone at the top'. The Reserve Bank expects the Board and senior management to demonstrate their commitment to risk management and foster a sound risk management environment in which staff will be actively engaged with risk management processes and outcomes, and a risk management function that is influential and respected. The development of the risk culture is likely to occur through an iterative process involving both the Board and senior management providing a consistent

28 It is the Board's responsibility to understand the business the bank operates and the inherent risks that result from the activities the Board allows the bank to undertake. At a minimum, capital must be adequate to allow the bank to survive a downturn or significant risk event by providing a buffer against losses which will bridge it across a downturn or series of events which extend over a period of time, potentially spanning more than a year or two. While the Reserve Bank sets minimum capital requirements in Prudential Standard No. 6: Capital Adequacy, these are bare minimums, which the Reserve Bank will view very seriously if breached. Since each bank's business is different with a different risk profile it is expected that the Board will set capital requirements suitable for the bank and must not abrogate its own responsibility to all stakeholders to ensure its capital is adequate, by just assuming it will operate at a margin above the minimum set by the Reserve Bank.

29 Including those resulting from severe (but plausible) changes in the environment and from multiple risks escalating and impacting on the bank at the one time.

30 Refer to the Institute of International Finance (2009) "Reform in the financial services industry: "Strengthening Practices for a More Stable System". In fostering an effective risk culture it is important that there is consideration of the culture across the whole organisation.

approach over time, in varying situations and aspects or parts of the business. It must be remembered that all operations of a business in varying ways is conducted and happens through people, who will inevitably have differing backgrounds and experiences. It is therefore important that the bank establishes what is acceptable and what is not acceptable as far as risk culture is concerned. This starts with recruitment practices and decisions about the selection of people for key positions.

33. A bank influences and communicates its desired risk culture through its business strategy, risk appetite, and understanding of key risks and capabilities, as well as how risk management behaviours are encouraged and rewarded.

34. A sound risk culture:

a) supports transparency and openness of risks, events and issues, and facilitates effective internal controls and risk reporting;

b) encourages awareness of risks and responsibility for managing those risks;

c) encourages staff at all levels to identify and report matters that might impact on risk. Management cannot do everything, people on the job are those closest to what is happening and are therefore likely to recognise if something is wrong or changing before anyone else in the organisation becomes aware of it;

d) ensures that appropriate actions are taken in a timely manner for issues and risks identified that are outside of set thresholds and tolerances/limits. For example, risk indicators that remain 'red' for extended periods of time could indicate complacency or a lack of funding in the overall management of risk; and

e) rewards staff for appropriate risk management behaviours. Typically, this would be achieved through incorporating risk management as a core responsibility within individual roles and responsibilities.

35. The Reserve Bank considers that the development of the desired risk culture would be assisted by a Code of Conduct, ongoing risk education and awareness training programs, processes to ensure behaviour is monitored and managed within the risk appetite, and robust and prudent risk management policies.

36. Remuneration policies will positively influence the desired risk culture if they are designed to encourage and provide incentives for employees to act responsibly and with integrity, in a manner consistent and integrated with the bank's risk management framework[31]. If some of an employee's remuneration is contingent on performance, then it is important that some of the performance indicators involve risk management. Performance indicators or targets for the achievement of remuneration that just reward business growth or profitability are likely to encourage risky behaviour to achieve those rewards, particularly if this component of the remuneration is substantial. Remuneration which is contingent on

31 Banks should seek expert guidance on the design of remuneration policies.

performance should be able to be adjusted down to zero where risk management has been unacceptable.

Group risk management

37. The Prudential Standard on Governance and Risk Management allows a bank that is part of a group to meet the requirements of the standard on a group basis provided that the Board of the bank is satisfied that the requirements are met in respect to that bank.

38. The Reserve Bank expects that the appropriateness of using a group risk management framework would be assessed by that bank according to the size, business mix, complexity and risks of that bank's operations. The purpose of this assessment is to ensure that the group's framework is 'fit for purpose' for the bank. The Reserve Bank expects that the assessment would be appropriately documented.

39. The Reserve Bank expects this assessment by the bank to be conducted prior to using the group's framework and after any changes to the group or the bank that may materially impact on the risk management framework. The bank needs to have a clear understanding of the reliance on, and interaction with the (group's) risk management framework, and understand the consequences of these arrangements for the risk profile of the bank.

Risk management framework

40. A risk management framework enables a bank to identify, analyse and manage the current and emerging material risks within its business. Effective approaches to risk management provide meaningful information that appropriately supports decision-making and oversight at each level within the bank. The risk management framework will ideally support an bank in:

a) identifying, analysing and understanding each of the material risks at all levels of the bank;

b) ensuring that appropriate strategies and policies and effective operating controls and other mitigants, are in place and operating effectively;

c) providing reliable and meaningful risk information (reporting) to decision makers;

d) ensuring that there is adequate oversight of the risk profile and management framework; and

e) facilitating a sound risk culture.

41. This is achieved, in part, through a clearly articulated risk appetite statement that outlines the bank's risk appetite and risk tolerances within its risk capacity32.

42. The Reserve Bank expects that the primary focus of a bank's risk management framework would be the management of risks in a way that is consistent with the best

32 Refer to Prudential Standard on Governance and Risk Management for the definitions of risk appetite and risk tolerance. Risk capacity is the maximum risk a bank can bear.

interests of depositors, the maintenance of the sound financial position of the bank and the bank's strategic objectives and business plan.

43. A bank would ordinarily ensure that appropriate controls are established that are consistent with the risk appetite, risk profile and capital strength, and steps are taken to ensure they are appropriately communicated within the bank. In order to assess whether the communication of controls has been appropriate, an bank would ordinarily take steps to assess whether the information has been received and understood.

44. The Prudential Standard on Governance and Risk Management requires the Board to ensure that it recognises uncertainties, limitations and assumptions attached to the measurement of each material risk. In addition to recognition of these matters by the Board, the Reserve Bank expects that they would be well understood within the bank.

45. Risk can arise from structures that impede transparency, such as special-purpose or related structures. The Reserve Bank expects that the bank's operational structure and associated risks would be well understood in the bank, recognised by the Board, taken into account in the risk management framework and reported, as appropriate (including to the Board or its committees where necessary).

46. Stress testing, including both scenario analysis and sensitivity analysis is used to assess a range of potential impacts as a result of different material risks. Stress testing is important in considering potential changes that could occur in the external operating environment, and provides a more forward looking view of a bank's risk profile. The Reserve Bank expects larger banks to undertake stress testing and this stress testing would be based on a combination of robust modelling and informed expert judgement, with effective senior management engagement and appropriate Board oversight.

47. As good practice, a bank would publicly disclose in an appropriate way (such as its published annual report where applicable) an outline of its risk management policies, including where relevant the policies governing dealings between the bank and other group members.

48. The risk management framework supports the Board and senior management in obtaining an appropriate view of the bank's overall risk profile[33]. Reporting of risk facilitates decision-making and oversight, taking into consideration the overall structure and nature of the bank's business and different approaches to managing different material risks. In understanding the overall risk profile of the bank, specific consideration would be given to:

a) identifying risks throughout the bank that, in combination, may have a material impact on the bank[34];

33 The risk profile is the sort of risks and level of those risks which the bank is experiencing i.e. the risks an bank is exposed to (actual and potential) and the level to which these risks have been allowed to reach.

34 The risk management process must be able to identify risks currently impacting the bank as well as being forward looking to anticipate new risks or changes to the environment which will change the level of material or key risks.

b) understanding the interaction of material risks throughout the bank. For example, a failure in processes or systems (operational risk) may result in loans not being properly monitored (credit risk); and

c) risks of contagion arising from issues identified with related parties (including any non-Reserve Bank regulated activities).

49. The Reserve Bank may require a bank, excluding FBBs, to have an Internal Capital Adequacy Assessment Process (ICAAP)[35]. These documents involve an integrated approach to capital adequacy and risk management aimed at ensuring that the capital held is adequate in the context of the risk profile and risk appetite of that bank. An bank's risk management framework and ICAAP/CMP are required to be integrated and consistent.

50. A bank is not required to duplicate content between its ICAAP summary statement or ICAAP report and its risk management strategy. However, the Reserve Bank expects that the risk management strategy would contain sufficient detail to provide a holistic view of the bank's strategy for managing risk without having to source other documents. Where other documentation contains additional detail, the Reserve Bank expects that cross-references will be clear and up-to-date to facilitate consistency and integration between the documents.

Material risks

51. The Prudential Standard on Governance and Risk Management identifies categories of risk that the risk management framework must, at a minimum, cover. The Reserve Bank's view is that the emphasis on each risk category is likely to differ according to the size, business mix, complexity and risks faced by of the bank. The Reserve Bank expects that an bank would be able to demonstrate how it determines the 'materiality' of risk categories and to identify the key risk drivers within each category. Communicating what the bank views as material is important to ensure that its approach is understood by its staff and is consistently applied across its operations.

Strategic and business planning

52. The Prudential Standard on Governance and Risk Management requires a bank to maintain a business plan that sets out its approach for the implementation of its strategic objectives. The business plan is an important management and control tool that enables a bank to identify how it will achieve its strategic objectives.

53. Fundamental to an effective risk management framework is a sound business plan that is consistent and integrated with the risk management strategy and risk appetite statement. The Reserve Bank expects that the bank's risk management framework will provide relevant information to senior management and the Board to facilitate their respective roles in the strategy and business planning process (e.g. areas of increased risk, changes in the environment, prioritisation and allocation of resources). The Reserve Bank also expects that

35 Reserve Bank will issue a separate Prudential Standard and Guidance on preparation of ICAAP.

the relevant components of the risk management framework would be reviewed in the context of the bank's strategic and business planning processes.

54. The Prudential Standard on Governance and Risk Management requires a rolling business plan of at least three years' duration that is reviewed at least annually. A rolling plan supports a medium to long-term view of business objectives, while the annual review ensures it is dynamic and updated to reflect current goals.

55. The Reserve Bank expects the bank's business plan review process would consider the impact on the risk profile of the bank's operations and identify the potential changes to the material risks. This would ordinarily include formal consideration of issues arising from planned material changes to the bank's operations and risks. It should also include a comprehensive review of the internal and external operating environment annually, before the business plan is extended for a further year.

56. The business plan must provide projections for both the revenue statement and balance sheet at a minimum. It should preferably not just be a plan for the year end, but should have monthly and quarterly targets for all major items in both the revenue statement and balance sheet. The Board and senior management should regularly review the actual to budget/plan figures during each year to determine if adequate progress against the plan is occurring. Timely action should be taken where the actual performance lags where it was planned to be on a monthly or quarterly basis, providing assumptions and circumstances have not materially changed, which may call for a changed approach to the altered environment.

Risk appetite statement

57. The risk appetite statement is used to communicate the Board's expectations of how much risk the bank is willing to accept. The Reserve Bank notes that, in practice it is likely that the risk appetite and risk appetite statement will be developed through an iterative process involving the Board and management. The Reserve Bank's view is that a reasonable and easily understood risk appetite statement that aligns to the approaches used to identify, assess and manage material risk is fundamental to risk management.

58. It is important that the Board is fully involved in the development and maintenance of the risk appetite statement and that it reflects the Board's risk tolerances[36], not managements, although management will have a considerable input into the discussions the Board has to establish its risk appetite. Once established, it is a means by which the Board conveys to management what sort of risks and the level of risks within which boundaries management

36 Various factors should be taken into account by the Board in setting risk tolerances/limits, but the capital strength must be a core consideration and the primary objective of the limits set must be to keep the bank safe and sound on an ongoing basis. The likelihood of a risk event occurring ranges from very regular or constant e.g. loan defaults, to very occasional, such as a major economic downturn, which tends to be cyclical over a period of years. A convenient way of handling risk is to use a simple matrix, comprising the severity of the impact of a risk on one scale and the frequency of occurrence on the other scale. Risks can be plotted on such a graph and grouped into risk categories e.g. happens often, low impact; happens regularly but not often, medium impact; happens rarely, high impact. Obviously risks which occur often and are of high impact on the bank need much more attention from the Board and management than risks which occur rarely and are low impact. However there is no requirement to handle risk in this way, but there must be an adequate framework established in terms of this Prudential Standard. An example of such a model is contained at Attachment B.

must operate the business(s) of the bank. The Board must therefore have 'ownership' of the risk appetite statement.

59. The articulation of risk appetite and risk tolerances is central to a risk appetite statement. Risk appetite is the degree of risk a bank is prepared to accept in the pursuit of its strategic objectives and business plan. Risk tolerances support the translation of the risk appetite by management into operational limits for the day-to-day management of material risks[37]. It may not be possible to set quantitative tolerances or limits for all risks.

60. The risk tolerances within the risk appetite statement should be expressed as a series of qualitative statements and quantitative limits and indicate to management with respect to risk "this much and no further" and the Board must make it clear it will not tolerate these limits being exceeded.[38]

61. The Board must ensure it receives reporting that allows it to monitor trend lines so that as limits are approached they can implement (through directions to management) increasingly urgent and stringent actions, depending on the rate of approach to limit(s) and how critically important the risk(s) is and how close it is getting to the limit[39].

62. The development and review of a bank's risk appetite statement will generally be performed as part of the strategic and business planning process. The risk appetite statement would provide relevant information on the Board's expectations regarding the risk appetite, and would in turn be updated to reflect any changes as a result of the strategic and business planning process. Naturally, consideration of the operating environment would form part of the business and strategic planning process[40].

63. The Reserve Bank expects that the Board would be actively engaged with management in developing and reviewing the risk appetite statement, and would be able to demonstrate ownership of the statement. The Reserve Bank considers that this might be achieved, in part, through reporting and communication processes and structures that enable the Board and/or Board Risk Committee to:

a) identify the bank's overall current risk profile and how this compares to its risk appetite and capital strength;

b) be satisfied that senior management's interpretation and application of the risk appetite and tolerances is appropriate; and

---

37 It is also good practice (but not a requirement) to identify a normal operating range for each material risk or key risk indicator. This will allow easier identification of risks which need closer monitoring when they move outside the normal operating range.

38 The Board must not tolerate breaches of its risk tolerances/limits and must, through directions to its management team, actively manage risks. To do so it must receive regular reporting which will indicate if risk tolerances/limits are being approached (which requires regular measurement of the risks). Action must be taken by the Board to avoid a risk rising to the point where it breaches a limit. The action must be commensurate in terms of severity of action and urgency with the likelihood of a risk tolerance or limit being breached.

39 See also Risk Tolerance below.

40 The risk appetite and risk tolerances should be changed when conditions change in the environment e.g. loan losses are likely to increase in the event of an economic downturn in the economy, so risk tolerances should be considered early in such a risk event, leading to changes in credit risk policies and the handling of problem loans (more intensive scrutiny). Because of this, Board's, as part of their risk responsibility, need to be examining the environment regularly in a forward looking manner and perusing data which will help them identify possible looming threats or a series of events which when combined, are likely to create a major risk event.

c) appropriately align risk appetite to the approach adopted in the risk management framework for assessing, monitoring and managing the different material risks.

64. The Reserve Bank expects a bank to communicate appropriate aspects of its risk appetite statement throughout its operations to ensure that the risk appetite statement is understood and consistently implemented. An appropriate summary of the risk appetite statement would include relevant information for the intended audience.

65. Risk appetite is a key consideration in developing policies in relation to key decision making processes. For example, when an bank develops a business case for a new product for a material risk area, the Reserve Bank expects that the risk management framework would be used to identify and assess risks, and that the risk appetite is considered in the decision making and implementation process.

66. A bank would generally use a variety of approaches and processes to assess different material risks. An bank with the capability to use risk quantification techniques would generally use them in the setting and monitoring of its risk appetite statement. Risk quantification techniques may provide an bank with assurance that the risk does not exceed the bank's risk tolerance and/or risk capacity. These techniques may not be appropriate for all types of risk. The Reserve Bank expects senior management to assess the appropriateness of such techniques before they are adopted and on an ongoing basis. The Reserve Bank expects that the results of such analysis and testing would be reported to the Board and/or Board Risk Committee and be taken into account when establishing or reviewing the risk appetite statement. The Reserve Bank expects the Board and/or Board Risk Committee to recognise the limitations and assumptions relating to any models used to measure components of risk that could materially affect its decision-making.

67. Where an international banking group operates both a subsidiary and a branch in Tonga, the Reserve Bank requires each bank to have a risk appetite statement that is tailored to its risk profile. Although risk appetite may be set by the overseas group on a divisional basis, the Reserve Bank nevertheless expects the branch risk appetite statement to appropriately address the risk profile of the Tongan branch operation.

Risk appetite

68. Risk appetite expresses the aggregate level and types of risk that a bank is willing to assume to achieve its strategic objectives and business plan before breaching its obligations or constraints determined by regulatory capital, liquidity or other needs.

69. In the Reserve Bank's experience, the risk appetite can be expressed in a number of ways to ensure that it is commonly understood and consistently applied across a bank. Generally, the risk appetite is expressed in the form of high level qualitative statements that clearly capture the bank's attitude to and level of acceptance of different risks. Where appropriate, the risk appetite statement would include quantitative limits and measures as well as qualitative ones.

Risk tolerance

70. Risk tolerances should be established for each material risk, taking into consideration the risk appetite. Risk tolerances are based on the maximum level of acceptable risk. To facilitate implementation and monitoring of the risk appetite in day-to-day business activities, a bank may also decide to set risk limits for more granular risks within each material risk.

71. Risk tolerances can be expressed in a number of different forms depending on the nature of the risk being managed. They can act as triggers for considering whether action is necessary in relation to the risk. Where possible, risk tolerance would be expressed as a measurable limit to enable a clear and transparent monitoring process that ensures the bank remains within the determined risk tolerance. An bank may also define key indicators with thresholds around the risk tolerance e.g. a 'normal' expected operating range for that risk.

72. Risk tolerances should be set which are both quantitative and qualitative. However, where possible, at least some of the measures used to articulate the risk tolerances for each key risk indicator should be quantitative measures. This allows the risk tolerances to be referenced directly into policy for each risk type and allow each risk to be more easily measured, evaluated and reported against the appetite/tolerance.

73. It is important that the key risk tolerances and reporting thereof are expressed in a quantitative way where possible e.g. for liquidity and number and percentage of delinquent loans in certain categories. This makes it clear when these important benchmarks are reaching unacceptable levels and makes monitoring simpler and easier, particularly for the Board and Board Risk Committee, whose non-executive members have limited time to consider matters compared to senior management.

74. The Reserve Bank recognises that, for some risks, a qualitative risk tolerance may be appropriate. In these circumstances, the bank would be expected to ensure the tolerance is well articulated to enable consistent implementation across the bank's operations and to determine when the risk tolerance has been exceeded.

75. Where a risk exposure falls outside the bank's risk tolerance, the Reserve Bank expects the bank would promptly develop and implement a plan of action to review the risk and ensure that it is brought within an acceptable tolerance.

Risk management strategy

76. The Prudential Standard on Governance and Risk Management requires an bank to formulate, maintain and give effect to a risk management strategy that provides an overview of how the risk management framework addresses each material risk for the bank, with reference to the relevant policies, standards and procedures.

77. The Reserve Bank expects that a risk management strategy would contain sufficient information to communicate, in general terms the bank's approach to risk management. This includes how it identifies, measures, evaluates, monitors, reports and controls or mitigates the material risks of its operations. The Prudential Standard on Governance and Risk Management requires that the risk management strategy list the policies and procedures dealing with risk management matters. Where these policies and procedures require Board

approval under other prudential standards, approval of the strategy does not negate the Board's responsibility to approve those individual documents.

Risk management function

78. A key role of a bank's risk management function is to provide independent and objective review and challenge, oversight, monitoring and reporting in relation to material risks arising from the bank's operations. An additional responsibility is to provide technical support and assist the Board, relevant committees and senior management to fulfil their respective roles in relation to the risk management framework.

79. The Reserve Bank expects the risk management function would also facilitate the building of risk management capabilities throughout the bank by providing specialist education, development program and advice to directors, senior management and staff of the bank. It would also typically facilitate the development of the Board's view of risk culture.

80. The Reserve Bank expects the roles and responsibilities of the risk management function to be clearly defined and documented as part of the risk management framework. These responsibilities include assisting with the development and maintenance of the risk management framework.

81. The Reserve Bank expects a risk management function to be appropriately structured to fulfil its roles and responsibilities. This may include co-locating risk management personnel with the business line divisions or functions that they are responsible for monitoring. For example, risk managers who focus on market risk may be assigned to a specialist market risk team that is physically located with the relevant trading/investment functions. Where risk management personnel are co-located in this way with different businesses across the bank, these personnel would be organisationally independent of the business reporting lines and remain part of the overall risk management function's reporting structure. It is important that the roles and responsibilities are clearly understood with clear reporting and escalation lines to the designated head of the risk management function, referred to as the Chief Risk Officer (CRO) (in this document) and responsible committees.

Head of risk or Chief Risk Officer

82. The Reserve Bank expects the risk management function to have sufficient stature, authority and resourcing to support sound risk-based decision-making. This is reflected in the requirement in the Prudential Standard on Governance and Risk Management that the head of the risk function must have authority to provide effective challenge to activities and decisions that may materially affect the bank's risk profile[41].

41 Ideally the head of the risk function must be independent from business lines, other revenue-generating responsibilities and the finance function. The head of risk must not be the Chief Executive Officer (CEO), Chief Financial Officer, or Head of Internal Audit. However, for smaller banks, where this is not considered feasible, the structure must seek to achieve the objectives of this Prudential Standard. The Reserve Bank may intervene and designate an alternative structure if it does not consider the structure established by a bank is not effectively achieving the objectives of this Prudential Standard. Nevertheless, the head of risk must always have a direct reporting line to the CEO, and have regular and unfettered access to the Board and the Board Risk Committee.

83. This can be further evidenced by a head of risk who is appropriately skilled, unencumbered by conflicts of interest with their risk management role and can speak with candour to the Chief Executive Officer (CEO), the Board and relevant committees. Under a three lines of defence model, the role and responsibilities of the head of risk are clearly within the second line.

84. The stature and authority of the head of risk would be supported by their being a senior executive, having an ability to influence material decisions and remuneration appropriate to their responsibilities. The Reserve Bank expects that the head of risk's authority and participation in decision-making would support risk-based considerations that are consistent with the bank's risk appetite statement, risk management strategy and business plan. It is important that the head of risk provides effective challenge as part of their participation in the decision-making process, ensuring that material decisions are risk based.

85. The Prudential Standard on Governance and Risk Management requires an bank to have a process for identifying, monitoring and managing perceived, potential and actual conflicts of interest. The Reserve Bank's requirement for a 'designated' rather than 'dedicated' head of risk provides scope for the person to have other roles and responsibilities, so long as there is no conflict of interest. There is no requirement for the person in the head of the risk function role to be called a Chief Risk Officer (CRO), but in larger banks this may be appropriate to the status and rank of the head of risk. Whatever the position is called and whether the person occupying the head of risk has other responsibilities apart from risk, it is important that the head of the risk function be at the same level as other executives reporting to the CEO, so that effective challenge can occur at the most senior management level – see previous paragraph.

86. The Prudential Standard on Governance and Risk Management sets out requirements for the independence of the head of risk and specifies roles that cannot also be performed by the head of risk. The Prudential Standard on Governance and Risk Management recognises that an bank may seek approval for alternative arrangements to those required in the Prudential Standard. This may be where the bank is materially constrained in appointing a head of risk (CRO) who is free from conflicts of interest, or for other reasons particular to that bank. The Reserve Bank expects these instances normally to be limited to smaller and less complex banks, but will consider applications from all banks, provided the applicant clearly sets out the exceptional circumstances that might warrant the Reserve Bank considering the alternative proposal. Where an bank seeks an alternative arrangement under the Prudential Standard on Governance and Risk Management, the Board is expected to demonstrate to the Reserve Bank that it has undertaken a process to identify conflicts, has established structural oversight and controls to mitigate the additional risk and is satisfied that the risk management framework will ensure these mitigants are adhered to. The Reserve Bank will assess the appropriateness of alternative arrangements on a case-by-case basis. The Reserve Bank expects that the Board would take into account the following controls and other mitigating factors that manage conflicts of interests including, but not limited to:

a) alternative sources of risk-based challenge to business lines;

b) the resources allocated to risk management;

c) executive level engagement in risk issues;

d) the strength of compliance and audit mechanisms;

e) oversight from the Board and its committees;

f) the experience and capabilities of the other risk management function personnel; and

g) the robustness of the regulated bank's and, where appropriate, the group's risk management framework.

87. The Prudential Standard on Governance and Risk Management requires that the risk management function, (via a CRO), has direct and unfettered access to the CEO, Board, Board Risk Committee and senior management. The Prudential Standard on Governance and Risk Management also requires the reporting line for the risk management function to be independent from business lines and to directly report to the CEO. Where a bank is part of a group, the head of risk of that bank may report to the group CRO as long as the group CRO reports directly to the group CEO.

88. The Prudential Standard on Governance and Risk Management recognises that a Tongan branch operation may seek an alternative arrangement for the requirement that the head of risk to report to the CEO. A Tongan branch operation can use a regional or global CRO who assumes the risk responsibilities for the branch. Due to their regional or global reporting lines, it may be impractical to require the CRO to report to the Tongan branch's Branch Manager. Where this is the case, the Reserve Bank expects that the designated CRO has sufficient oversight of, and involvement with, the management of risk in the branch. The Reserve Bank expects the branch would be able to demonstrate that the CRO can fulfil his or her roles and responsibilities to the Tongan bank, evidenced by regular and unfettered access to the Tongan branch Senior Overseas Officer (i.e. located outside Tonga) or Compliance Committee.

89. For the avoidance of doubt, the Prudential Standard on Governance and Risk Management does not require the designated head of the risk management function to be called a CRO.

Compliance function

90. The Prudential Standard on Governance and Risk Management requires a designated compliance function to have a reporting line independent from business lines to support clear and timely reporting of compliance risks.

91. The Reserve Bank envisages that for smaller and less complex banks, the head of risk would be able to provide this independent reporting line and that they may have responsibility for the compliance function. Where a head of risk is also the head of the compliance function, he or she is expected to effectively fulfil the responsibilities for each function. In the situation where there is one person heading both risk and compliance, the bank needs to consider alternative arrangements for ensuring the risk function is complaint with its responsibilities and that the compliance function is adequately identifying, monitoring, measuring and managing risks.

92. The structure of the compliance function is a matter for the regulated bank. Where an bank combines its risk and compliance functions, the Reserve Bank expects that the bank would allocate sufficient resourcing to fulfil the roles and responsibilities of each function.

Outsourcing

93. The Reserve Bank does not expect that outsourcing the risk management and/or compliance functions would be a common practice. Where a bank considers there is adequate justification, this is considered to be a material business activity for the purposes of the outsourcing section of the Prudential Standard on Operational Risk.

Monitoring and reporting Oversight and escalation processes

94. The Reserve Bank expects a bank's risk management framework to ensure that the Board and senior management receive regular, concise and meaningful assessment of actual risks relative to the bank's risk appetite and the operation and effectiveness of controls.

95. A bank's formal escalation procedures would ordinarily cover reporting of exceptions to risk appetite, risk tolerances and more granular risk limits. This reporting would include sufficient commentary to facilitate management review and understanding of the report content, where necessary.

96. An example of a relatively simple model for measuring risk and standardising the measurement of risk within the overall banks risk profile, is contained at **Attachment B**. This example provides for the level of different risks to be compared so that different risks can be prioritised and receive more Board and senior management focus, particularly with respect to monitoring and managing and mitigating those risks that are determined to be higher priority at any particular time.

Information systems for business reporting

97. The Reserve Bank expects that a bank would, as part of its risk management framework, establish, maintain and document effective Management Information Systems (MIS) commensurate with the size, business mix and complexity of its operations.

98. Effective MIS provide appropriate information at each level of management and decision making within the bank. Such information systems assists in the management, communication and reporting of risk issues and outcomes and assist the management of the bank to appropriately monitor and manage different material risks. The MIS would be sufficiently flexible to support decision-making during periods of stress, when the bank's risk profile may significantly change.

99. The Reserve Bank envisages that a bank would implement controls for ensuring data in information and reporting systems is sufficiently current, accurate and complete such that data quality is adequate for timely and accurate analysis and reporting of risk. Internal information and reporting systems would be secure and supported by adequate business continuity and disaster recovery arrangements.

100. An bank is expected to maintain adequate data security, including the maintenance of a back-up copy of all customer and general ledger files and transactions, on at least a daily basis. These back-up copies are vital in the event of a major loss of data, which might occur through fire or other hazard. The back-up copies must be kept in a secure location remote from the main data facility.

101. A well-functioning information and reporting system would typically:

a) produce appropriate risk and compliance data and reports;

b) incorporate information that is relevant to decision-making;

c) report accurate, reliable and timely information;

d) allow the bank to identify, assess and monitor business activities, existing and emerging risks, financial position and performance;

e) allow the bank to monitor the effectiveness of, and compliance with, its internal control systems and report any exceptions that arise; and

f) be reviewed regularly to assess the timeliness and relevance of information generated and the adequacy, quality and accuracy of the system's performance over time.

Annual declaration regarding risk management

102. The Prudential Standard on Governance and Risk Management requires a bank to provide the Reserve Bank with an annual declaration regarding its risk management framework.

103. The Prudential Standard on Governance and Risk Management requires the risk management declaration to be submitted to the Reserve Bank within three (3) months of an bank's annual balance date.

104. The Prudential Standard on Governance and Risk Management does not prohibit a bank's risk management declaration being encompassed in the risk management declaration documentation of a group, where applicable. Where a bank's declaration is encompassed within the group declaration, the bank's Board remains responsible for any qualifications in the declaration that relate to that bank. Where a risk management declaration is made on a group basis, the Prudential Standard on Governance and Risk Management requires any qualification to identify whether it related to the bank or the group's risk management framework. A qualification for the bank may not mean that a group wide qualification needs to be made, and vice versa. However, where a group's Board has taken the decision that a qualification at the bank level does not result in a group declaration qualification, the reason for this decision would be articulated.

105. Where a bank's declaration regarding the risk management framework is encompassed within the group declaration, the combined declaration can be submitted to the

Reserve Bank at the time the risk management declaration of the Head of the Group, in an overseas jurisdiction, is required to be submitted.

106. While this annual declaration regarding the risk management framework does not have to be audited, the Reserve Bank expects that the Board would have obtained reasonable assurance and, if necessary, considered independent advice on the matters covered by the declaration, prior to the signing of the declaration by the required signatories. The extent of enquiry required prior to making the declaration is a matter for the judgment of each Board of a bank. The wording of the declaration allows materiality to be taken into account when making the declaration.

107. Before submission of this declaration and notification, the Reserve Bank expects an bank to conduct an annual review to establish compliance with, and effectiveness of, the risk management framework (and identify breaches). The Reserve Bank considers it would also be appropriate for an bank to include in the annual review consideration and assessment of the suitability and adequacy of the risk management framework, which also needs to be considered regularly.

108. While the declaration must be signed by various parties, the annual review should, where possible, be conducted by the third line of defence (internal and/or possibly external audit), to gain maximum objectivity from the first and second lines of defence. However, given the depth of the extent and depth of the review, the Reserve Bank will accept the third line of defence can carry out the review as a part of its rolling audit plan, so that different aspects of the risk management framework are covered over a year. A bank can decide how it wants to approach the review, to provide itself with the maximum benefit and assurance.

109. This review must be reported to the Board Audit Committee or, in the case of a foreign bank to the Senior Overseas Officer (i.e. outside of Tonga) or the Compliance Committee.

110. The Reserve Bank will accept annual reviews that explore particular elements of the risk management framework in depth and on a rotational basis. For example, if an bank's risk management framework has six material elements, it may choose to review two of these every year. The structure of such a program of review is at the discretion of the regulated bank. The annual review sign-off would include those reviews conducted during the year since the previous such sign-off. The Reserve Bank expects that all elements of the risk management framework would be subject to review at least every three years.

111. The Reserve Bank envisages that some branch operations would be subject to group internal audits of compliance with, and effectiveness of, its risk management framework. The Reserve Bank may approve alternative timing to this annual review, such as on a biennial basis if satisfied that those arrangements will, in the Reserve Bank's view, achieve the objectives of this requirement. The Reserve Bank will assess the appropriateness of alternative arrangements on a case-by-case basis with considerations including, but not limited to, the:

a) size, business mix and complexity of the branch operations;

b) process the Senior Overseas Officer or a Board Committee has undertaken to satisfy themselves that an alternate timing of review is appropriate;

c) additional controls in place to mitigate the risk of non-compliance in interim years; and

d) robustness of the branch operations and, where appropriate, the robustness of the group's risk management framework.

112. Subparagraph (f) of the risk management declaration in the Prudential Standard on Governance and Risk Management includes the statement that "the bank is satisfied with the effectiveness and reliability of the processes and systems surrounding the production of financial information at the bank" (and group where appropriate). The Reserve Bank's expectation is that the term 'financial information' in this part of the declaration would be read broadly and capture more than information related to the financial statements. For example, prudential returns, disclosures and other similar documents/information would ordinarily also be considered for the purposes of the declaration.

Reserve Bank notification requirements

113. The Prudential Standard on Governance and Risk Management requires a bank to notify the Reserve Bank of material changes to the size, business mix and complexity of the bank's business operations. The Reserve Bank expects that this would include, but not be limited to, the following changes, where material:

a) events such as proposals relating to major modifications to, or the re-organisation of, the functions of the bank;

b) proposed acquisitions;

c) changes to business lines and products;

d) changes in organisational structure; and

e) deviations from the risk management strategy.

114. The Prudential Standard on Governance and Risk Management requires a bank that conducts business outside of Tonga to notify the Reserve Bank when it becomes aware that its right to conduct business in any other jurisdiction has been materially affected. A restriction on the ability of an bank to conduct business overseas could impact on its Tongan operations, and may have resulted from weaknesses in risk management. The Reserve Bank expects to be informed, at a minimum, when the bank's right to conduct business has:

a) ceased in a jurisdiction;

b) been limited by a law of any jurisdiction in which business is being conducted;

c) been otherwise materially affected under a law of any jurisdiction in which business is being conducted; or

d) otherwise been withdrawn; and where applicable, changes to the ability of a group member to conduct business that materially impacts on the Tongan operation's risk profile.

115. The Reserve Bank expects that a bank would be in regular dialogue with its supervisors about potential material changes to the bank. The Reserve Bank expects that, at the latest, notification in accordance with the requirements in the Prudential Standard on Governance and Risk Management would be made within 10 business days of the Board becoming aware of a current or proposed material change to the bank's risk profile or business operations.

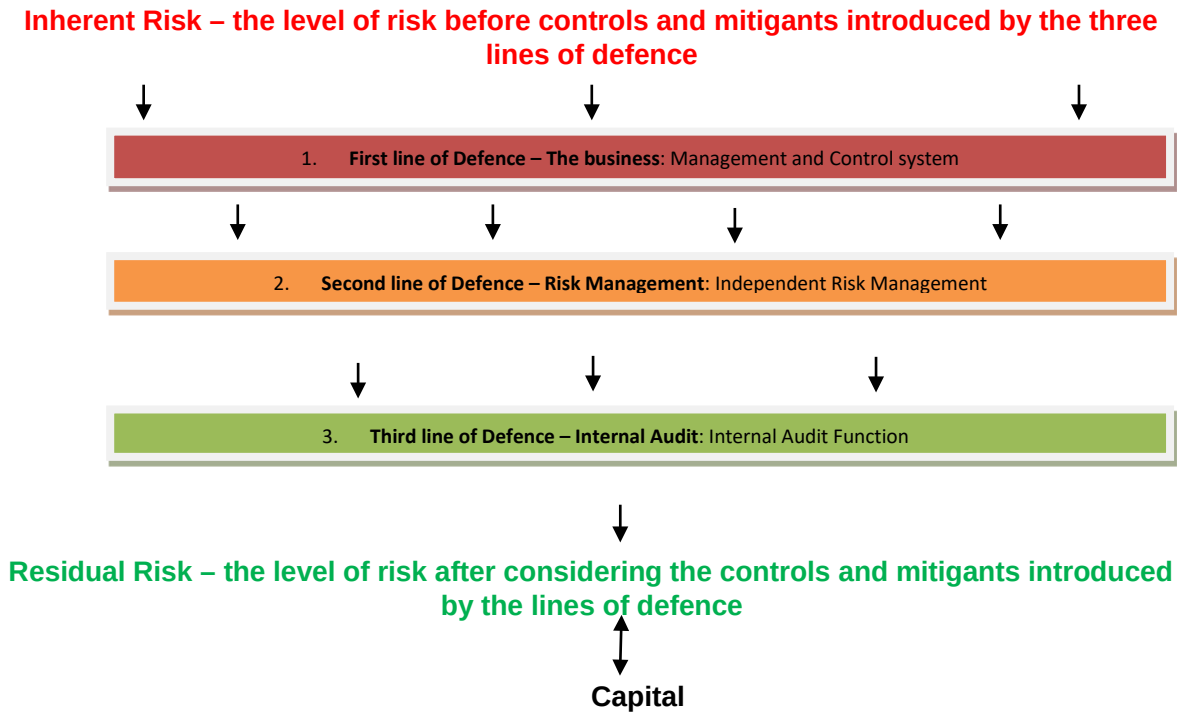
National Reserve Bank of Tonga

Attachment A

A Diagrammatic Representation of the three Lines of Defence Risk Governance Model

The systems and elements which comprise the RMF will always be completely integrated into a banks function/business. The RMF is considered fundamental to achieving a banks longer term viability and success and hence it should always have the strongest support from the Board and senior management.

A suitable RMF involves a three lines of defence (3LoD) model that is commensurate with its size, business mix and complexity. This 3LoD Model is described diagrammatically below:



Lines of Defence

The three lines of defence model refers to the broad responsibilities for risk management within a bank, as follows:

First Line of Defence – Within a bank, the business unit(s) hold primary responsibility for the risks it faces. Risk is managed in each business/market segment unit firstly by identification of the inherent risks it creates through its business activities, then by measurement and assessment of these risks and finally by considering the impact of a range of risk management controls and risk mitigation treatments at the business unit level. The business unit must then monitor the risks on an ongoing basis. To briefly outline the business unit responsibilities within the 3LoD model, it:

- implements, continually enhances and maintains the risk management framework including:
    - Identification, monitoring, measurement and effective management/mitigation of risks; and
    - Identifies, records, escalates and manages risk issues.
- Will include management committees, delegated authorities etc.

Second Line of Defence – The Risk Management function independently ensures risks are being appropriately identified, analysed, evaluated, treated, monitored and reported. A major focus of the Risk Management division is to ensure that the first line of defence is adequate. To briefly outline the risk management unit responsibilities within the 3LoD model, it:

- provides independent oversight of the banks risk profile and risk management framework, including:
    - effective challenge to the activities and decisions that materially affect the banks risk profile;
    - assistance in developing, continually enhancing and maintaining the risk management framework; and
    - independent reporting lines to appropriately escalate issues.

Third Line of Defence - Internal Audit is responsible for identifying risk management problems, such as inadequately identified, measured, monitored or managed credit risks that have not been picked up. Internal Audit are responsible for auditing the risk management function and the business to identify problem areas. To briefly outline the internal audit unit responsibilities within the 3LoD model, it:

- on a progressive basis, but at least annually, provides another level of independent assurance through audit processes that the risk management framework has been complied with in all business areas and is operating effectively;

Residual Risk

Residual risks are the risks or risk levels that still remain after considering the risk controls and mitigation undertaken by the three lines of defence. A bank does not seek to eliminate residual risk completely as it recognises that:

- it is usually considered uneconomic to try and eliminate all risk;
- acceptance of risk is what generates return and profit for a bank through an appropriate risk/return trade-off. However to achieve the right risk/return balance, it is imperative that a bank understands all of its risk(s), has measured the level of risk and is controlling and managing these risks appropriately. A bank does not accept open ended risks;
- a bank through the Board must have a documented risk appetite/tolerance which means a certain level of residual risk is accepted, but risk limits are established which represent the absolute boundaries within which management must operate the business.

Capital

The level and quality of capital must be commensurate with the residual risk faced by a bank.

Attachment B

A Possible Model for Measuring Risk

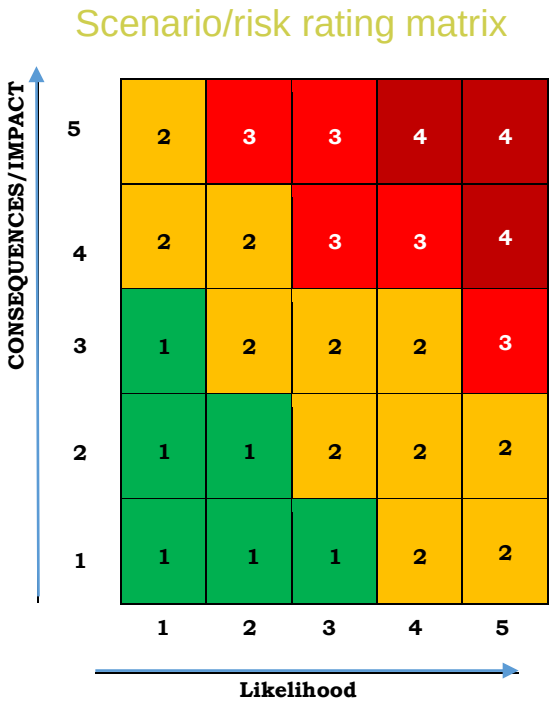
A bank can use any model for measuring risk which is effective, the Reserve Bank does not stipulate the way in which a bank measures risk. However, Prudential Banking Standard No. 9: Governance and Risk Management does stipulate that risks must be measured.

The following example is provided as one relatively simple model that banks internationally have used as a means of standardising the measurement of risk, so that risks can be measured against each other. This allows higher or more threatening risks to be prioritised.

In this example of the measurement of risk, the risk management framework uses ***consequence*** and ***likelihood*** parameters to be applied to assess the level of risk in each of the risk categories in the framework. Each risk, but as a minimum, those in the Risk Appetite statement, should be assessed firstly in terms of the impact or consequences on the bank if the risk occurs. Secondly, each risk is then assessed in terms of its likelihood of the risk occurring. These assessments and measurement of risk are on a scale of 1 to 5, with 1 being the lowest and 5 being the highest.

Obviously a risk that will have a high impact on a bank and happens frequently, or is expected to happen frequently because of changes to the operating environment, are risks the Board and senior management need to focus heavily on monitoring (i.e. good reporting) and mitigating. This risk assessment needs to be conducted reasonably frequently because the internal and external environment faced by a bank does change over time. In periods of rapid change the Board needs to ensure the frequency of risk assessment and measurement keeps up to date with the changing risk profile of the bank.

This is diagrammatically represented in the following risk assessment table, which establishes risk ratings. The tolerance definitions are mapped to the risk rating schedule as follows:



Note that in the numbering system in the above table to prioritise risks, 1 refers to a low likelihood and low/little consequence, while a 4 refers to a high likelihood and high/serious consequence. This is sometimes called a risk "heat" map, which reflects a traffic light situation. Green is akin to go, amber means a warning or transition and caution must be exercised and be prepared to stop, while red means stop or a 'no-go' zone. The further more extreme risks in the colour crimson zone, means high danger and a risk or combination of risks which has the potential to bring the bank into an area where it cannot be considered safe and sound.

The description of the Impact and Likelihood rating criteria scales are contained below under the heading 'Examples of Risk & Control Rating Criteria'. These are just suggestions for banks to work on and develop. Each material risk within the Risk Appetite statement will contain a number of quantitative and qualitative measures which will determine where risk tolerances are established, and preferably identify the green zone boundaries for each material risk, the boundaries for amber and where the red zone or risk tolerance or risk limit is established. Once this is done the various risks can be mapped on the above matrix which then provides a good visual reference for where risk priorities are to be placed (i.e. which material or other risks require more attention from time to time). The Board and senior management then need regular reporting so they can monitor where risk levels are relative to their pre-established Risk Appetite and change attention or implement mitigation and management strategies as necessary.

The risk rating levels for the above table and the risk tolerance levels that correspond to these risk levels are shown in the following table[42]:

42 Note that these are residual risk levels. In other words it is the inherent risk after application by a bank of management and controls within its risk management framework.

	Risk rating level*	Risk Tolerance level	(Example of) Description
4	**Level 4 – Extreme** (The risk will have a very significant impact on the bank's earnings and capital within twelve months)	**'Very low : no tolerance/** level **Zero**	The bank has no appetite for this risk and will do everything in our power to avoid it and will proactively seek to eliminate it.
3	**Level 3 – High** minimise (The risk will have a material impact on the bank's earnings and capital within the foreseeable future)	**'Low : outside risk tolerance'**	The bank will proactively seek to this risk exposure level, however we recognise that a small element of this risk level may at times be approached and will need to be managed down in achieving our business objectives.
2	**Level 2 – Medium** (The risk will have a moderate negative Impact on the bank's earnings and capital)	**'Moderate : within tolerance, \but close to outside tolerance'**	The bank acknowledge that this is a risk level which will may be incurred as part of our business as usual objectives, but we will endeavour to manage it down into the green zone.
1	**Level 1 - Low** (The risk is unlikely to negatively influence the bank's earnings and capital to any noticeable extent in the foreseeable future)	**'High : within risk tolerance'**	The bank sees this risk level as a necessary component of our business strategy and will actively pursue this risk within our risk profile. This will be done with regard to balancing risk against return as part of our overall risk philosophy.

(***** The risk rating level will be identified using the scenario/risk rating matrix above)

Examples of Risk & Control Rating Criteria

Consequence or Impact is determined through creation of the following criteria:

Impact Category	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Extreme
Financial	Insignificant financial impact (≤ $10,000)	Minor financial impact ($10,000 to 100,000)	Moderate financial impact ($100,000 to $250,000)	Major financial impact ($250,000 to $2 million)	Extreme financial impact (≥ $2 million)
Regulatory	No impact (Policy and internal use)	Little impact (Policy and internal use)	Non-material remediation required / Routine Regulator notification	Regulator investigation / Enforceable undertakings	Formal undertaking (strict liability / licence conditions) / fine
Reputation	No publicity	Minor short term damage	Limited adverse media attention and/or some short term damage and/or complaints to industry complaints body	Local adverse media attention and/or substantial short to medium term damage	Local adverse media attention and/or substantial medium to long term damage
Customer	Insignificant impact / small scale (to part of customer base, channel, region, portfolio)	Minimal impact / small scale (to part of customer base, channel, region, portfolio)	Moderate impact / small scale (to part of customer base, channel, region, portfolio)	Moderate impact and scale (some part of customer base, channel, region, portfolio)	Significant impact (to most customers in one channel, region, portfolio)
Employees	Insignificant impact to our staff	Minimal impact to our staff	Some impact to our staff in more than one team within one line of business	Some impact to our staff in more than one line of business	Loss of key specialists / team(s) or significant adverse impact to our staff in more than one line of business

Likelihood is determined through consideration of the following criteria:

Likelihood		
Level	**Scale**	**Description**
5	Almost certain	The event is expected to occur in most circumstances. • Greater than 90% chance of occurring. This means it occurs greater than 52 times in a year i.e. it is at least a weekly event.
4	Likely	The event will probably occur in most circumstances. • Greater than 75-90% chance of occurring. This means it occurs between 12 and 52 times in a year.
3	Possible	The event may occur in most circumstances. • Greater than 25-75% chance of occurring. This means it occurs between once and 12 times in a year.
2	Unlikely	The event could occur in some circumstances. • Greater than 10-25% chance of occurring. This means it occurs between once and 10 times in 10 years. (should the upper end be 2.5 times in 10 years
1	Rare	The event may occur but only in exceptional circumstances. • Less than 10% chance of occurring. This means it occurs less than once in 10 years.