



PRUDENTIAL SUPERVISION OF THE COMMERCIAL BANKS

CBS

PRUDENTIAL STATEMENTS

Prudential Statement 1

Governance and Risk Management



Objectives and key requirements of this Prudential Statement

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

That each locally incorporated financial institution must establish and implement an in-house Corporate Governance and Risk Management Policy approved by the Board.

Foreign subsidiary operations may adapt Group Policy but must consider the size, nature and scope of local operation and must include the requirements of this Policy.



Contents

Authority.....	4
Application.....	4
Definitions	4
Ownership/Shareholding Structure	4
Role of Board of Directors	5
Role of the Senior Management.....	7
Board Audit Committee.....	8
Strategic and Business Planning	9
Risk Management Framework.....	10
Internal Audit	13
Fit and Proper.....	13
Attachment A	17
Attachment B	18

Authority

This Prudential Statement is made under Section 3 (2), of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act 1996.

This Prudential Statement sets out the minimum requirements that a Financial Institution must meet in promoting effective governance and risk management.

Definitions

Financial Institution ó bank entity licensed under the Financial Institutions Act 1996.

Non-executive Director - a director who is not a member of management of the Financial Institution.

Independent Director - a non-executive director who is free from any business or other association ó including those arising out of a substantial shareholding, involvement in past management or as a supplier, customer or adviser ó that could materially interfere with the exercise of their independent judgement.

Shareholder ó a person who owns or who has authority to exercise power over ten percent (10%) or more of the Financial Institution's voting stock.

Corporate Governance ó the oversight mechanisms, including the processes, structures and information used for directing and overseeing the management of a company.

Risk Management Framework - systems, structures, policies, processes and people within a Financial Institution that identify, measure, monitor and control material risk.

Material Risks - risk that could have a material impact, both financial and nonfinancial, on the institution or on the interests of depositor.

Ownership/Shareholding Structure

1. The Bank has taken the view that no single shareholder (or group of associated shareholders) of a bank should be in a position to exercise control or influence over the policies or operations of a bank.
2. Banks usually have a very high gearing of outside creditors (mostly depositors) to shareholders funds. This is an essential feature of banking and requires that depositors have confidence in banks.

3. It is in the best interest of depositors for a bank to have a broad range of its shareholders (represented by directors) involved in the formulation and implementation of the bank's policies and operations.
4. The likelihood of banks getting in to difficulties stemming from major errors in judgement, imprudence, dishonesty or other possible irregularities are less likely to occur if decisions are made collectively.
5. The Bank expect that no person (or group of associated persons), whether local or foreign, may own more than twenty percent (20%) of the voting shares of a bank.
6. Any transfer of shares that may result in a single shareholder (or group of associated shareholders) owning or exercising power over twenty percent (20%) of the voting stock of a bank shall require the prior approval of the Central Bank.

Role of Board of Directors

7. The Board of Directors of a Financial Institution (the Board) is ultimately responsible for the sound and prudent governance and risk management of the institution.
8. The Board must have a formal charter that sets out the roles and responsibilities of the Board.
9. 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.
10. The Board must ensure that directors and senior management of the Financial Institution, collectively, have the full range of skills needed for the effective and prudent operation of the Financial Institution, and that each director has skills that allow them to make an effective contribution to Board deliberations and processes. This includes the requirement for directors to have the necessary skills, knowledge and experience to understand the risks of the Financial Institution, including its legal and prudential obligations, and to ensure that the Financial Institution is managed in a way that takes into account these risks. This does not preclude the Board from supplementing its skills and knowledge through the use of external consultants and experts.
11. Members of the Board must be available to meet with the CBS on request.
12. The Financial Institution must provide the external auditor of the Financial Institution with the opportunity to raise matters directly with the Board.

Board Composition

13. The Board of a Financial Institution must have a minimum of five directors.

14. The Board must have a majority of independent directors¹.
15. The chairperson of the Board must be an independent director of the Financial Institution.
16. A majority of directors present and eligible to vote at all Board meetings must be non-executives.
17. The chairperson of the Board cannot have been the Chief Executive Officer (CEO) of the regulated institution at any time during the previous three years. If the position of the CEO is unexpectedly vacated, the chairperson may serve as an interim CEO. After a period of 90 days, approval must be sought from the CBS to allow this arrangement to continue.
18. The Board must be available to meet with the CBS on request, collectively and individually at the discretion of the CBS.
19. For locally-owned and incorporated Financial Institutions, a majority of directors must be ordinarily resident in Samoa.
20. For foreign-owned locally incorporated Financial Institutions, at least two of the directors must be ordinarily resident in Samoa, at least one of whom must also be independent.
21. For a Financial Institution that is a subsidiary of another CBS-regulated institution or an overseas equivalent², the Board must have a majority of non-executive directors, but these non-executive directors need not all be independent. They can include Board members or senior management of the parent company or its subsidiaries, but not executives of the regulated institution or its subsidiaries.
22. A Financial Institution to which paragraph 15 applies will be required to have, at a minimum, two independent directors, in addition to an independent chairperson, where the Board has up to seven members. Where the Board has more than seven members, the Financial Institution will be required to have at least three independent directors, in addition to an independent chairperson.
23. For the purposes of meeting the requirements in paragraph 17, the independent directors on the Board of the parent company or its other subsidiaries can also sit as independent directors on the Board of the regulated institution.

¹ If the Board is in doubt regarding a director's independence, the Financial Institution may refer the matter to the CBS for guidance. *See Attachment A*

² An "overseas equivalent" is one which is not licensed in Samoa but is authorized and subject to prudential regulation in a foreign country

Regulated Institutions that are Part of a Corporate Group

24. Where a Financial Institution is part of a corporate group and the regulated institution utilizes group policies or functions, the Board must ensure that these policies and functions give appropriate regard to the Financial Institution's business and its specific requirements.

Board Performance Assessment and Renewal

25. The Board must have procedures for assessing, at least annually, its performance relative to its objectives. It must also have in place a procedure for assessing, at least annually, the performance of individual directors.
26. 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.

Role of the Senior Management

27. The Board is accountable to the Central Bank while the Senior Management is accountable to the Board;
28. Senior Management is responsible for directing and overseeing the effective management of the institution's operations;
29. Senior Management is responsible for developing the in-house Corporate Governance and Risk Management Policy for Board approval and the implementation of the Policy;

Key Responsibilities of Senior Management include but is not limited to:

30. Developing the business objectives, strategies, plans, organisational structure and controls and policies for Board approval;
31. Implementing and monitoring the Board-approved business objectives, strategies, plans, organisational structure and controls, and policies;
32. Promoting the safety and soundness of the financial institution by ensuring compliance with the applicable laws;
33. Undertake the necessary due diligence in appointing the employees; and
34. Ensuring that employees have the appropriate level of training and a training development framework.

Persons not to be constrained from providing information to the CBS

35. The Board and senior management of a Financial Institution must establish and maintain policies and procedures to ensure that no current or former officer, employee or contractor

(including professional service provider) of a Financial Institution is constrained or impeded, whether by confidentiality clauses or other means, from disclosing information to the CBS, that may be relevant to the prudential supervision of the Financial Institution.

36. The Board and senior management of a Financial Institution 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 Financial Institution.
37. Financial Institution 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 CBS.

Board Audit Committee

38. A Financial Institution must have a Board Audit Committee, which assists the Board by providing an objective non-executive review of the effectiveness of the Financial Institution's financial reporting and risk management framework unless, with respect to risk management, there is another Board Committee which carries out this function. The Board Audit Committee must have sufficient powers to enable it to obtain all information necessary for the performance of its functions.
39. The Board Audit Committee must have at least three members. All members of the Committee must be non-executive directors of the Financial Institution. A majority of the members of the Committee must be independent.
40. The chairperson of the Board Audit Committee must be an independent director of the Financial Institution.
41. The chairperson of the Board can sit on the Board Audit Committee, but cannot chair the Committee.
42. The Board Audit Committee must have a charter that includes a reference to the Committee's responsibility for the oversight of the CBS prudential reporting requirements, as well as other financial reporting requirements, professional accounting requirements, internal and external audit, and the appointment of the Financial Institution's external auditor.
43. The Board Audit Committee must review the external auditor's engagement at least annually, including assessing whether the auditor meets the Audit Independence tests set out in International Standard on Auditing (ISA).
44. The Board Audit Committee must regularly review the internal and external audit plans, ensuring that they cover all material risks and financial reporting requirements of the Financial Institution.
45. The Board Audit Committee must hold management to account for process and risk management deficiencies identified in the work of both the internal and external audits. As

such, the Committee must have in place a system to track and respond to audit deficiencies and ensure timely corrective action is taken by management.

46. The Board Audit Committee must ensure the adequacy and independence of both the internal and external audit functions.
47. The members of the Board Audit Committee must, at all times, have free and unfettered access to senior management, the internal auditor, the heads of all risk management functions and the Financial Institution's external auditor, and vice versa.
48. The Board Audit Committee must establish and maintain policies and procedures for employees of the Financial Institution 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.
49. Members of the Board Audit Committee must be available to meet with the CBS on request.
50. The Board Audit Committee must invite the regulated institution's external auditor to meetings of the Committee.
51. The internal auditor must have a direct reporting line and unfettered access to the Board Audit Committee.

Strategic and Business Planning

52. The Board and senior management must develop a strategic plan for the Financial Institution, 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.
53. The Board 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.
54. A Financial Institution 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.
55. A Financial Institution must identify and consider the material risks associated with its strategic objectives and business plan, and must explicitly manage these risks through the risk management framework, including how changing these plans affects its risk profile.

Risk Management Framework

56. A Financial Institution must maintain a risk management framework that enables it to appropriately develop and implement strategies, policies, procedures and controls to effectively manage its risks. The Financial Institution must have policies and procedures that provide the Board with a comprehensive institution-wide view of its material risks.
57. A Financial Institution'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.
58. A Financial Institution 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 other relevant committee.
59. A Financial Institution's risk management framework must, at a minimum, include:
- a) risk appetite statement;
 - b) 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 institution;
 - d) a management information system that adequately measures and reports on all material risks;
 - e) risk management function;
 - f) a review process to ensure that the risk management framework is effective in identifying, measuring, monitoring and controlling material risks.
60. A Financial Institution's management information system must provide the Board and senior management with regular, accurate and timely information in relation to the institution's profile, and how the profile is within the risk appetite.
61. A Financial Institution'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.

Risk Appetite Statement

62. A Financial Institution 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. For foreign owned institutions, appropriate senior management can set the risk appetite statement and this must be approved by the board.

63. A Financial Institution's risk appetite statement must, at a minimum, convey:
- a) level of aggregate risk that the Board is willing to assume and manage in the pursuit of the institution'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 limit;
 - c) the process for monitoring compliance with each risk limit and for taking appropriate action in the event that it is breached; and
 - d) the timing and process for review of the risk appetite.

Risk Management Strategy

64. A Financial Institution must maintain a risk management strategy (RMS) that addresses its key risks. The RMS must be approved by the Board.
65. At a minimum, an RMS must:
- a) describe each of the Financial Institution's key risks 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 institution have awareness of the risk management framework and for instilling an appropriate risk culture across the Financial Institution.

Risk Management Function

66. A Financial Institution 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 institution;
 - 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 staff who have clearly defined roles and responsibilities and who possess appropriate experience and qualifications to exercise those responsibilities;
 - e) has access to all aspects of the institution that have the potential to generate material risk, including information technology systems and systems development resources; and

- f) is required to notify the Board of any significant breach of, or material deviation from, the risk management framework.
67. A Financial Institution may engage the services of an external service provider to perform part of the risk management function where the institution can demonstrate to the CBS that the risk management function meets the requirements in paragraph 53.
68. Outsourcing any part of the risk management function by a Financial Institution must also meet the requirements of *Prudential Statement – Outsourcing*.

Compliance Function

69. A Financial Institution must have a designated compliance function that assists senior management in effectively managing compliance risks.
70. 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.

Risk Management Declaration

71. The Board must make an annual risk management framework declaration to the CBS within 90 days of the institution's balance date, stating that, to the best of its knowledge and having made appropriate enquiries:
- a) the Financial Institution has in place systems for ensuring compliance with all prudential requirements;
 - b) the risk management framework is appropriate for the size and complexity of the Financial Institution; and
 - c) the internal control systems in place are operating effectively.

The declaration must be signed by the chairperson of the Board and the chairperson of the board risk committee or audit committee.

72. The Board 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.
73. A Financial Institution must submit to the CBS a copy of its risk appetite statement and RMS, no more than 10 business days after Board approval, both upon initial adoption and for any material changes.
74. A Financial Institution must notify the CBS as soon as practicable, and no more than 10 business days, 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.

Internal Audit

75. A Financial Institution must have an operationally independent and adequately resourced internal audit function.
76. The objectives of the internal audit function must include evaluation of the adequacy and effectiveness of the financial and risk management framework of the Financial Institution.
77. To fulfil its functions, the internal auditor must, at all times, have unfettered access to all the Financial Institution's business lines and support functions.
78. A Financial Institution must ensure that the scope of internal audit includes a review of the policies, processes and controls put in place by management to ensure compliance with the CBS's prudential requirements.

Fit and Proper

79. A Financial Institution must have a written policy relating to the fitness and propriety of its responsible persons.
80. The Fit and Proper Policy must be approved by the Board.
81. A Financial Institution must take all reasonable steps to ensure that each of its responsible persons is aware of, and understands, the provisions of its Fit and Proper Policy.

Responsible Persons

82. A responsible person of a Financial Institution is:
 - a) a director of the Financial Institution;
 - b) a senior manager of the Financial Institution; or
 - c) an auditor of the Financial Institution.
83. The CBS may determine that any person is a responsible person if the CBS is satisfied that the person plays a significant role in the management or control of the Financial Institution, or that the person's activities may materially impact on prudential matters.
84. The CBS may determine that a person is not a responsible person in relation to a position, responsibility or activity if the CBS is satisfied that the person does not play a significant role in the management or control of the regulated institution or that the person's activities may not materially impact on prudential matters.

Senior Managers

85. Senior manager in relation to a Financial Institution means a person (other than a director of that Financial Institution) who:

- a) makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of the Financial Institution; or
- b) has the capacity to affect significantly the Financial Institution's financial standing; or
- c) may materially affect the whole, or a substantial part, of the business of the Financial Institution or its financial standing through their responsibility for:
 - (i) enforcing policies and implementing strategies approved by the Board of the Financial Institution; or
 - (ii) the development and implementation of systems that identify, assess, manage or monitor risks in relation to the business of the Financial Institution; or
 - (iii) monitoring the appropriateness, adequacy and effectiveness of risk management systems.

Criteria to Determine if a Responsible Person is Fit and Proper

86. Each Financial Institution must clearly document the competencies required for each responsible person position, such as, but not limited to:
- a) good character i.e. honesty, integrity, fairness and reputation;
 - b) competence, diligence, capability, soundness of judgment; and
 - c) financial soundness³.

Process for Assessment of Fitness and Propriety

87. The Fit and Proper Policy must include the process for fit and proper assessment. The processes must include:
- a) who will conduct fit and proper assessments on behalf of the Financial Institution;
 - b) what information will be obtained and how it will be obtained;
 - c) the matters that will be considered before determining if a person is fit and proper for a responsible person position; and
 - d) the decision-making processes that will be followed.
88. The Fit and Proper Policy must specify the actions to be taken where a person is assessed as not fit and proper.
89. The Fit and Proper Policy must provide that a copy of the Policy is given to:
- a) any candidate for election as a director as soon as possible after the candidate is nominated; and
 - b) any other person before an assessment of their fitness and propriety is conducted.

³ See Attachment B

90. The Fit and Proper Policy must require a fit and proper assessment to be completed before a person becomes the holder of a responsible person position unless the CBS has determined that the person is a responsible person under paragraph 72. In such cases, the Fit and Proper Policy must require an assessment to be provided within 28 days of the person becoming the holder of the responsible person position.
91. Interim appointment to a responsible person position may be made without a full fit and proper assessment for a period of up to 90 days, including any prior period of interim appointment. Prior to making such an appointment, reasonable steps must be taken, as specified in the Fit and Proper Policy, to assess the fitness and propriety of the person. The Financial Institution must complete a full fit and proper assessment prior to appointing the person to the responsible person position on a permanent basis.
92. The Fit and Proper Policy must require periodic reassessment of fitness and propriety for each responsible person position.
93. When an assessment is conducted, a Financial Institution must make all reasonable enquiries to obtain information that it believes may be relevant to an assessment of whether the person is fit and proper to hold a responsible person position.
94. Where a responsible person has been assessed as fit and proper, but the Financial Institution subsequently becomes aware of information that may result in the person being assessed as not fit and proper, the Financial Institution must undertake a full fit and proper reassessment.
95. The Fit and Proper Policy must contain adequate provisions to encourage any person to disclose information that may be relevant to a fit and proper assessment to the Financial Institution or the CBS.
96. The Fit and Proper Policy must require that sufficient documentation for each fit and proper assessment is retained to demonstrate the fitness and propriety of the Financial Institution's current, and recently past, responsible persons.

When a Responsible Person is not Fit and Proper

97. Where a Financial Institution has assessed that a person is not fit and proper, or a reasonable person in the regulated institution's position would make that assessment, the institution must take all steps it prudently can to ensure that the person:
- a) is not appointed to; or
 - b) for an existing responsible person, does not continue to hold the responsible person position.

Informing the CBS

98. A Financial Institution must, within 28 calendar days of when this Prudential Statement applies to it, notify the CBS of the following information for each responsible person:
- a) the person's full name;

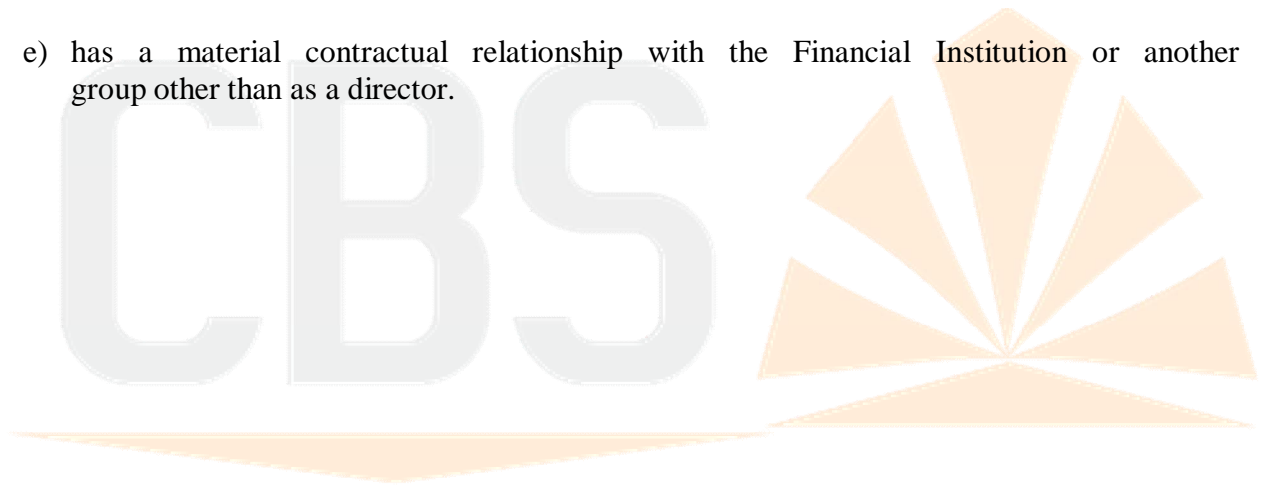
- b) the person's date of birth (for identification purposes only);
 - c) the person's position and main responsibilities; and
 - d) a statement of whether the person has been assessed under the Fit and Proper Policy.
99. A Financial Institution must ensure that the information provided under paragraph 87 remains correct for all its responsible persons. It must provide revised information to the CBS within 28 days of any change or new appointment.
100. A Financial Institution must notify the CBS within 10 business days if it assesses that a responsible person is not fit and proper. If the person remains in the responsible person position, the notification must state the reason for this and the action that is being taken.



Attachment A

A director is not independent if the director:

- a) is a substantial shareholder of the Financial Institution or an officer of, or otherwise associated directly with, a substantial shareholder of the Financial Institution;
- b) is employed, or has previously been employed in an executive capacity by the Financial Institution or another group member, and there has not been a period of at least three years between ceasing such employment and serving on the Board;
- c) has within the last three years been a principal of a material professional adviser or a material consultant to the Financial Institution or another group member, or an employee materially associated with the service provided;
- d) is a material supplier or customer of the Financial Institution or other group member, or an officer of or otherwise associated directly or indirectly with a material supplier or customer; or
- e) has a material contractual relationship with the Financial Institution or another group other than as a director.



Attachment B

Fitness and Proprietary criteria

GOOD CHARACTER

Good character - honesty, integrity fairness and reputation - are qualities that are demonstrated over time. In determining a person's good character, and to guide the fit and proper assessment, the Financial Institution should consider all appropriate factors, including, but not limited to:

- a) Whether the person has been convicted of a criminal offence, particularly an offence relating to dishonesty, fraud or financial crime;
- b) Whether the person has been the subject of any adverse findings or any settlement in civil proceedings, particularly in connection with banking or other financial business, misconduct or fraud;
- c) Whether the person, or any business in which the person is controlling shareholder or has controlling interest or exercises significant influence, has been investigated and disciplined or suspended by a regulatory or professional body, a court or tribunal, whether publicly or privately;
- d) Whether the person has been the owner, manager or director of a company, partnership or other organization that has been refused registration, authorization, membership or a licence to conduct trade, business or profession, or has had that registration, authorization, membership or licence revoked, withdrawn or terminated;
- e) Whether, as a result of the removal of the licence, registration or other authority the person has been refused the right to carry on a trade, business or profession requiring a licence, registration or other authorization;
- f) Whether the person has been a director, partner, or otherwise involved in the management of a business that has gone into receivership, insolvency, or compulsory liquidation while the person was connected with that organization or within a reasonably short period (e.g. one year) after the person's departure from the institution;
- g) Whether the person has been dismissed, asked to resign or resigned from employment or from a position of trust, fiduciary appointment or similar position because of questions about honesty and integrity;
- h) Whether the person has ever been disqualified from acting as a director or serving in a managerial capacity because of wrongdoing; or
- i) Whether the person has not been fair, truthful and forthcoming in dealings with customers, superiors, auditors and regulatory authorities within the past ten years and has been the subject of any justified complaint relating to regulated activities; and
- j) Whether the person demonstrates a readiness and willingness to comply with the requirements and standards of the regulatory system and other legal, regulatory or professional requirements and standards.

COMPETENCE AND CAPABILITY

A person must demonstrate the competence and ability to understand the technical requirements of the Financial Institution's business, the material risks and management processes and controls, with due regard to the interests of all stakeholders.

In assessing the competence and capability of a person, all relevant factors should be considered, including, but not limited to:

- a) Whether the person has demonstrated, through qualifications and experience, the capacity to successfully undertake the responsibilities of the position;
- b) Whether the person has ever been disciplined by a professional, trade or regulatory body, dismissed or requested to resign from any position or office for negligence, incompetence, fraud or mismanagement; and
- c) Whether the person has a sound knowledge of the business and the responsibilities of the position.

FINANCIAL SOUNDNESS

As an indication of a person's capacity to contribute to the safety and soundness of a financial institution and protection of the interests of depositors and other stakeholders, a person should demonstrate the prudent management of his/her own financial affairs.

In determining a person's financial soundness, all relevant factors should be considered, including but not limited to:

- a) Whether the person has been the subject of any judgment or award that remains outstanding or was not satisfied within a reasonable period; and
- b) Whether the person has made any arrangements with his creditors, filed for bankruptcy, been adjudged bankrupt, had assets confiscated, or has been involved in proceedings relating to any of the aforementioned.

The fact that a person may be of limited financial means will not, in itself, affect the person's ability to satisfy the financial soundness criteria.

Prudential Statement 2

Capital Adequacy



Objectives and key requirements of this Prudential Statement

This paper outlines the Central Bank of Samoa's framework for the supervision of the capital adequacy of banks.

The Central Bank attaches great importance to ensuring that individual banks maintain adequate capital in relation to the size and nature of their business. Capital represents a bank's own funds and provides the bank with its core of resources for operations and for its fixed assets. More importantly, capital primarily serves as a cushion against unexpected losses. Thus, it provides protection to depositors and other creditors of a bank. And since it provides protection against losses, it helps to promote public confidence in individual banks and in the banking system in general.

Having a minimum capital standard and compliance with that standard does not ensure that a bank maintains an appropriate amount of capital. The amount of capital that is appropriate for a bank depends on the level of the various risks it assumes, the quality of the management of those risks, the extent and nature of their concentration, the projected increase in risk assets and other factors. Moreover, capital adequacy is not the only measure of the overall strength of a bank. Prudential assessments also need to consider, among other things, asset quality, adequacy of liquidity, quality of management and earning performance.

The Central Bank's approach to the assessment of the capital adequacy of banks centres on a risk-based capital ratio that expresses capital as a percentage of risk-weighted assets and off-balance sheet exposures. This is the preferred method for assessing capital adequacy because it recognises the importance of the quality of capital elements and the different levels of relative riskiness of both on and off-balance sheet exposures of banks.

Contents

Authority.....	23
Application.....	23
Definitions	23
Basic Elements.....	23
Minimum Capital Standards	24
Components of Capital	24
Risk Weighting	26
Off Balance Sheet Items	27
Attachment A ó Capital Adequacy Forms.....	28



Authority

This Prudential Standard is made under Section 3 (2) of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act.

Definitions

‘Off- balance sheet exposures’ represent activities which do not appear on but have the potential to materialize and recognised on the balance sheet. Each exposure is assigned a conversion factor to evaluate its on-balance sheet value before applying a risk weight to calculate its credit risk adjusted value.

‘Risk-weighted assets’ refers to total assets that have been reevaluated to reflect associated level of credit risk. This includes both on-balance sheet lending exposures and credit equivalent amount of off-balance sheet activities. The risk weight applied to an asset is an indication of its risk of default.

‘Tier one capital’ commonly referred to as core capital, incorporating the highest quality elements, i.e permanently and freely accessible funds available to absorb unexpected losses.

‘Tier two capital’ also known as secondary or supplemental capital incorporates elements that have the capacity to absorb unexpected losses but that are less permanent in nature.

Basic Elements

1. The capital of banks has been defined to include among other things, paid-up capital, disclosed reserves and retained earnings, asset revaluation reserves and hybrid capital, term subordinated and other similar instruments.
2. The computation of the risk-based capital ratio focuses primarily on the level of credit risk (i.e. the risk of counterparty default which is the major risk facing most banks) whether arising from on-balance sheet or off-balance sheet activities. It takes account of the varying levels of risk by categorising and assigning risk weights to every on and off-balance sheet exposure based on the type of obligor, the strength of the underlying collateral, the existence of government guarantees and the maturity of the item. It also takes account of the likelihood that the off-balance sheet items will result in credit exposures.
3. When assessing capital adequacy, the Central Bank must be satisfied that specific reserves have been established by the individual banks for known or foreseeable losses. If specific provisions for losses are inadequate, the amount of capital is overstated. Only when specific reserves are maintained at acceptable levels can compliance with the minimum capital standard be assessed. And in this regard, it is expected that banks have the capability to assess all risks but more

importantly the ability to perform a detailed credit analysis of their loan portfolio and to determine the appropriate level of reserves for specific assets or classes of assets.

4. The Bank will establish procedures with individual banks which will define the circumstances in which banks will be expected to discuss their capital position with the Central Bank. In general, these procedures will begin with formal notification to the bank that its current level of capital seems inadequate to support an increase in risk assets. The bank's management will then be required to develop a plan acceptable to the Central Bank designed to achieve an adequate level of capital. The Bank may require that the plan include measures such as reducing or eliminating dividends, reducing the level of risk in the bank, infusing fresh capital or undertaking institutional strengthening to improve the quality of management and management practices. The procedures will also include a series of enforcement proceedings in the event that the bank's management fails to develop an acceptable plan or to adhere to an approved plan.
5. The appropriateness of particular capital ratios and the prudential arrangements for the supervision of banks' capital generally, will be kept under review.

Minimum Capital Standards

6. Every bank operating in Samoa must maintain at all times a level of capital which is prudent in relation to the size and nature of its business and, in any event:
 - a) **Total capital** as a minimum percentage of the bank's risk-weighted exposures shall be no less than fifteen percent (15%).
 - b) **Tier one capital** or **"core" capital** as a minimum percentage of the bank's risk weighted exposures shall be no less than seven and a half percent (7.5%).
 - c) **Tier two capital** or **supplemental capital** shall not exceed hundred percent (100%) of core capital.

Components of Capital

7. **Total capital**, for the purposes of these requirements is defined as the sum of tier one capital and tier two capital.
8. **Tier one capital** is made up of the most important elements of capital. It includes issued share capital and other net worth items which meet all of the following requirements:
 - a) In the case of a capital instrument, it must be issued and fully paid-up; it must be permanently and freely available to absorb unexpected losses i.e. there should be no specified redemption or repayment date, not repayable or redeemable at the option of the holder; it must not be encumbered in any way or earmarked to particular assets or to particular categories of banking activities;
 - b) It should not impose a fixed charge on the bank's earnings i.e. interest obligations must be allowed to be waived if the financial condition of the bank would not support payment and interest obligations so waived must not cumulate;

- c) In a winding-up, must constitute a residual interest such that no distributions may be made to shareholders unless and until all actual and contingent obligations to all creditors of the bank have been discharged.
- d) Based on the foregoing, tier one capital includes:
 - i. Permanent shareholders' equity in the form of:
 - 1) issued and fully paid-up ordinary share capital; and
 - 2) irredeemable non-cumulative preference shares;
 - ii. Disclosed reserves in the form of:
 - 3) non-repayable share premium arising from the issuance of tier one capital instruments;
 - 4) general reserves created by appropriation of earnings; and
 - 5) prior years' audited retained profit, net of any appropriations such as tax payable, dividends, transfers to other reserves or provisions.

Deductions from tier one capital:

The following items must be deducted from **tier one capital**:

- i. Current year's losses
 - ii. Good will and other intangible assets such as organization expenses and amounts paid for franchises to operate the bank
 - iii. All future income tax benefits not deducted elsewhere (e.g. under Item 9c below) net of deferred tax liabilities (i.e. the amount of tax obligation on the current year's and the previous year's income). This means that these future income tax benefits should be deducted only to the extent that the amount exceeds the amount of tax obligation on the current year's and the previous year's income. If the current year's assessable income is negative, the full amount of the future income tax benefits should be deducted.
9. **Tier two capital** consists of equity and other net worth items that can also serve as a cushion for unexpected losses but do not meet the requirements stated in item 8 above. Tier two capital includes:
- a) Unaudited retained profit, net of any appropriations such as tax payable, dividends, transfers to other reserves or provisions
 - b) Asset revaluation reserves arising from a formal revaluation of tangible fixed assets where the revaluations have been subject to audit or review by the bank's auditors.
 - c) General provisions for bad and doubtful debts net of any associated future income tax
 - d) benefits provided that the net amount to be included in tier two capital should not exceed 1.25% of the bank's total risk-weighted exposures
 - e) Hybrid capital instruments i.e. hybrid forms of debt and preference shares (and associated share premium) such as perpetual cumulative preference shares, mandatory cumulative convertible debt and perpetual subordinated debt which meet the following requirements:

- i. they are unsecured, subordinated and fully paid-up;
 - ii. they are not redeemable at the option of the issuer or without the prior consent of the Central Bank;
 - iii. they are available to participate in losses without the bank being obliged to cease trading;
 - iv. interest obligations should be allowed to be deferred whether the profitability of the bank would not support payment.
- f) Term subordinated debt and similar instruments (e.g. cumulative redeemable preference shares) which meet the following requirements:
- i. the claims of holders in respect of payment of both principal and interest are fully subordinated to those of all unsubordinated creditors; and
 - ii. the debt instruments have a minimum original fixed term to maturity of over five years and will be subject to a straight line amortisation in the last five (5) years of its life so that no more than twenty percent (20%) of the original amount issued shall be included in capital in the final year before redemption is possible.
- g) Any proposed issue of hybrid capital and term subordinated debt or similar instruments (described above) must be structured so that they meet in substance as well as in form the requirements of the particular category of capital where they are proposed to be included as stated in the Basle capital measurement framework. Any bank which proposes to issue these instruments must therefore satisfy the Bank that these requirements have been met prior to making the issue.

Risk Weighting

10. The following is a summary of risk-weighting categories, (weighted on the basis of the relative degree of riskiness) that will apply to a bank's on and off-balance sheet exposures:

0%

- a) Cash (including foreign cash)
- b) Claims on the Central Bank of Samoa
- c) Claims on the Central Bank of Samoa
- d) Claims on central governments and central banks denominated in national currency and funded in that currency
- e) Loans which are explicitly, irrevocably and unconditionally guaranteed by the Government of Samoa or the Central Bank of Samoa except that in the case of claims covered by partial guarantees, only that part which is fully covered by the guarantee will have a 0% risk weight.
- f) Securities issued by Government-owned or controlled institutions the repayment of which is explicitly and unconditionally guaranteed by the Government of Samoa

- g) Loans which are fully and formally collateralised by: (1) cash deposited with the lending bank or, (2) securities issued by the Government of Samoa or by the Central Bank of Samoa or, (3) securities issued by Government-owned or controlled institutions the repayment of which is explicitly and unconditionally guaranteed by the Government of Samoa

20%

- a) Claims on banks which are registered or licensed in the country of domicile by the appropriate banking supervisory authorities (includes cash items in process of collection)

100%

- a) All holdings of equity investments
- b) Investment in fixed assets e.g. premises, sites, equipment and other fixed assets less associated accumulated depreciation
- c) All other exposures/assets not in any of the foregoing categories except that any asset item already deducted from capital (Items 5b and 5c above) will not be subject to any risk weight

Off-Balance Sheet Items

11. The following is a list of credit conversion factors that will be applied to take account of the credit risk on the different types of off-balance sheet exposures. The credit conversion factor will be multiplied by the risk weight applicable to the nature of the counterparty for on-balance sheet transactions (Item 6 above).

100% Direct credit substitutes, i.e. general guarantees of indebtedness where the bank undertakes to carry out the financial obligations of a counterparty which fails to do so (i.e. general guarantees of indebtedness where the bank undertakes to carry out the financial obligations of a counterparty which fails to do so (e.g. loan guarantees and standby letters of credit serving as financial guarantees for loans or securities)

50% Transaction-related contingent items, e.g. performance bonds, bid bonds, warranties and performance-related standby letters of credit which fulfil the same function as a performance bond

20% Trade-related contingent items, e.g. documentary letters of credit (where the bank guarantees payment in favour of an exporter against the presentation of shipping documents) and other trade financing transactions e.g. shipping guarantees or bill of lading bonds (which are secured against underlying shipments of goods).

Attachment A

CAP - 1

(BANK NAME) _____

REPORT FORM FOR THE COMPUTATION OF CAPITAL ADEQUACY RATIO

As of :

	<u>Line Reference c/</u>	<u>Amount in Tala Thousand</u>
<u>A. MEASUREMENT OF CAPITAL</u>		
<u>Tier One Capital</u>		
1. Paid-up ordinary share capital	L214	
2. Irredeemable non-cumulative preference shares	n/a	
3. Non-repayable Share premium reserves	L216	
4. General Reserves	L217	
5. Prior years' audited retained profit, net appropriations (e.g. tax payable, dividends, transfers to other reserves or provisions)	L220	
<u>Less:</u>		
6. Current years' losses *	L221	
7. Goodwill and other intangible assets	n/a	
8. All future income tax benefits not deducted elsewhere (e.g. Item 11 below) net of deferred tax liabilities a/	L95	
Sub-total - Tier One Capital	(A1)	
<u>Tier Two Capital</u>		
9. Unaudited retained profit, net of appropriations (e.g. tax payable, dividends, transfers to other reserves or provisions) **	L221	
10. Revaluation reserves	L218	
11. General provision for doubtful debts net of associated future income tax benefits (net amount should not exceed 1.25% of total risk-weighted exposures)	L206	
12. Hybrid capital instruments	n/a	
13. Term subordinated debt and similar instruments	n/a	
Sub-Total - Tier Two Capital (shall not exceed 100% of Tier One Capital)		
Total Capital (Tier One plus Tier Two)	(A)	

a/ Deductible only if future income tax benefits is greater than the deferred tax liabilities.

* L221 Applies only if the bank incurs losses in its current year of operations.

** L221 Applies only to profits achieved by the bank in its current year of operations.

n/a Represents items that banks in Samoa may not have established under their present capital structure

c/ Refer line Reference as provided in Form 1-KB for the completion of this report form.

B. RISK-WEIGHTED BALANCE SHEET EXPOSURES	<u>Line Reference</u>	<u>Amount in Tala Thousand</u>
Total Assets	L97	
<i>Less:</i>		
<u>Provision/Other Deductions:</u>		
1. Specific provision for doubtful debts	L207	
2. Provision for depreciation	L208	
3. Other-Asset items deducted from Capital (ie. Goodwill, Intangible Assets and Future Income Tax Benefits)	L95	
<u>Risk-Adjusted Balance Sheet Exposures:</u>		
0% Risk-Weighted Assets		
4. Cash(including foreign cash)	L2 + L10	
5. Claims on the Government of Samoa	L24-L29, L74-L75	
6. Claims on the Central Bank of Samoa	L4 to L7	
7. Claims on central governments and central banks denominated in national currency and funded in that currency ***	L12+L18+L19+L89	
8. Loans guaranteed by the Government of Samoa or by the Central Bank of Samoa	L237	
9. Securities issued by government-owned or controlled institutions the payment of which is guaranteed by the Government	L235	
10. Loans fully collateralised by:		
a. Cash deposits with the Bank	L238	
b. Securities issued by the Government of Samoa or by the Central Bank of Samoa	L236	
c. Securities issued by the Government-owned or controlled institutions the repayment of which is guaranteed by the Government of Samoa or by the Central Bank of Samoa	n/a	
Sub Total x 100%		
20% Risk-Weighted assets		
11. Claims on banks (including cash items in process of collection)	(L11 to L16) (L61 to L64,L70-L71,L88)	
Sub-Total x 80%		
50% Risk Weighted Assets		
12. Housing loans fully secured by mortgage against the residential properties****	L239	
Sub-Total x 50%		
TOTAL RISK-WEIGHTED BALANCE SHEET EXPOSURES		(B)

*** L12 refers only to claims pertaining to central governments and central banks (if any).

**** L239 refers only to loans relating to housing where the property is or will be occupied by borrower or is rented and where the loan is fully secured by mortgage against the residential property.

C. RISK-WEIGHTED OFF-BALANCE SHEET EXPOSURES				
	<u>Line Ref</u>	<u>Principal Amount</u>	<u>Credit Conversion Factor</u>	<u>Risk Adjusted Value b/</u>
Direct credit substitutes				
1. Amount subject to 0% risk weight d/	L223		100%	
2. Amount subject to 100% risk weight				
Transaction-related contingent items				
3. Amount subject to 0% risk weight d/	L224		50%	
4. Amount subject to 100% risk weight				
Trade-related contingent items				
5. Amount subject to 0% risk weight d/	L225		20%	
6. Amount subject to 100% risk weight				
Total Risk-Weighted Off-Balance Sheet Exposure				(C)
<u>D. CALCULATION OF TOTAL RISK-WEIGHTED EXPOSURES</u>				
7. Total risk-weighted balance sheet exposures (B)				
8. Total risk-weighted off-balance sheet exposures (C)				
Total - Risk-weighted exposures				(D)
<u>E. CALCULATION OF THE CAPITAL RAITOS</u>				
9. Total Capital / Total Risk-Weighted Exposures (A/D) x 100				
10. Tier One Capital / Total Risk-Weighted Exposures (A1/D) x 100				
11. Tier Two Capital / Total Risk-Weighted Exposures				
b/ Risk adjusted value = Principal Amount x Credit Conversion Factor x Risk Weight				
d/ Refer only to off-balance sheet exposure which is fully collateralised by cash deposited with the bank or is guaranteed by the Government of Samoa or by the Central Bank of Samoa.				

Prudential Statement 3

Credit Risk



Objectives and key requirements of this Prudential Statement

This Prudential Statement aims to ensure that all Financial Institutions control credit risk by adopting a prudent credit risk management framework, centered on policies and procedures. These policies and procedures must particularly apply to the recognition, measurement, reporting of, and provisioning for impaired facilities.

That each locally incorporated financial institution must establish and implement an in-house Credit Risk Policy approved by the Board.

Foreign subsidiary operations may adapt Group Policy but must consider the size, nature and scope of local operation and must include the requirements of this Policy.

The key requirements of this Prudential Statement are that a Financial Institution must:

- have an effective credit risk framework that is supported by a robust system for the prompt identification, monitoring, measurement and control of its credit risk;
- be commensurate with the nature, scale and complexity of the institution;
- maintain a portfolio of high-quality assets (loans and investments) that are well diversified and does not present undue risk to capital;
- regularly review its credit risk management systems, taking account of changing operating circumstances, activities and risks;
- have systems to recognize and report impaired facilities and;
- maintain provisions and reserves adequate to absorb credit losses in the portfolio.

This Prudential Statement also covers credit risk in the investment portfolio unless the CBS issues a separate Prudential Statement. All language that can be applicable to the identification, measurement, monitoring, and control of credit risk in the investment portfolio applies if the term “investment securities” can be substituted for “loans” regardless of whether or not the term investment is actually stated.

Contents

Authority.....	34
Application.....	34
Definitions	34
Key Principles	34
Board and Senior Management Responsibilities	35
Credit Risk Management Framework	36
Credit Policies	37
Credit Granting	38
Credit Administration	40
Credit Risk Monitoring	41
Internal Credit Risk Rating System.....	41
Portfolio Review System.....	42
Asset Classification	42
Provisions for Loans Losses	44
Interest Suspension.....	45
Renegotiated or Restructured Loans	45
Managing Problem Credits	46
Attachment A	47

Authority

This Prudential Statement is made under Section 3 (2), of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act.

Definitions

Financial Institution ó bank entity licensed under the Financial Institutions Act 1996.

Facilities ó all loans and other financial products and services provided by a Financial Institution to an entity which give rise to a credit exposure on the entity.

Large Exposure ó exposure to a counterparty or a group of related counterparties which is greater than or equal to 10% of a Financial Institution's capital base.

Non-Performing ó loan is nonperforming when payments of interest and/or principal are past due by 90 days or more, or payments must be capitalized, refinanced, or delayed by agreement, due to inability to repay; or any loan that is current or past due that shows deterioration such that the likelihood of past due or default status is very high and warrants recognition of the deterioration. In addition, external events such as bankruptcy, debt defaults elsewhere and similar tangible signs of financial distress would likely lead to nonperforming status recognition. And at any time where there is doubt that payments will be made in full.

Collateral such as specialised manufacturing facilities and equipment for ongoing operations would not normally be considered well-secured because of the difficulties of actual foreclosure or of disposing of the collateral in a timely manner at values sufficient to protect the Financial Institution from loss.

Key Principles

1. Credit risk ó the risk of counterparty default ó usually represents the single largest risk facing Financial Institutions. The presence of a well-functioning credit risk management system is, therefore fundamental to the safety and soundness of Financial Institutions.
2. It is the responsibility of the Board of Directors (Board) and senior management of a Financial Institution to oversee the nature and level of credit risk which all Financial Institutions undertake. This responsibility includes ensuring that a Financial Institution has in place:
 - (a) credit risk management policies, procedures and controls appropriate to the complexity, scope and scale of its business;
 - (b) appropriate controls to ensure adequate provisions in compliance with the Financial Institution's stated policies and procedures, applicable accounting framework and the requirements of this Prudential Statement; and

(c) a realistic assessment of asset quality.

Board and Senior Management Responsibilities

3. The Board and management are responsible for the sound management of the Financial Institution's credit risk and must ensure the Financial Institution has a robust credit risk management framework to manage this risk accordingly.
4. The Board must establish a credit risk appetite and adopt a credit risk strategy and risk management framework commensurate with the credit risk appetite.
5. The Board and management must have a sound credit granting process that is properly communicated throughout the organization. Approval and authorizations must be well developed, and provide the necessary controls to mitigate risk.
6. The Board and management must establish a system of independent ongoing credit review that provides the Board with regular information about the credit risk, asset quality, trends in individual credits, portfolio segments, and the portfolio in aggregate.
7. A Financial Institution's senior management must, at a minimum:
 - (a) develop the credit management strategy, policies and processes in accordance with the Board-approved risk appetite;
 - (b) ensure that the Financial Institution maintains sufficient credit quality at all times;
 - (c) determine the structure, responsibilities and controls for managing credit risk and for overseeing the credit portfolio;
 - (d) ensure that the Financial Institution has adequate internal controls to safeguard the integrity of its credit risk management processes;
 - (e) establish a set of reporting criteria specifying the scope, manner and frequency of reporting for various recipients (such as the Board, senior management and the risk and credit committees) and the parties responsible for preparing the reports;
 - (f) establish the specific procedures and approvals necessary for exceptions to policies and limits, including the escalation procedures and follow-up actions to be taken for breaches of policy limits;
 - (g) closely monitor current trends and potential market developments that may present challenges for managing credit risk, so that appropriate and timely changes to the credit risk management strategy can be made as needed; and
 - (h) continuously review information on the Financial Institution's credit developments and report to the Board on a regular basis.
8. A Financial Institutions must identify and manage credit risk inherent in all products and activities. The institution must ensure that the risks of new products and activities are subject

to adequate procedures and controls before being introduced or undertaken, and approved in advance by the Board or its appropriate committee.

9. The Board and senior management must be able to demonstrate a thorough understanding of the links between credit risk and other risks within the Financial Institution, including liquidity, market, operational and reputation risks.

Credit Risk Management Framework

10. The Financial Institution's credit risk management framework must include, at a minimum:
 - (a) A statement of the Financial Institution's credit risk appetite, representing the amount of credit risk that the Board is willing to accept in the Financial Institution to meet its strategic objectives;
 - (b) a robust management information system that produces data and other information required for adequately assessing the credit risk exposure of the institution, including levels of impairment, accounting for asset impairment and reporting to CBS;
 - (c) a defined organizational structure;
 - (d) the credit management strategy and policy;
 - (e) operating standards in the form of policies, procedures and controls, for identifying, measuring, monitoring and controlling its credit risk in accordance with its credit risk appetite;
 - (f) senior management and other relevant personnel that have the necessary experience to manage credit risk;
 - (g) regular reporting on the existing credit risk of the Financial Institution and, information on new or emerging credit risks; and
 - (h) annual review and approval by the Board.
11. A Financial Institution's credit risk management framework must include comprehensive documented policies, procedures and controls addressing at a minimum the following:
 - (a) board and senior management responsibilities;
 - (b) credit policies;
 - (c) credit granting;
 - (d) credit administration;
 - (e) concentrations;
 - (f) credit risk monitoring;
 - (g) internal credit risk rating system;
 - (h) portfolio review system;
 - (i) collateral role, purpose and valuation;
 - (j) asset classification including the write-off of uncollectible facilities;
 - (k) provisions for loans losses and the adequacy of reserves for current and future losses;
 - (l) interest suspension;

- (m) renegotiated or restructured loans; and
 - (n) managing problem credits.
12. A Financial Institution's credit risk management framework must clearly set out the organizational structure as it relates to credit for the Financial Institution, and define the roles and responsibilities of management and staff involved in managing credit risk. It must be well integrated into the Financial Institution's overall risk management process.
 13. A Financial Institution's credit risk management function must be staffed with personnel who have the skills and authority to challenge the Financial Institution's credit risk management practices.
 14. The credit management strategy must be appropriate for the nature, scale and complexity of the Financial Institution. In formulating this strategy, the Financial Institution must consider its legal structure, key business lines, the breadth and diversity of markets, products and jurisdictions in which it operates, and regulatory requirements.
 15. The credit management strategy, key policies for implementing the strategy, and the credit risk management structure must be communicated throughout the organization by senior management.
 16. A Financial Institution must have adequate policies, procedures and controls in place to ensure that the Board and senior management are informed immediately of new and emerging credit concerns. These include a significant decline in the quality of underwriting, high or increasing exceptions to policy, noncompliance with policy, material or persistent breaches of limits, or changes in external market conditions that could signal future difficulties.
 17. The credit risk management framework must be subject to effective and comprehensive independent review on an ongoing basis. In most cases, the independent reviews could be facilitated by a Financial Institution's internal audit function but may require the engagement of independent parties outside of this function.

Credit Policies

18. The Board must adopt credit policies that clearly outline the Financial Institution's view of business development priorities and the terms and conditions that are necessary for loans to be approved.
19. The credit policies must be updated at a regular interval to reflect changes in the economic outlook and the evolution of the Financial Institution's loan portfolio.
20. The credit policies must be communicated timely and be implemented by all levels of the Financial Institution through appropriate procedures. It should be distributed to all lending authorities and credit officers.
21. At a minimum, credit policies must include:
 - (a) the identification of credit risk, both on and off the balance sheet, by investments, portfolio, products, sectors, and geographic segments;

- (b) areas of credit in which the Financial Institution plans to lend and not lend (acceptable and unacceptable types of credit);
- (c) target market within each lending segment and level of diversification/concentration;
- (d) clear guidelines for each of the various types of credits, including (but not limited to) loans, overdrafts, mortgages and leases;
- (e) terms and conditions under which it will consider an application for each type of credit facility that the Financial Institution will provide, including acceptable loan tenor, type of acceptable collateral security, maximum loan to value ratio, and types of borrowers, currencies, geographies, industries and sectors;
- (f) specified acceptable and unacceptable financial quality and repayment performance measures, such as debt service coverage ratios, cash flow, liquidity, and debt to worth ratios;
- (g) the Financial Institution's formal credit approval process - detailed and formalized credit evaluation and appraisal process, administration and documentation;
- (h) credit approval authority;
- (i) concentration and diversification limits for connected counterparties, industries or economic sectors, geographic regions, and products;
- (j) credit pricing strategy;
- (k) roles and responsibilities of staff involved in credit;
- (l) guidelines on monitoring and reporting system;
- (m) internal risk grading criteria;
- (n) criteria for past due, non-accrual, and restructuring of loans;
- (o) guidelines on management of problem loans;
- (p) authority for approval of allowance for losses and write-offs;
- (q) identification, reporting, and approvals of exceptions to policy and procedures,
- (r) internal control systems for disbursement of funds that require completion of all legal and required actions and conditions be met prior to authorization to disburse funds; and
- (s) quantitative and qualitative targets.

Credit Granting

22. A Financial Institution must have a well-defined credit granting strategy, in line with its stated credit risk appetite, and well-defined criteria for granting of credit.

23. Before granting credit, a Financial Institution must receive sufficient information to enable a comprehensive assessment of the true risk profile of the counterparty, including up to date financial information.
24. At a minimum, the factors to be considered and documented in approving credits must include:
- (a) the purpose of the credit, the source of repayment and the consistency between these two elements;
 - (b) the integrity and reputation of the counterparty;
 - (c) the current risk profile (including the nature and aggregate amounts of risks) of the counterparty and its sensitivity to economic and market developments;
 - (d) the counterparty's repayment history and consistency, financial trends, current capacity to repay, the stated source of repayment, and financial and cash flow projections;
 - (e) a forward-looking analysis of the capacity to repay based on various scenarios;
 - (f) the legal capacity of the counterparty to assume the liability;
 - (g) for commercial credits, the counterparty's business expertise and the status of its economic sector and position within that sector;
 - (h) the proposed terms and conditions of the credit, including covenants designed to identify early signs of deterioration and allow the Financial Institution to take preemptive action to protect its loan; and
 - (i) the adequacy and enforceability of collateral or guarantees.
25. The assessment of a borrower's ability to repay must include at a minimum analysis of common financial ratios of current and historical financial condition along with full analysis of financial position or net worth of the borrower, and financial performance or income and expenditure of the borrower.
26. For non-retail counterparties the following minimal financial ratios should be analyzed to demonstrate adequate debt serviceability, evidence of liquidity and adequate security coverage; and any other relevant indicators.
27. For retail counterparties, this analysis should include consideration of debt service coverage ratio, loan-to-value ratio and credit scores where applicable.
28. A Financial Institution must not substitute collateral for a comprehensive assessment of the counterparty's capacity to repay the facility, nor can it compensate for insufficient information. An institution may utilize collateral and guarantees to help mitigate risks inherent in individual credits but transactions should be entered primarily on the strength of the counterparty's repayment capacity.

29. A Financial Institution must have policies covering the acceptability of various forms of collateral, procedures for the ongoing valuation of such collateral, and a process to ensure that collateral is, and continues to be, enforceable and realizable.
30. Regarding guarantees, Financial Institutions must evaluate the level of coverage being provided in relation to the credit-quality and legal capacity of the guarantor.
31. The Financial Institution must have ongoing access to borrower's financial information, including the submission of financial statements where applicable. For non-retail borrowers, this requirement should include the audited financial statements by a Chartered Practicing Accountant for the last financial year, cash flow statements and any other report where applicable.

Credit Administration

32. Credit administration is a critical and independent function in maintaining the safety and soundness of a Financial Institution. The credit administration function provides the physical aspects of granting and maintaining credit.
33. A typical credit administration unit should perform the functions of credit documentation, disbursement and monitoring; loan repayment; and maintenance of credit files, collateral and security documents. Once a credit is granted, it is the responsibility of Credit Administration to ensure that the credit is properly maintained.
34. Credit administration must ensure completeness of documentation (loan agreements, guarantees, transfer of title of collaterals etc.) in accordance with approved terms and conditions. This includes keeping the credit file up to date, obtaining current financial information, sending out renewal notices and preparing various documents such as loan agreements.
35. The Financial Institution must ensure:
 - (a) the efficiency and effectiveness of credit administration operations, including monitoring documentation, contractual requirements, legal covenants, collateral recordation;
 - (b) the accuracy and timeliness of information provided by management information systems;
 - (c) the adequacy of controls over all credit administration procedures; and
 - (d) compliance with prescribed management policies and procedures as well as applicable laws and regulations.
36. Senior management must understand and demonstrate that it recognizes the importance of this element of monitoring and controlling credit risk, to help ensure the various components of credit administration to function appropriately.

Credit Risk Monitoring

37. A Financial Institution's credit risk management framework must provide for the systematic and regular monitoring of credit risk, to assist the Board and senior management in obtaining, on a regular basis, a view of trends and other changes in the overall nature and levels of credit risk, and in assessing the adequacy of provisions, and capital.
38. A Financial Institution's credit risk monitoring must include measures that:
- (a) enable the Board and senior management to readily understand the current (and changing) financial condition of its borrowers, individually and in aggregate;
 - (b) ensure that all credits are in compliance with existing covenants;
 - (c) allow management to view customer credit lines usage and to take timely action when these lines are not used as approved;
 - (d) ensure that the projected source of repayment, including cash flow and sale of assets, meet debt servicing requirements on an ongoing basis;
 - (e) ensure that, where applicable, collateral provides adequate coverage relative to the obligor's current condition;
 - (f) identify and classify potential problem credits on a timely basis;
 - (g) ensure the accuracy of the information submitted to the Board and management.
39. A Financial Institution's credit risk monitoring must comprise a full suite of asset quality indicators including qualitative and quantitative quality reports. Examples of quantitative credit risk ratios are listed in attachment A.

Internal Credit Risk Rating System

40. A Financial Institution must develop an internal credit risk rating system for its credit risk assets. The risk rating should categorize all credits into various classes on the basis of underlying credit quality and ability to repay.
41. All facilities should be assigned a risk rating. When deterioration in repayment ability is noted, the risk rating should be changed within the earlier of 30 calendar days or quarter end. The rating system should be consistent with the nature, size and complexity of a Financial Institution's activities.
42. The risk rating system must have the following parameters at a minimum:
- (a) covers a broad range of the Financial Institution's credit exposure, including on and off-balance sheet exposures, investments, and other credit exposure assets;
 - (b) covers both performing and non-performing assets;

- (c) has several grades covering exposures, with the lowest rating accorded to those where losses are expected;
- (d) has more than one risk grade for performing credits;
- (e) can be readily mapped to the regulatory classifications (õstandardõ or õcurrentõ, õspecial mentionõ, õsubstandardõ, õdoubtfulõ and õlossõ);
- (f) is consistent with the nature, size and complexity of the Financial Institution's activities; and
- (g) provides ongoing updated risk ratings at renewals and when borrower financial condition changes.

Portfolio Review System

- 43. A Financial Institution must have an established portfolio review system that is aimed at identifying credit quality in the portfolio by risk rating the individual credits and reviewing the accuracy of those ratings over time.
- 44. A Financial Institution's portfolio review system should ensure that timely and adequate management action is taken to maintain the quality of the loan portfolio and that adequate provisions for losses are established and maintained.
- 45. A Financial Institution must recognise that maintaining loss provisions is a stabilising factor and that failure to make adequate provisions may result in misrepresentation of a Financial Institution's financial condition.
- 46. The portfolio review system should include an annual risk based review of portfolio quality and condition, including a reassessment of the internal credit rating of individual exposures, with a minimum sample review ratio of sixty percent (60%) of outstanding loan volume.
- 47. The portfolio review system should include a summary report presented to the Board (at least annually) that contains the scope and results of the review, risk rating downgrades and upgrades, conclusions regarding documentation, policy and procedure compliance, and adequacy of provisioning.
- 48. The portfolio review system must sample various portfolio segments, sectors, and types of loans, as well as size of loan.
- 49. The portfolio review and asset classification is predicated on the ability of Financial Institution staff (or as necessary external service providers) to perform appropriate financial analysis of the counterparty's ability to repay the debt as structured. The analysis must include assessment as specified in paragraphs 25, 26 and 27 of this Prudential Statement.

Asset Classification

- 50. A Financial Institution must assign credit classifications to all direct and indirect extensions of credit including loans and advances, accounts receivable, property acquired in settlement

of loans, equity investments, contingent items in the nature of direct credit substitutes and miscellaneous asset accounts.

51. A Financial Institution must classify assets for regulatory reporting and provisioning in the following categories:

Standard /Pass/Acceptable

Assets in this category are not subject to criticism. In general, performing loans, loans and other assets which are fully and formally collateralised, both as to principal and interest, by cash or by deposits with the lending Financial Institution or by securities issued by the Government or by the CBS, are exempted from classification regardless of arrears or other adverse credit factors.

The standard category includes assets which are not considered to have problems. Assets falling into the latter three categories below possess various degrees of well-defined weaknesses and are collectively referred to as 'classified' assets.

Financial Institutions should begin to develop a grading system with multiple 'standard' ratings based upon capacity to repay, level and liquidity of collateral support, tenor, and other financial metrics. When pricing loans these same attributes are used to determine the necessary risk premiums required of an approved loan. The grading system is complementary to the pricing system of the Financial Institution.

Special Mention

A special mention asset has potential weaknesses that deserve management's close attention. If left uncorrected, these potential weaknesses may result in deterioration of the repayment prospects for the asset or in the institution's credit position at some future date. Special mention assets are not adversely classified and do not expose an institution to sufficient risk to warrant adverse classification.

Substandard

Substandard assets are not protected by the current financial soundness and paying capacity of the counterparty. Substandard assets are those whose primary sources of repayment are insufficient to service the debt and the Financial Institution is constrained to look to secondary sources (e.g. collateral, sale of fixed assets, refinancing or fresh capital) for the repayment of loan. Substandard assets display well-defined credit weaknesses that jeopardise the full settlement of the debt.

Substandard assets may also include assets which carry more than a normal degree of risk due to the absence of current and satisfactory financial information or inadequate collateral documentation. •

Non-performing assets which have been 'past due' for at least 90 days should be, at a minimum, classified as substandard.

Doubtful

Doubtful assets exhibit all the weaknesses inherent in assets classified as *substandard* with added characteristics that the assets are not *well-secured*. These weaknesses make collection in full, on the basis of currently existing facts, conditions and values, highly questionable and improbable. The possibility of loss is high, but because of certain important, reasonably and timely specific pending factors which may strengthen the asset, its classification as an estimated loss is deferred until a more precise status is obtained. *Non-performing* assets which have been *past due* for more than 180 days must be classified as doubtful.

Because assets in this classification are pending specific and timely events it is not appropriate to continue a doubtful classification for more than 12 months.

Loss

Assets classified as loss are considered uncollectible and their continued inclusion in the Financial Institution's books as Financial Institution assets is not warranted. This classification does not mean that the asset has no recovery or salvage value. Rather, that it is neither practical nor desirable to defer writing off the asset even though it is possible that partial recovery may be affected in the future. Financial Institutions should not retain assets on the books while attempting long-term recoveries. Losses should be taken into account in the period in which they are identified as uncollectible. *"Non-performing"* assets which have been *"past due"* for at least one year are also classified *loss* unless such assets are *well-secured*, legal action has commenced and timely realisation of the collateral or successful enforcement of the guarantees can be expected.

52. Nothing contained above prevents a Financial Institution from making a more conservative classification if such is warranted based upon its own analysis of the counterparty's financial condition, ability and willingness to repay.
53. When applying the risk grading to a counterparty that has more than one credit facility, the Financial Institution must apply the rating consistently to all loans that are subject to the same source of repayment, obligor financial strength (or lack thereof) or other factors unless the Financial Institution can prove that one or more of the other loans has a well-defined separate source of repayment that is not jeopardized.

Provisions for Loans Losses

54. A Financial Institution must apply minimum regulatory provisions, as follows:

Standard	1%
Special mention	10%
Substandard	20%
Doubtful	50%
Loss	100%

55. Nothing contained above prevents a Financial Institution from maintaining larger provisions or additional provisions for loan losses if it feels this is warranted based on the condition of the Financial Institution's portfolio, changes in lending practices, economic trends and loss experience.

Interest Suspension

56. All "sub-standard", "doubtful" and "loss" assets must be placed on non-accrual basis within 30 days of such designation. All previously accrued but uncollected interest should be reversed from income by debiting the profit and loss account and crediting the interest in suspense account established for each asset placed on a non-accrual basis.
57. "Non-performing" assets should only be restored to an accrual basis upon the full settlement of all delinquent principal and interest and in accordance with the same performance requirements as renegotiated and restructured loans below. Funds for the repayment of delinquent principal and interest should not be obtained through the creation of new loans from the same Financial Institution.

Renegotiated or Restructured Loans

58. A Financial Institution must have policies and procedures that address restructured or renegotiated loans. The restructured loan designation applies to loans which, because of weaknesses in the counterparty's financial condition or ability to pay, have been refinanced, rescheduled, rolled-over or otherwise modified at favourable terms and conditions for the borrower. The modification may include lengthening of repayment schedules or lowering interest rates to meet the borrower's debt service abilities.
59. While loan restructuring can be considered a management tool to maintain or improve asset quality or the soundness of lending operations, troubled restructurings should be carefully analysed to ensure that the modification is not delaying or avoiding recognition of necessary risk rating classification, provisioning, non-accrual, non-performing, or write downs associated with the concessions. In this process, it is expected that the Financial Institution will take all action to enhance the creditworthiness of the facility, including obtaining additional collateral, guarantors, control over borrower cash flows, ongoing interim and annual financial information submissions, and the implementation of loan covenants.
60. If the restructuring occurs after the counterparty has been graded as Substandard or worse, the supporting documentation for restructuring must be robust given the presumption that a substandard borrower exhibits well-defined weaknesses and financial difficulties. The Financial Institution's analysis must reflect why this restructuring is in its best interest.
61. For restructurings that reflect a concession by the Financial Institution to the counterparty, such as reduced interest rate, extended amortization schedules, and other similar concession criteria, the Financial Institution must revalue the loan as if granted at current interest rates and repayment terms. The result may be a discount of the loan value and would require a write down in the Financial Institution's accounts.
62. Restructured loans should be classified as Substandard until a sustained and satisfactory record of repayment performance has been achieved, for a minimum period of six months, under the new repayment program. Upon satisfactory completion of the minimum period the Financial Institution can return the credit to accrual status.

63. Repeat loan restructuring should be avoided. If a second restructuring is approved the repayment history required before returning the credit to performing status and removal from substandard is increased to 12 months.
64. The restructuring of loans to connected borrowers (See the *Example Draft Prudential Statement – Connected Lending and Activities, and Direct Ownership Interests*) must be on terms not less favourable to the Financial Institution than those offered to other clients.

Managing Problem Credits

65. The credit risk policy must define the Financial Institution's system of managing their problem assets. Once a loan is identified as a problem, it should be managed under a dedicated remedial process.
66. Responsibility for such credits may be assigned to the originating business function, a specialized workout section, or a combination of both, depending upon the size and nature of the credit and the reason for its problems.
67. When a Financial Institution has significant credit-related problems, it is important to segregate the workout function from the credit origination function. The additional resources, expertise and more concentrated focus of a specialized workout section normally improve collection results. In such case, the Recovery Unit, shall manage accounts with sustained deterioration (a risk rating of Substandard or worse).
68. The recovery unit's primary functions should be to:
 - (a) determine account action plans or recovery strategies;
 - (b) monitor compliance with the action plan, adjusting the plan as necessary;
 - (c) pursue all options to maximize recovery, including placing customers into legal proceedings or liquidation as appropriate;
 - (d) ensure adequate and timely loan loss provisions are made based on actual and expected losses;
 - (e) regular review of substandard or worse accounts; and
 - (f) regular reporting to the Board on the overall problem loan portfolio and in particular, the large and complex credits.

Attachment A

RATIO	INTERPRETATIONS
NPL ratio ó that is nonperforming as a percentage of total loans and advances.	Level and severity of non-performing loans and advances. An assessment of the portfolio quality, credit analysis and management and level of potential future write-offs. This ratio also gives an indication of the quantum of non-income generating loans.
NPL minus provision for loan losses/ tier one capital	Gives an indication of the impairment to capital
Provisions for loan losses / NPL	Level and adequacy of provision made for portfolio losses
Past due loans/NPL	Level of unsatisfactory assets past maturity date - indicates severity of delinquency.
Total delinquency - all loans in arrears and nonperforming overdrafts compared to total loans and advances	Gives an indication of the total risk in the credit portfolio
Amount outstanding by sector/Total Loans	Portfolio concentration by sector. It is an indication of the Financial Institution's vulnerability to the performance of a sector.
Amount outstanding by largest borrower (group)/Total Loans	Portfolio concentration by individual or borrower group. It is an indication of the Financial Institution's vulnerability to the performance of a small group of customers.

Prudential Statement 4

Large Exposures



Objective and key requirements of this Prudential Statement

The purpose of this Prudential Statement is to protect the safety and soundness of Financial Institutions by preventing excessive investments in or loans to any one person or group of interrelated persons who are financially interdependent.

Excessive exposure to a single customer or group of customers is a significant risk for Financial Institutions. The CBS seeks to promote diversification to reduce credit risk in a Financial Institution's loan portfolio.

It is the responsibility of the Board of Directors and management of each Financial Institution to adopt policies and procedures which ensure that all exposures comply with the limits set forth in this Prudential Statement. They must ensure that the policies and procedures are made and administered in accordance with prudent lending practices



Contents

Authority.....	51
Application.....	51
Definitions	51
Control of Large Exposures and Risk Concentrations	544
Loans to Partnerships	55
Prudential Limits.....	55
Prior Consultation Requirements	56
Notification Requirements.....	56
Concentration of Risk.....	56
Non-Conforming Exposures	57
Other Matters	57
CBS Final Authority.....	58

Authority

This Prudential Statement is made under Section 3 (2) of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act.

Definitions

CBS to add definitions from The Banking Act, the Financial Institutions Act, and existing Prudential Statements as appropriate.

Financial Institution ó bank entity licensed under the Financial Institutions Act 1996.

Large Exposure – exposure to a counterparty or a group of related counterparties which is greater than or equal to 10% of a Financial Institution's Total Capital.

Exposure – the aggregate of all actual and potential claims as well as, commitments and contingent liabilities arising from on-and off-balance sheet transactions, in both the banking and trading books, to single counterparties and groups of connected counterparties, or groups of related counterparties reflecting the maximum possible loss from their failure to perform on such exposures, and

- (a) includes, but is not limited to:
 - i. outstanding balances of all loans and advances;
 - ii. holdings of debt and/or equity securities;
 - iii. inter-bank lending, derivative transactions, securities financing transactions and trading activities;
 - iv. all unused advised off-balance sheet commitments whether revocable or irrevocable; and
 - v. the credit equivalent amounts of all market-related contracts.
- (b) excludes:
 - i. exposures deducted from a Financial Institution's capital;
 - ii. exposures to the extent that they are secured by cash deposits; and
 - iii. exposures to the extent that they are guaranteed by, or secured against securities issued by, governments or central banks (being the Samoan government, foreign governments and central banks which receive a zero per cent risk-weight).

Group of Related Counterparties ó where two or more individual counterparties are linked by cross guarantees; common ownership or management; the ability to exercise control over the borrower, whether direct or indirect; or other financial interdependency such that the financial soundness of any of them may affect the financial soundness of the other(s); or other connections or relationships which, according to a Financial Institution's assessment, identify the counterparties

as constituting a single risk. The definition also includes persons who are family members that are financially inter-dependent upon one or more persons or companies within the group.

Control - when:

- (a) one or more persons acting together directly or indirectly own or have power to vote 20% or more of the voting shares of another person; or
- (b) one or more persons acting together control, in any manner, the election of a majority of the directors, trustees, or others exercising similar functions of another person; or
- (c) any other circumstances exist which indicate that one or more persons acting together exercise a controlling influence, directly or indirectly, over the activities, management, practices or policies of another person.

Corporate Group – a corporation plus all its subsidiaries and associates

Holding company- a company is another company's holding company if that other company is its subsidiary

Person – an individual or any legal entity

Related Persons – two persons will be considered to be related if one person has the ability, directly or indirectly, to control the other person or to exercise significant influence over the financial and operating decisions of the other person, or if both persons are subject to common control or common significant influence.

Related Company – a company is related to another company if:

- a) the other company is its holding company or subsidiary; or
- b) more than half of the issued shares of the company, other than shares that carry no right to participate beyond a specified amount in a distribution of either profits or capital is held by the other company and companies related to that other company (whether directly or indirectly, but other than in a fiduciary capacity); or
- c) more than half of the issued shares, other than shares that carry no right to participate beyond a specified amount in a distribution of either profits or capital, of each of them held by members of the other (whether directly or indirectly, but other than in a fiduciary capacity); or
- d) the businesses of the companies have been so carried on that the separate business of each company, or a substantial part of it, is not readily identifiable; or
- e) there is another company to which both companies are related; and "related company" has a corresponding meaning

Significant Influence – the ability to participate in a material way in the financial and operating policies and decisions of another person. The absence of absolute control does not preclude the

ability to exert significant influence over the policies and decisions of another person. If one person holds, directly or indirectly through subsidiaries, 10% or more of the voting power over another person, it will be presumed that the first person exerts or has the ability to exert significant influence over the second person. Conversely, if a person holds, directly or indirectly through subsidiaries, less than 10% of the voting power over another person, it will be presumed that the first person does not exert or have ability to exert significant influence unless there are compelling circumstances to the contrary. A substantial or majority ownership in one person by a second person does not preclude a third person from having significant influence over the first person.

Subsidiary – a person in which another person owns, directly or indirectly, more than fifty per cent of the outstanding voting stock.

A company in which another company:

- a) controls the composition of the board of the company
- b) is in a position to exercise, or control the exercise of, more than one-half the maximum number of votes that can be exercised at a meeting of the company; or
- c) holds more than one-half of the issued shares of the company, other than shares that carry no right to participate beyond a specified amount in a distribution of either profits or capital; or
- d) is entitled to receive more than one-half of any dividend paid on shares issued by the company, other than shares that carry no right to participate beyond a specified amount in a distribution of either profits or capital

Single Borrower is any single person that is a borrower. A group of closely related borrowers (legal, natural or both) is also to be regarded as a single customer. This means that a Financial Institution's exposure to each borrower which belongs to a group will be combined and the combined exposure will be deemed to be in respect of a single customer. The general test to be applied is whether the combined exposure represents a single risk to the lending Financial Institution, i.e. the borrowers are so interconnected that if one borrower experiences financial difficulties, the other borrower or borrowers are also likely to encounter payment difficulties. Indications (and examples) of such interconnections or group relations which are generally classified as a single risk are as follows:

- (a) Companies with common ownership or cross ownership (e.g. a parent or holding company and its subsidiaries);
- (b) Borrowers linked by guarantees or cross-guarantees or which share the same collateral, the proceeds from the credit facility are re-loaned or given to another person (i.e. accommodation);
- (c) the proceeds from the credit facility are used for the direct benefit of another person (the "use" test); or
- (d) the two persons constitute a common enterprise and the enterprise is expected to generate or provide the funds to repay the credit facility/ies (the "source" test). A

common enterprise includes loans to borrowers who are related directly or indirectly through common control, provided that 50 percent or more of one borrower's gross receipts or gross expenditures are derived from transactions with the other borrower.

Total Capital to the sum of Tier One and Tier Two capital as defined in Prudential Statement No 2

Control of Large Exposures and Risk Concentrations

1. A Financial Institution must incorporate the management of risk concentrations to counterparties, industries, countries and asset classes into its risk management framework.
2. The Board of a Financial Institution (Board) is responsible for establishing and monitoring compliance with policies governing large exposures and risk concentrations of the Financial Institution.
3. The Board and senior management of a Financial Institution should ensure that:
 - (a) adequate systems and controls are in place to identify, measure, monitor, and control large exposures and risk concentrations of the Financial Institution in a timely manner; and
 - (b) large exposures and risk concentrations of the Financial Institution are kept under regular review.
4. The Board must ensure that these policies are reviewed regularly (at least annually) and that they remain adequate and appropriate for the Financial Institution. Any material changes to established policies must be approved by the Board.
5. A Financial Institution's large exposures and concentrations policy must, as a minimum, cover the following:
 - (a) specific exposure limits to capital for:
 - i. various types of counterparties (e.g. governments, Financial Institutions and foreign equivalents, corporate and individual borrowers);
 - ii. a group of related counterparties;
 - iii. individual industry sectors (where applicable);
 - iv. individual countries (where applicable); and
 - v. various asset classes (e.g. property holdings and other investments) that are commensurate with the Financial Institution's capital base and balance sheet size;
 - (b) the circumstances in which the above exposure limits may be exceeded and the authority required for approving such excesses; and
 - (c) the procedures for identifying, measuring, monitoring and reporting large exposures of the Financial Institution.

6. A Financial Institution must, where appropriate, conduct stress testing and scenario analysis of its large exposures and risk concentrations to assess the impact of changes in market conditions or key risk factors (e.g. economic cycles, interest rate, liquidity conditions or other market movements) on its risk profile and earnings.

Loans to Partnerships

7. For purposes of this Prudential Statement, the total exposure to a partnership shall include the loans and advances to all general partners but not the credits to limited partners unless:
 - (a) the proceeds of loans and advances to limited partners are used for the direct benefit of the partnership; or
 - (b) the loans and advances to limited partners are repayable primarily from the profits of the partnership.
8. For purposes of this Prudential Statement, the total exposure of each general partner shall include exposures to the partnership but not exposures to limited partners unless:
 - (a) the proceeds of credits to limited partners are used for the direct benefit of the general partners; or
 - (b) the credits limited partners are repayable primarily from funds provided by the general partners.
9. For purposes of this Prudential Statement, a loan to a person for purchasing an interest in the partnership will be combined with loans made to the partnership.
10. If a partnership agreement specifies that limited partners are not liable for the debts of the partnership, the rules in paragraphs 7, 8, and 9 above will apply to all general partners but not to limited partners. However, if the partnership agreement specifies that limited partners are liable for a portion of the partnership debt in proportion to their partnership interest, then their pro rata share of the partnership debt will be combined with their personal loans to determine the total exposure of the Financial Institution.

Prudential Limits

11. A large exposure is an exposure to a counterparty or a group of related counterparties which is greater than or equal to ten percent (10%) of a Financial Institution's Total Capital.
12. The maximum aggregate exposure of a Financial Institution to a counterparty or a group of related counterparties and any external parties (other than governments and central banks) unrelated to the Financial Institution is twenty-five percent (25%) of Total Capital.
13. Financial Institutions should treat the twenty-five percent (25%) limit as the upper limit for an exposure. The CBS expects Financial Institutions to establish lower internal limits for its daily activities, in line with their risk appetite

14. Family members are not considered to be connected where the Financial Institution can demonstrate that any extension of credit is supported by a clearly defined and authenticated separation of family member financials. This includes separate financial statements, income sources, sources of repayment, and deposit accounts. Comingling of funds supports the conclusion that a connection exists. Notwithstanding the above, a Financial Institution can choose to treat such exposures as connected should it consider appropriate to do so.

Prior Consultation Requirements

15. A Financial Institution must consult with the CBS prior to committing to any proposed exposures to counterparties, other than governments and central banks, in excess of fifteen percent (20%) of its Total Capital.
16. The CBS may, in writing, set a higher consultation threshold or waive the prior consultation requirements for individual Financial Institutions where the CBS is satisfied with the robustness of the Financial Institution's credit risk management systems and controls.

Notification Requirements

17. A Financial Institution must notify the CBS immediately of any breach of the prescribed limits under paragraphs 11 - 14 or other specific limits imposed by the CBS, including remedial actions taken or planned to deal with the breach.
18. A Financial Institution must inform the CBS immediately where it has concerns that its large exposures or risk concentrations have the potential to impact materially upon its capital adequacy, along with proposed measures to address these concerns.

Concentration of Risk

19. Where a Financial Institution has several large exposures (excluding any exposure to governments and central banks) or where in the CBS's opinion, the Financial Institution is exposed to a significant level of risk concentration, CBS may require the Financial Institution to maintain a higher capital ratio. In considering whether a Financial Institution's capital ratio should be increased, the CBS will take account of the following factors:
 - (a) consistency with the Financial Institution's policy on large exposures and risk concentrations;
 - (b) the number of exposures, their individual and combined size and risk grading; and
 - (c) the characteristics of the Financial Institution, including the nature of its business and the experience of its management.
20. The CBS may also direct a Financial Institution to take measures to reduce its level of risk concentration.

Non-Conforming Exposures

21. Exposures which do not conform to the limits in paragraphs 11 -14 when this Prudential Statement comes into effect, or which subsequently become nonconforming, will be treated as follows:
- (a) Exposures made prior to the date of this Prudential Statement which exceed the limits in paragraph 21 will not be cited in contravention of this Prudential Statement but will be noted as "nonconforming". A Financial Institution may renew, extend the maturity of, or restructure a nonconforming exposure without contravening this Prudential Statement provided the Financial Institution makes a documented good faith effort to bring the exposure into conformance with the requirements of this Prudential Statement, unless:
 - i. the Financial Institution increases the exposure or otherwise advances additional or new funds to the person;
 - ii. a new borrower replaces the original borrower;
 - iii. the CBS determines that the renewal, extension, or restructuring of the exposure is designed to evade the limits in Prudential Statement; or
 - iv. the renewal, extension or other modification of the maturity of the exposure exceeds one year.
 - (b) If an exposure conforms to the limits in paragraph 21 when made but subsequently exceeds the limits because:
 - i. the Financial Institution's capital declines as a result of operating losses; or
 - ii. the borrower merges or forms a common enterprise with another borrower; or
 - iii. the Financial Institution merges with another Financial Institution which also holds exposures to the borrower; or
 - iv. of changes to the lending limits or the method for calculating capital; or
 - v. an exception under paragraph 21 no longer applies then the exposure will be treated as "nonconforming".
22. If an exposure becomes "nonconforming", the Board or senior management are required to act promptly to bring the exposure into compliance unless doing so would adversely affect the ability of the Financial Institution to receive full repayment of the credit.

Other Matters

23. The limits in this Prudential Statement apply to all exposures, including any loans and advances which have been written off in whole or in part, or against which the Financial Institution has raised specific provisions for losses. Loans and advances that have been discharged by a court or that are no longer legally enforceable shall not be included in the total for determining compliance with the limits.
24. Any exposure or portion thereof that has been sold as participation to another Financial Institution shall not count against the limits in this Prudential Statement. For this exception to apply, the participation must be covered by a written agreement which specifies that:

- (a) the interest rate on the portion of the exposure sold under the participation agreement is equal to or less than the interest rate shown in the contract between the lending Financial Institution and the counterparty;
 - (b) the maturity of the portion of the exposure sold under the participation agreement is no longer than the maturity shown in the contract between the lending Financial Institution and the counterparty; and
 - (c) in the event of a default both Financial Institutions will share in payments and recoveries on a pro rata basis according to their respective participation percentages at the time of default.
25. When two or more Financial Institutions grant an exposure to a single borrower under a single credit facility (e.g. a syndicated credit), the limits in this Prudential Statement apply only to the funds provided by each Financial Institution and representing that Financial Institution's pro rata share of the total credit facility. For this exception to apply, the syndication agreement must be in writing and must specify explicitly the terms and exposures of each Financial Institution in the syndicated credit.
26. Accrued but uncollected interest is not subject to the limits in this Prudential Statement. Capitalised interest (that is, interest which has been added to the outstanding principal balance of a credit facility as a result of a renewal or restructuring of the credit facility and which has not been reversed or otherwise suspended from income) however, will be considered when determining compliance with the limits.

CBS Final Authority

27. In cases of uncertainty for purposes of this Prudential Statement, the CBS has the final determination based on the particular facts and circumstances, when exposures nominally granted to one person shall be combined with credits to another person.
28. Notwithstanding the limits in this Prudential Statement, the CBS may, in writing, set specific limits on a Financial Institution's exposures to particular counterparties, groups of counterparties, industry sectors, countries or asset classes, including property holdings and any other investments, on a case-by-case basis, having regard to the Financial Institution's individual circumstances.

Prudential Statement 5

Connected Lending and Activities, and Direct Ownership Interests



Objective and key requirements of this Prudential Statement

This Prudential Statement requires a Financial Institution to adopt policies and procedures to appropriately manage risks associated with:

- financial transactions with insiders, individuals and other parties which are connected through ownership, employment or control of the Financial Institution; and
- using its capital to make direct ownership interests in other financial entities.

The ultimate responsibility for the management of the above risks rests with the Board of Directors.



Contents

Authority	62
Application.....	62
Definitions	62
Board and Senior Management Responsibilities	62
Connected Lending	63
Connected Non-Credit Activities.....	64
Direct Ownership Interests	64
Dealings with Related Entities.....	64
Prior Approval Requirements	65
Notification Requirements.....	65



Authority

This Prudential Statement is made under Section 3 (2) of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act.

Definitions

Insiders ó primarily directors, officers, employees, and those that can influence decision making in the Financial Institution. It also includes in some cases, individuals who through contract, or circumstances can influence decisions or have access to confidential information within the Financial Institution. Circumstances and situations may present additional situations where an individual or individuals could be considered insiders.

Connected Lending ó all forms of direct and indirect credit (on and off balance sheet, loans, investments and claims) exposures of a Financial Institution to individuals or to parties which are connected to that Financial Institution through ownership or control. In the context of direct exposure, it includes a Financial Institution's exposure where a director, officer or shareholder of the Financial Institution is liable jointly or severally or as a guarantor. It also includes a Financial Institution's exposure to any company where it has an equity interest.

Connected lending in the context of indirect exposure includes exposures to any immediate family member of any director, officer or shareholder and to any company, partnership, association or group of individuals whether incorporated or not, wherein any director, officer or shareholder of the Financial Institution has an interest or is a director, partner, manager, member, shareholder, agent or otherwise.

Officer ó Chief Executive Officer, Senior Executives, Managers, Secretary and others who are generally known to be representatives of the Financial Institution.

Shareholder ó a person who owns or who has authority to exercise power over ten percent (10%) or more of the Financial Institution's voting stock.

Connected Activities ó all the elements contained in the definition of connected lending after substituting the language "direct and indirect lending exposures" with the term "non-lending financial transaction".

Board and Senior Management Responsibilities

1. The Board is ultimately responsible for the sound and prudent management of the risks associated with connected lending, connected activities, and direct ownership interests of the Financial Institution.

2. The Board must ensure that the Financial Institution has in place a risk management framework that incorporates the management of risk connected lending, connected activities, and direct ownership interests of the Financial Institution. The Board must approve all aspects of the framework.
3. The senior management must implement a connected lending and activities policy, approved by the Board. The policy must include appropriate processes to identify connected lending and activities; and the additional required steps and conditions under which insiders' activities, both credit and non-credit, are handled. This includes the annual requirement for a conflict of interest statement from all significant parties within the Financial Institution.
4. The Financial Institution must define the term significant parties to include at a minimum senior management, all directors, and majority shareholders.
5. The connected lending and activities policy must address the credit and non-credit approval process for insiders, which will include elevated approval authorizations for all aspects of credit management. Such approvals must include the same level of scrutiny and documentation that is required for non-insiders. The affected insider must not take part in any discussion or voting of the insider transaction.
6. The Board must ensure that terms and conditions provided to insiders are the same as those provided to non-insiders. The Board and management must establish a process that will ensure and demonstrate that insider interest rates, terms and conditions are not preferential.

Connected Lending

7. A Financial Institution must not be used as a funding vehicle or "front" for the operations of "connected" borrowers or any of its associates. It must not give a general guarantee of the repayment of any liability of a "connected" borrower or an associate and should ensure that a "connected" borrower or an associate does not, to up-grade the status of its liabilities, seek to give an impression that the Financial Institution's financial resources stand generally behind, or could be called upon to stand behind, its operations.
8. A Financial Institution's financial dealings with any "connected" borrower or with an associate must be based on normal Financial Institution principles, i.e. Financial Institution would be expected to subject the financial position of a "connected" borrower or an associate to as close a scrutiny as it would in the case of an unrelated customer; and all transactions must be on commercial terms and conditions.
9. Any explicit financial commitment by a Financial Institution to a "connected" borrower or to an associate should be limited as to amount, i.e. it should not be open-ended.
10. A Financial Institution must be able to provide the CBS data in respect to any financial exposure to its "connected" borrowers and its associates.

Connected Non-Credit Activities

11. Connected non-credit activities (connected activities) include the purchase of services and supplies, rentals of equipment, real estate and Financial Institution promises, or any other transaction of a financial nature. Such activities require a higher level of transparency. Any proposed significant connected activities must be approved by a majority of the members of the Board, with any interested director abstaining. Where available and appropriate such proposals should reflect due diligence with other vendors or service providers to ensure and demonstrate that the actions taken are in the best interest of the Financial Institution and not the insider.
12. It is the duty of every director and officer who has an interest in any proposal for connected activities to declare his or her relationship or interest in that proposal. The declaration should be recorded and should form part of the documents relating to the proposal. A director or officer who has made a declaration should not take part in any way in any evaluation, deliberations or decisions relating to that application.

Direct Ownership Interests

13. The Board must adopt a risk appetite statement for direct ownership interests. It must include acceptable and unacceptable Financial Institution ownership interests.
14. A Financial Institution may, with the prior approval of the CBS, invest in other financial intermediaries or companies which are in the field of financial intermediation; or involvement in non-financial areas that are of substantial relevance to Financial Institution operations.
15. A Financial Institution may invest in a wholly owned subsidiary for these same purposes. Such investments must demonstrate a reasonable Financial Institution business need that warrants the investment.
16. The aggregate total for all investments at any one time is limited to ten percent (10%) of the Financial Institution's total capital. For the purposes of this calculation the investment portion of the ratio is the aggregate total of cash or the initial documented market value of non-cash assets used for the investment.

Dealings with Related Entities

17. For the purposes of this Prudential Statement, all entities where the Financial Institution has an equity investment in that entity that is five percent (5%) or greater of the its Total Capital is considered a related entity.
18. Where appropriate, the CBS may deem that other entities (and their subsidiaries) are a related entity of a Financial Institution.

19. The Board must establish, and monitor compliance with, policies governing all dealings with related entities. The policies, including any material changes thereto, must be provided to the CBS if requested.
20. A Financial Institution's policies on related-entity dealings must, at a minimum, include:
 - a) a requirement that the Financial Institution address risks arising from dealings with related entities as strictly as it would address its risk exposures to unrelated entities;
 - b) prudent limits on exposures to related entities at both an individual and aggregate level;
 - c) procedures for resolving any conflict of interest arising from such dealings; and
 - d) requirements relating to the transparency of individual and third-party dealings associated with related entities.
21. Terms or conditions imposed by a Financial Institution in relation to its dealings with related entities that are inconsistent with the benchmark for unrelated entities must be approved by the Board with justifications fully and clearly documented in a register. The Financial Institution must make this register available for inspection by the CBS if so requested.
22. A Financial Institution must not have unlimited exposures to related entities either in aggregate or at an individual entity level (ie a general guarantee of the obligations of a related entity).

Prior Approval Requirements

23. A Financial Institution must request and receive prior approval from the CBS before:
 - (a) entering into a credit exposure with a related party of more than ten percent (10%) of Total Capital;
 - (b) establishing or acquiring a subsidiary;
 - (c) committing to any proposal to acquire (whether directly or indirectly) more than twenty percent (20%) of equity interest in an entity; and
 - (d) taking an equity interest in an entity arising from the work-out of a problem exposure.

Notification Requirements

24. A Financial Institution must report any equity investments that are not subject to the prior approval requirements set out in paragraph 22, in writing, to the CBS within 30 calendar days of undertaking the investment.

Prudential Statement 6

Liquidity Risk



Objectives and key requirements of this Prudential Statement

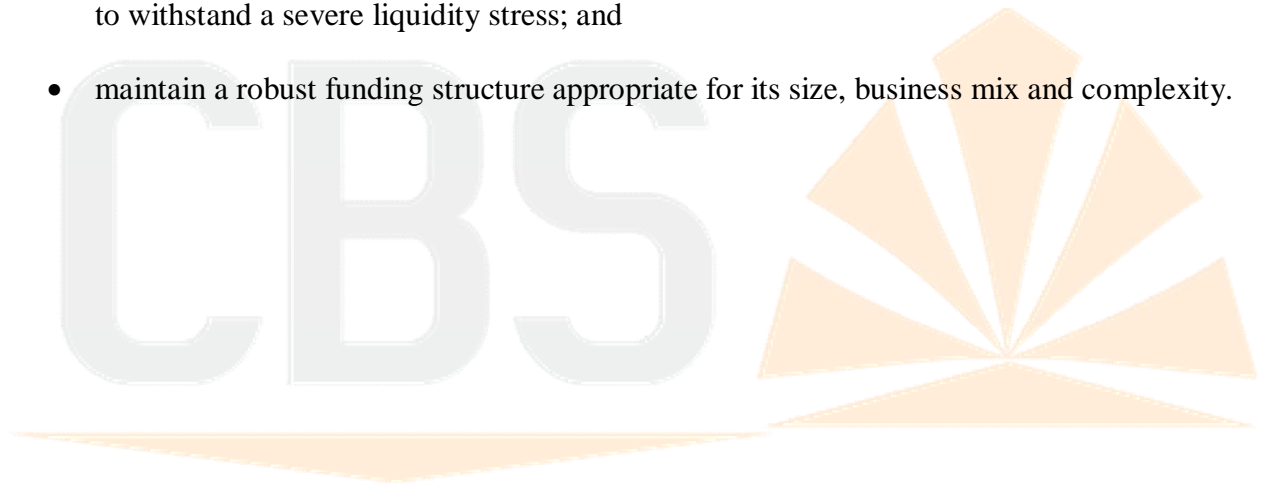
This Prudential Statement requires a Financial Institution to adopt prudent practices in managing its liquidity risks and to maintain an adequate level of liquidity to meet its obligations as they fall due across a wide range of operating circumstances.

That each locally incorporated financial institution must establish and implement an in-house Liquidity Risk Management Policy approved by the Board.

Foreign subsidiary operations may adapt Group Policy but must consider the size, nature and scope of local operation and must include the requirements of this Policy.

The key requirements of this Prudential Statement are that a Financial Institution must:

- have a risk management framework to identify, measure, monitor, and control liquidity risk that is commensurate with the nature, scale and complexity of the institution;
- maintain a portfolio of high-quality liquid assets sufficient in size to enable the institution to withstand a severe liquidity stress; and
- maintain a robust funding structure appropriate for its size, business mix and complexity.



Contents

Authority.....	69
Application.....	69
Definitions	69
Key Principles	69
Board and Senior Management Responsibilities	69
Liquidity Risk Management Framework.....	71
Management of Liquidity Risk	72
Annual Funding Strategy.....	73
Contingency Funding Plan	73
Minimum Quantitative Requirements	74
Stress Testing	74
Attachment A -Minimum Liquidity Holdings (MLH).....	75
Attachment B ó Liquidity Stress Testing using -going concernøscenario	76

Authority

This Prudential Statement is made under, Section 3 (2) of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act.

Definitions

CBS to add definitions from The Banking Act, the Financial Institutions Act, and existing Prudential Statements as appropriate.

Financial Institution a bank entity licensed under the Financial Institutions Act 1996.

Key Principles

1. A Financial Institution is responsible for the sound management of its liquidity risk and must have a robust framework to manage its liquidity risk accordingly.
2. A Financial Institution must always maintain sufficient liquidity to meet its obligations as they fall due and hold a minimum level of high-quality liquid assets (HQLA) to survive a severe liquidity stress.
3. A Financial Institution must ensure that its activities are funded with stable sources of funding on an ongoing basis.
4. A Financial Institution must inform the CBS as soon as possible of any concerns it has about its current or future liquidity, and its plans to address these concerns. If a Financial Institution experiences a severe liquidity stress, it must notify CBS immediately and advise the action that is being taken to address the situation.

Board and Senior Management Responsibilities

5. A Financial Institution's Board of Directors (Board) is ultimately responsible for the sound and prudent management of the liquidity risk of the Financial Institution.
6. A Financial Institution must maintain a liquidity risk management framework commensurate with the level and extent of liquidity risk to which the Financial Institution is exposed from its activities. The Board must approve all aspects of the framework.
7. The liquidity risk management framework must include, at a minimum:
 - a) a statement of the Financial Institution's liquidity risk appetite;
 - b) the liquidity management strategy and policy of the Financial Institution;

- c) the Financial Institution's operating standards (e.g. in the form of policies, procedures and controls) for identifying, measuring, monitoring and controlling its liquidity risk in accordance with its liquidity risk appetite;
 - d) the Financial Institution's funding strategy, and
 - e) a contingency funding plan.
8. The Board must ensure that:
- a) senior management and other relevant personnel have the necessary experience to manage liquidity risk; and
 - b) the Financial Institution's liquidity risk management framework and liquidity risk management practices are documented and reviewed at least annually.
9. The Board must review regular reports on the liquidity of the Financial Institution and, where necessary, information on new or emerging liquidity risks.
10. A Financial Institution's senior management must, at a minimum:
- a) develop a liquidity management strategy, policies and processes in accordance with the Board approved liquidity risk appetite;
 - b) ensure that the Financial Institution maintains sufficient liquidity;
 - c) determine the structure, responsibilities and controls for managing liquidity risk and liquidity positions, and outline these elements clearly in the Financial Institution's liquidity policies;
 - d) develop a liquidity policy that includes review of its 30 and 90-day liquidity position, loan to deposit guidelines and limits, loans to capital limits, and borrowing limits;
 - e) ensure that the Financial Institution has adequate internal controls to enforce the integrity of its liquidity risk management processes;
 - f) ensure that stress tests, contingency funding plans and holdings of HQLA are effective and appropriate for the Financial Institution;
 - g) establish a set of reporting criteria, specifying the scope, manner and frequency of reporting for various recipients and the parties responsible for preparing the reports;
 - h) establish the specific procedures and approvals necessary for exceptions to policies and limits, including the escalation procedures and follow-up actions to be taken for breaches of limits;
 - i) closely monitor current trends and potential market developments that may present challenges for managing liquidity risk so that appropriate and timely changes to the liquidity management strategy can be made as needed; and

- j) continuously review information on the Financial Institution's liquidity developments and report to the Board on a regular basis.
- 11. Senior management and the Board must be able to demonstrate a thorough understanding of the links between funding liquidity risk (the risk that a Financial Institution may not be able to meet its financial obligations as they fall due) and market liquidity risk (the risk that liquidity in financial markets, such as the market for debt securities, may reduce significantly), as well as how other risks, including credit, market, operational and reputation risks, affect the Financial Institution's overall liquidity risk management strategy.

Liquidity Risk Management Framework

- 12. A Financial Institution's liquidity risk appetite defines the level of liquidity risk that the Financial Institution is willing to assume. The liquidity risk appetite must be documented and appropriate for the Financial Institution's operations.
- 13. The liquidity risk appetite must be reviewed, at least annually, to reflect the Financial Institution's financial condition and funding capacity.
- 14. In setting the liquidity risk appetite, the Board and senior management must ensure that the risk appetite allows the Financial Institution to effectively manage its liquidity in such a way that it can withstand a prolonged period of stress.
- 15. A Financial Institution's liquidity risk management framework must be formulated to ensure that the Financial Institution maintains sufficient liquidity, including a cushion of unencumbered HQLA, to withstand a range of stress events, including those involving the loss or impairment of both unsecured and secured funding sources.
- 16. A Financial Institution's liquidity risk management framework must be well integrated into the Financial Institution's overall risk management process.
- 17. The liquidity management strategy must include specific policies on liquidity management, such as:
 - a) the composition and maturity of assets and liabilities;
 - b) the diversity and stability of funding sources;
 - c) acceptable type, duration and limits on borrowings;
 - d) the approach to managing liquidity in different currencies, across borders, and across business lines and legal entities; and
 - e) the approach to intraday liquidity management.
- 18. The liquidity management strategy must be appropriate for the nature, scale and complexity of the Financial Institution. In formulating this strategy, the Financial Institution must consider its legal structure, key business lines, the breadth and diversity of markets, products and jurisdictions in which it operates.
- 19. The liquidity management strategy, key policies for implementing the strategy and the liquidity risk management structure must be communicated throughout the organisation by senior management.

20. A Financial Institution must have adequate policies, procedures and controls in place to ensure that the Board and senior management are informed immediately of new and emerging liquidity concerns. These include increasing funding costs or concentrations, increases in any funding requirements, the lack of availability of alternative sources of liquidity, material and/or persistent breaches of limits, a significant decline in the cushion of unencumbered HQLA, or changes in external market conditions that could signal future difficulties.
21. Senior management must be satisfied that all business units conducting activities that have an impact on liquidity are fully aware of the liquidity management strategy and operate in accordance with approved policies, procedures, limits and controls.
22. The liquidity risk management framework must be subject to effective and comprehensive independent review on an ongoing basis.

Management of Liquidity Risk

23. A Financial Institution must have a sound process for identifying, measuring, monitoring and controlling liquidity risk. This process must include a robust framework for comprehensively projecting cashflows arising from assets, liabilities and off-balance sheet items over an appropriate set of time horizons.
24. A Financial Institution must set limits to control its liquidity risk exposure and vulnerabilities. Limits and corresponding escalation procedures must be reviewed regularly. Limits must be relevant to the business in terms of its location, complexity of activity, nature of products, currencies and markets served.
25. Where a liquidity risk limit is breached, a Financial Institution must implement a plan of action to review the exposure and reduce it to a level that is within the limit.
26. A Financial Institution must actively manage its collateral positions, differentiating between encumbered and unencumbered assets.
27. A Financial Institution must design a set of early warning indicators to aid its daily liquidity risk management processes in identifying the emergence of increased risk or vulnerabilities in its liquidity position or potential funding needs. Such early warning indicators must be structured to assist in the identification of any negative trends in the Financial Institution's liquidity position and lead to an assessment and potential response by management to mitigate the Financial Institution's exposure to these trends.
28. A Financial Institution must have a reliable management information system that provides the Board, senior management and other appropriate personnel with timely and forward-looking information on the liquidity position of the Financial Institution.
29. A Financial Institution must actively manage its intraday liquidity positions and risks to meet payment and settlement obligations on a timely basis under both normal and stressed conditions.

30. A Financial Institution must develop and implement costs and benefits allocation process for funding and liquidity that appropriately apportions the costs of prudent liquidity management to the sources of liquidity risk, and provides appropriate incentives to manage liquidity risk.
31. A Financial Institution active in multiple currencies must:
 - a) maintain HQLA consistent with the distribution of its liquidity needs by currency;
 - b) assess its aggregate foreign currency liquidity needs and determine an acceptable level of currency mismatches; and
 - c) undertake a separate analysis of its strategy for each currency in which it has material activities, considering potential constraints in times of stress.

Annual Funding Strategy

32. A Financial Institution must:
 - (a) develop and document an annual funding strategy, which must be provided to the CBS on request;
 - (b) maintain an ongoing presence in its chosen funding markets and strong relationships with funds providers; and
 - (c) regularly gauge its capacity to raise funds quickly. It must identify the main factors that affect its ability to raise funds and monitor those factors closely to ensure that estimates of fund-raising capacity remain valid.
33. The annual funding strategy must be approved by the Board and supported by robust assumptions in line with the Financial Institution's liquidity management strategy and business objectives.
34. The funding strategy must be reviewed on a regular basis and updated as necessary for changed funding conditions or a change in the Financial Institution's strategy.
35. A Financial Institution must advise the CBS of any material changes to the Financial Institution's funding strategy.

Contingency Funding Plan

36. A Financial Institution must have a formal contingency funding plan that clearly sets out the strategies for addressing liquidity shortfalls in emergency situations. The plan must outline policies to manage a range of stress environments, establish clear lines of responsibility, include clear invocation and escalation procedures and be regularly tested and updated to ensure that it is operationally robust.
37. A Financial Institution's contingency funding plan must be commensurate with its complexity, risk profile, scope of operations and role in the financial systems in which it operates. The plan must articulate available contingency funding sources and the amount of funds a Financial Institution estimates can be derived from these sources, clear escalation and

prioritisation procedures detailing with when and how each of the actions can and must be activated, and the lead time needed to tap additional funds from each of the contingency sources.

38. The contingency funding plan must provide a framework with a high degree of flexibility so that a Financial Institution can respond quickly in a variety of situations.
39. The plan's design, scope and procedures must be closely integrated with the Financial Institution's ongoing analysis of liquidity risk and with the assumptions used in its stress tests and the results of those stress tests. As such, the plan must address issues over a range of different time horizons, including intraday.
40. The plan must address a retail deposit run and must include measures to repay retail depositors as soon as practicable. The retail run contingency plan must not rely upon closing distribution channels to retail depositors. The retail run contingency plan must seek to ensure that in the event of a loss of market confidence in the Financial Institution, retail depositors wishing to retrieve their deposits may do so as quickly and as conveniently as is practicable in the circumstances, and within the contractual terms and conditions applicable to the relevant deposit products.
41. A Financial Institution's contingency funding plan must be reviewed and tested regularly to ensure its effectiveness and operational feasibility.
42. A Financial Institution must review and update its plan at least annually for the Board's approval, or more often as changing business or market circumstances require.

Minimum Quantitative Requirements

43. A Financial Institution is required to maintain a minimum liquidity holding (MLH) of ten percent (10%) of its liabilities in specified liquid assets, as described in Attachment A.
44. A Financial Institution is required to meet this minimum quantitative requirement on a continuous basis.
45. Where the CBS is not satisfied with the adequacy of a Financial Institution's liquidity management framework or where it has particular concerns about a Financial Institution's liquidity, it may require the Financial Institution to hold a higher specified amount of liquid assets.

Stress Testing

46. Financial Institutions must complete going concern scenario analysis. The going concern scenario requires a Financial Institution to model the expected behaviour of cashflows in the ordinary course of business for a future period at least equal to 12 months, as described in Attachment B.

Attachment A -Minimum Liquidity Holdings (MLH)

- 1) A Financial Institution is required to maintain a portfolio of liquid assets (referred to as minimum liquidity holdings (MLH)) of ten percent (10%) of its liabilities in specified liquid assets, as defined in paragraph 3 of this Attachment.
- 2) For this Prudential Statement, liabilities are defined as total on-balance sheet liabilities and irrevocable commitments (except where approved for a prudential purpose by CBS).
- 3) For the MLH requirement, liquid assets must be free from encumbrances (except where approved for a prudential purpose by the CBS) and include:
 - (a) notes and coin and settlement funds;
 - (b) debt securities guaranteed by the Samoan Government;
 - (c) debt securities issued by supranational and foreign governments;
 - (d) Financial Institution bills, certificates of deposits (CDs) and debt securities;
 - (e) deposits (at call and any other deposits readily convertible into cash within two business days) held with other Financial Institutions net of placements by other Financial Institutions; and
 - (f) any other securities approved by the CBS.
- 4) All debt securities must be eligible for repurchase agreement with the CBS and must not be subordinated.
- 5) A Financial Institution must ensure it has the operational capacity to liquidate any securities held as liquid assets within two business days.
- 6) Notwithstanding paragraph 1 of this Attachment, the CBS may, where it is not satisfied with the adequacy of a Financial Institution's liquidity management framework, or where it has particular concerns about a Financial Institution's liquidity, require the Financial Institution to hold a higher amount of liquid assets, as defined in paragraph 3 of this Attachment.
- 7) To ensure that the MLH requirement is not breached, a Financial Institution must set a trigger ratio above its MLH requirement and must ensure that it manages its liquidity in accordance with its trigger ratio.
- 8) A Financial Institution must inform the CBS immediately when it becomes aware that its liquid assets may fall below its MLH requirement and advise the CBS of the remedial action taken or planned to restore its liquidity position above its MLH requirement.

Attachment B – Liquidity Stress Testing using ‘going concern’ scenario

- 1) Financial Institutions must address a ‘going-concern’ scenario, which refers to the normal behaviour of cashflows in the ordinary course of business. A Financial Institution’s going concern reporting must show how obligations and commitments are met on a day-to-day basis.
- 2) To demonstrate that a Financial Institution can meet commitments and obligations under normal operating conditions, the deficits reported under the ‘going concern’ scenario (up to 12 months) must not exceed the Financial Institution’s normal capacity to fund.
- 3) Scenario analysis reports provided to the CBS under the ‘going concern’ scenario must take the form of maturity profiles of cashflows (in domestic and foreign currencies separately) based on assumptions agreed with CBS.

Scenario analysis depends heavily on the assumptions of future cashflows associated with the behaviour of a Financial Institution’s assets, liabilities and off-balance sheet activities under different operating scenarios. CBS recognises that considerable judgement and discretion is involved in making these underlying assumptions, which may vary substantially among Financial Institutions depending on their individual business profiles. A Financial Institution is expected to take a conservative approach in assessing future cashflows. CBS will assess the suitability of the assumptions made. A Financial Institution must be able to provide analysis and evidence to justify the assumptions underlying this scenario. CBS may require, where it is not satisfied with the suitability of a Financial Institution’s assumptions, that the Financial Institution revise those assumptions as directed by the CBS.

- 4) A Financial Institution must document in its liquidity management policy statement the underlying assumptions adopted for its scenario analyses. The assumptions must be subject to regular review to take account of changes in the Financial Institution’s operations and market environment. A Financial Institution must consult the CBS prior to making any material changes to these agreed assumptions.

Prudential Statement 7

Business Continuity Management



Objectives and key requirements of this Prudential Statement

This Prudential Statement requires each Financial Institution to implement a whole-of-business approach to business continuity management that is appropriate to the size and complexity of its operations. Business continuity management increases resilience to business disruption arising from internal and external events and may reduce the impact on the Financial Institution's reputation, profitability and depositors.

The key requirements of this Prudential Statement are that:

- a Financial Institution must identify, assess and manage business continuity risks;
- a Financial Institution must develop and maintain a Business Continuity Plan; and
- a Financial Institution must notify the CBS in the event of certain disruptions.



Contents

Authority.....	80
Application.....	80
Definitions	80
The Role of the Board and Senior Management.....	80
Business Continuity Management.....	81
BCM Policy	81
Business Impact Analysis	82
Recovery Objectives and Strategies.....	82
Business Continuity Planning.....	82
Review and Testing of BCP.....	83
Audit Arrangements	83

Authority

This Prudential Statement is made under Section 3(2) of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act.

Definitions

Business Continuity Management ó a whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimize the operational, financial, legal, reputational and other material consequences arising from a disruption.

Business Impact Analysis ó it is a dynamic process for identifying critical operations and services, key internal and external dependencies and appropriate resilience levels. It assesses the risks and potential impact of various disruption scenarios on an institution's operations and reputation.

Recovery Strategy ó sets out recovery objectives and priorities that are based on the business impact analysis. Among other things, it establishes targets for the level of service the institution would seek to deliver in the event of a disruption and the framework for ultimately resuming business operations.

Business Continuity Plan ó detailed guidance for implementing the recovery strategy. They establish the roles and allocate responsibilities for managing operational disruptions and provide clear guidance regarding the succession of authority in the event of a disruption that disables key personnel. They also clearly set out the decision-making authority and define the triggers for invoking the Plan.

Critical business operations ó the business functions, resources and infrastructure that may, if disrupted, have a material impact on the Financial Institution's business functions, reputation or profitability, and as such depositors' interests.

Business disruption ó any interruption to normal business working conditions that may have a material impact on the Financial Institution's business functions, reputation or profitability, and as such depositors' interests.

The Role of the Board and Senior Management

1. A Financial Institution must identify, measure, monitor and control potential business continuity risks to ensure that it can meet its financial obligations to its depositors.
2. A Financial Institution's Board and senior management are collectively responsible for the institution's business continuity.

3. The Board must approve the Financial Institution's Business Continuity Management Policy (BCM Policy).
4. BCM should be an integral part of the overall risk management program of a Financial Institution.
5. The Board must ensure that the Financial Institution's business continuity risks and controls are considered as part of its overall risk management systems and when completing a risk management declaration required to be provided to CBS⁴.

Business Continuity Management

6. BCM is a whole-of-business approach that includes policies, standards and procedures for ensuring that critical business operations are maintained or recovered in a timely fashion, in the event of a disruption. Its purpose is to minimize the financial, legal, regulatory, reputational and other material consequences arising from a disruption.
7. A Financial Institution's BCM must, at a minimum, include:
 - a) a BCM Policy in accordance with paragraphs 9 and 10;
 - b) a business impact analysis (BIA) including risk assessment in accordance with paragraphs 11 and 12;
 - c) recovery objectives and strategies; in accordance with paragraphs 13 and 14;
 - d) a business continuity plan (BCP) including crisis management and recovery in accordance with paragraphs 15 to 18; and
 - e) programs for:
 - i. review and testing of the BCP in accordance with paragraph 19; and
 - ii. training and ensuring awareness of staff in relation to BCM.

BCM Policy

8. A Financial Institution must have an up-to-date documented BCM Policy that sets out its objectives and approach in relation to BCM.
9. The BCM Policy must clearly state the roles, responsibilities and authorities to act in relation to the BCM Policy.

⁴ Refer to *Prudential Statement Governance and Risk Management*

Business Impact Analysis

10. A BIA involves identifying all critical business functions, resources and infrastructure of the Financial Institution and assessing the impact of a disruption on these.
11. When conducting the BIA, the Financial Institution must consider:
 - a) plausible disruption scenarios over varying periods of time;
 - b) the period of time for which the Financial Institution could not operate without each of its critical business operations;
 - c) the extent to which a disruption to the critical business operations might have a material impact on the interests of depositors of the Financial Institution; and
 - d) the financial, legal, regulatory and reputational impact of a disruption to a Financial Institution & critical business operations over varying periods of time.

Recovery Objectives and Strategies

12. Recovery objectives are pre-defined goals for recovering critical business operations to a specified level of service (recovery level) within a defined period (recovery time) following a disruption.
13. A Financial Institution must identify and document appropriate recovery objectives and implementation strategies based on the results of the BIA and the size and complexity of the Financial Institution.

Business Continuity Planning

14. A Financial Institution must maintain at all times a documented BCP that meets the objectives of the BCM Policy.
15. A copy of the Plan must be maintained at an off-site location readily available in the event of a disruption.
16. The BCP must document procedures and information that enable the Financial Institution to:
 - a) manage an initial business disruption (crisis management); and
 - b) recover critical business operations.
17. The BCP must reflect the specific requirements of the Financial Institution and must identify:
 - a) critical business operations;
 - b) recovery levels and time targets for each critical business operation;

- c) recovery strategies for each critical business operation;
- d) infrastructure and resources required to implement the BCP;
- e) roles, responsibilities and authorities to act in relation to the BCP; and
- f) communication plans with staff and external stakeholders.

Review and Testing of BCP

- 18. A Financial Institution must review and test its BCP at least annually, or more frequently if there are material changes to business operations, to ensure that the BCP can meet the BCM objectives. The results of the testing must be formally reported to the Board or to delegated management.
- 19. The BCP must be amended to fix any problems or issues identified as part of the review and testing required under paragraph 21.

Audit Arrangements

- 20. A Financial Institution's internal audit function, or an external expert, must periodically review the BCP and provide an assurance to the Board or to delegated management that:
 - a) the BCP is in accordance with the Financial Institution's BCM Policy and addresses the risks it is designed to control; and
 - b) testing procedures are adequate and have been conducted satisfactorily.
- 21. The CBS may request the external auditor of the Financial Institution, or another appropriate external expert, to provide an assessment of the Financial Institution's BCM arrangements. Any such report must be paid for by the Financial Institution and must be made available to the CBS.

Prudential Statement 8

Outsourcing

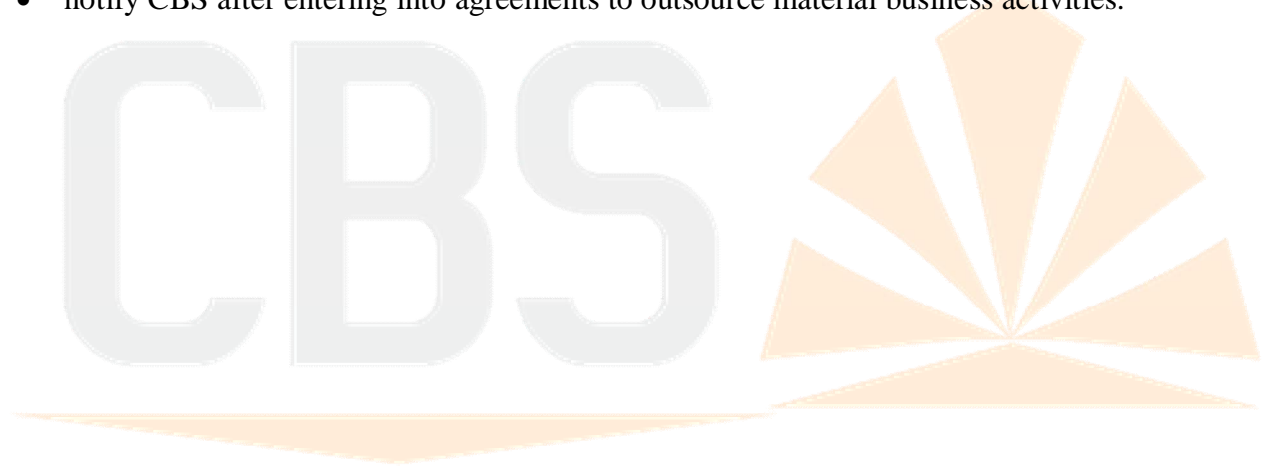


Objectives and key requirements of this Prudential Statement

This Prudential Statement requires that all outsourcing arrangements involving material business activities entered into by a Financial Institution be subject to appropriate due diligence, approval and ongoing monitoring. All risks arising from outsourcing material business activities must be appropriately managed to ensure that the Financial Institution is able to meet its financial obligations to its depositors.

The key requirements of this Prudential Statement are that a Financial Institution must:

- maintain an outsourcing policy covering material business activities;
- have effective policies and procedures in place to manage the outsourcing of material business activities;
- consult with CBS prior to entering agreements to outsource material business activities to service providers that conduct their activities outside Samoa; and
- notify CBS after entering into agreements to outsource material business activities.



Contents

Authority.....	87
Application.....	87
Definitions	87
Materiality.....	87
The Role of the Board and Senior Management.....	88
Outsourcing Policy.....	88
Assessment of Outsourcing Options	88
The Outsourcing Agreement.....	89
CBS Access to Service Providers	90
Notification Requirement	90
Offshoring Arrangements ó Requirement for Consultation	91
Monitoring the Relationship.....	91
Audit Arrangements	91

Authority

This Prudential Standard is made under Section 3 (2) of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act.

Definitions

Material Business Activity is one that has the potential, if disrupted, to have a significant impact on the Financial Institution's business operations or its ability to manage risks effectively, having regard to such factors as:

- the financial and operational impact and impact on reputation of a failure of the service provider to perform over a given period of time;
- the cost of the outsourcing arrangement as a share of total costs;
- the degree of difficulty, including the time taken, in finding an alternative service provider or bringing the business activity in-house;
- the ability of the Financial Institution or member of the group to meet regulatory requirements if there are problems with the service provider;
- potential losses to the Financial Institution's or group's customers and other affected parties in the event of a service provider failure; and
- affiliation or other relationship between the Financial Institution or group and the service provider.

Outsourcing is entering into an arrangement with another party (including a related entity) to perform, on a continuing basis, a material business activity that currently is, or could be, undertaken by the institution itself.

Offshoring is means the outsourcing of a material business activity where the outsourced activity is to be conducted outside Samoa. Offshoring includes arrangements where the service provider is incorporated in Samoa, but the physical location of the outsourced activity is outside Samoa. Offshoring does not include arrangements where the physical location of an outsourced activity is within Samoa but the service provider is not incorporated in Samoa.

Materiality

1. This Prudential Statement only applies to the outsourcing of a material business activity as defined in this Prudential Statement.

2. For the purposes of this Prudential Statement, the internal audit function is a material business activity.

The Role of the Board and Senior Management

3. A Financial Institution must identify, measure, monitor and control risks associated with outsourcing to meet the institution's obligations to its depositors.
4. A Financial Institution must have procedures to ensure that all the institution's relevant business units are aware of the outsourcing policy, and have processes and controls for monitoring compliance with the policy.
5. The Board is ultimately responsible for oversight of any outsourcing arrangement.
6. The Board must approve the institution's outsourcing policy.
7. The Board of a Financial Institution must ensure that outsourcing risks and controls are taken into account as part of the institution's risk management strategy and when completing a risk management declaration required to be provided to the CBS.
8. The Board and senior management must provide all information relating to any outsourced material business activity to the CBS upon request.

Outsourcing Policy

9. The senior management is responsible for developing and implementing an outsourcing policy that sets out the approach to outsourcing of material business activities, including a detailed framework for managing all such outsourcing arrangements.
10. The outsourcing policy must set out specific requirements in relation to outsourcing to related bodies corporate and outsourcing to service providers conducting the material business activity outside Samoa.

Assessment of Outsourcing Options

11. A Financial Institution must be able to demonstrate to the CBS that, in assessing the options for outsourcing, it has:
 - (a) prepared a business case for outsourcing the material business activity;
 - (b) undertaken a transparent competitive selection process;
 - (c) undertaken due diligence on the chosen service provider, including the ability of the service provider to conduct the business activity on an ongoing basis;
 - (d) involved the Board in approving the agreement;

- (e) considered all the matters outlined in paragraph 14, that must, at a minimum, be included in the outsourcing agreement itself;
 - (f) established procedures for monitoring performance under the outsourcing agreement on a continuing basis;
 - (g) addressed the renewal process for outsourcing agreements and how the renewal will be conducted; and
 - (h) developed contingency plans that would enable the outsourced business activity to be provided by an alternative service provider or brought in-house if required.
12. A Financial Institution must be able to demonstrate to the CBS that, in assessing the options for outsourcing to related bodies corporate, it has taken into account:
- (a) the changes to the risk profile of the business activity that arise from outsourcing the activity to a related body corporate and how this changed risk profile is addressed within the institution's risk management framework;
 - (b) that the related body corporate has the ability to conduct the business activity on an ongoing basis;
 - (c) the required monitoring procedures to ensure that the related body corporate is performing effectively and how potential inadequate performance would be addressed;
 - (d) contingency issues in accordance with Prudential Statement - Business Continuity Management should the outsourced activity need to be brought in-house; and
 - (e) the need to apply any of the requirements set out in paragraph 15 to the extent they are relevant to outsourcing agreements with related bodies corporate.

The Outsourcing Agreement

13. Each outsourcing arrangement must be a documented legally binding agreement. The agreement must be signed by all parties to it before the outsourcing arrangement commences.
14. At a minimum, the agreement must address the following matters:
- (a) the scope of the arrangement and services to be supplied;
 - (b) commencement and end dates;
 - (c) review provisions;
 - (d) pricing structure;
 - (e) service levels and performance requirements;

- (f) the form in which data is to be kept and clear provisions identifying ownership and control of data;
 - (g) reporting requirements, including content and frequency of reporting;
 - (h) audit and monitoring procedures; business continuity management;
 - (i) confidentiality, privacy and security of information;
 - (j) default arrangements and termination provisions;
 - (k) dispute resolution arrangements;
 - (l) liability and indemnity;
 - (m) sub-contracting;
 - (n) insurance; and
 - (o) offshoring arrangements (including through subcontracting).
15. A Financial Institution that outsources a material business activity must ensure that its outsourcing agreement includes an indemnity to the effect that any sub-contracting by a third-party service provider of the outsourced function will be the responsibility of the third-party service provider, including liability for any failure on the part of the sub-contractor.

CBS Access to Service Providers

16. An outsourcing agreement must include a clause that allows the CBS access to documentation and information related to the outsourcing arrangement. The outsourcing agreement must include the right for the CBS to conduct on-site visits to the service provider if CBS considers this necessary in its role as prudential supervisor.
17. Where a Financial Institution enters an outsourcing arrangement with a related body corporate, the Financial Institution must ensure that access by the CBS to the related body corporate is not impeded.
18. A Financial Institution must take all reasonable steps to ensure that a service provider will not disclose or advertise that the CBS has conducted an on-site visit, except as necessary to coordinate with other institutions regulated by the CBS that are existing clients of the service provider.

Notification Requirement

19. A Financial Institution must notify the CBS as soon as possible after entering into an outsourcing agreement, and in any event no later than 20 business days after execution of

the outsourcing agreement. This notification requirement applies to all outsourcing of material business activities.

20. When a Financial Institution notifies the CBS of a new outsourcing agreement, it must also provide a summary to the CBS of the key risks involved in the outsourcing arrangement and the risk mitigation strategies put in place to address these risks.

Offshoring Arrangements – Requirement for Consultation

21. A Financial Institution must consult with the CBS prior to entering into any offshoring agreement involving a material business activity so that the CBS may satisfy itself that the impact of the offshoring arrangement has been adequately addressed as part of the institution's risk management framework.
22. If, in the CBS's view, the offshoring agreement involves risks that the Financial Institution is not managing appropriately, the CBS may require the Financial Institution to make other arrangements for the outsourced activity.

Monitoring the Relationship

23. A Financial Institution must ensure the institution has sufficient and appropriate resources to manage and monitor each outsourcing relationship. The type and extent of resources required will depend on the materiality of the outsourced business activity. At a minimum, monitoring must include:
 - (a) maintaining regular contact with the service provider; and
 - (b) a process for regular monitoring of performance under the agreement, including meeting criteria concerning service levels.
24. A Financial Institution must advise the CBS of any significant problems that have the potential to materially affect the outsourcing arrangement and, as a consequence, materially affect the business operations, profitability or reputation of the institution.
25. Where an outsourcing agreement is terminated, a Financial Institution must notify the CBS as soon as practicable and provide a statement about the transition arrangements and future strategies for carrying out the outsourced material business activity.

Audit Arrangements

26. A Financial Institution's internal audit function must review any proposed outsourcing arrangement and regularly review and report to the Board on compliance with the institution's outsourcing policy.
27. The CBS may request the external auditor of an institution, or an appropriate external expert, to provide an assessment of the risk management processes in place with respect to an arrangement to outsource a material business activity. Such reports will be paid for by the institution and must be made available to the CBS.

Prudential Statement 9

Audit



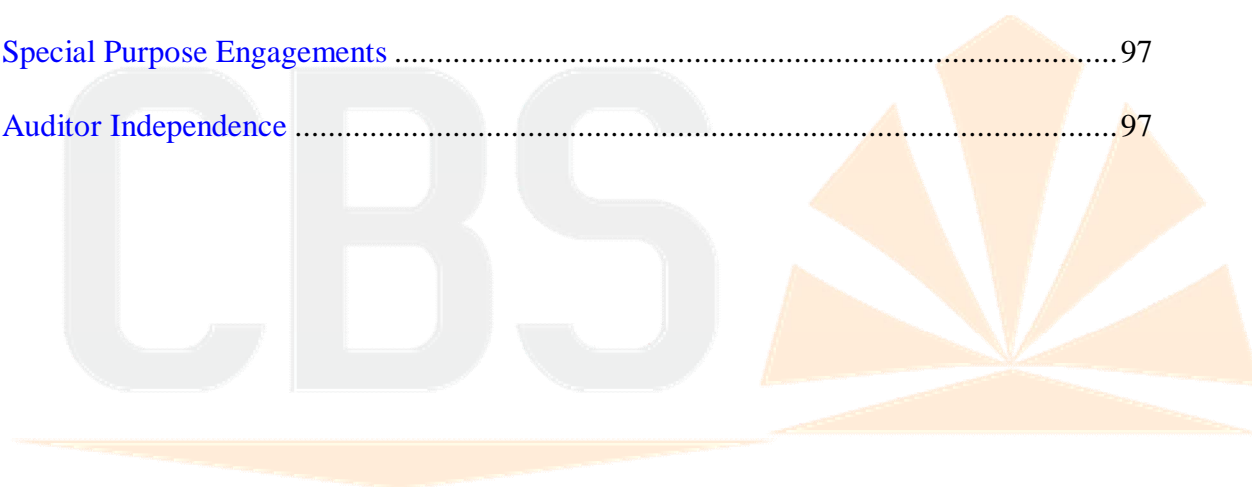
Objectives and key requirements of this Prudential Statement

This Prudential Statement requires Financial Institutions to establish appropriate external audit arrangements, in relation to the operations of the institution. The audit arrangements of Financial Institutions must consider the size, complexity and risk profile of the institution.



Contents

Authority.....	95
Application.....	95
Definitions	95
General Requirements	95
Fitness and Propriety of the Appointed Auditor	95
Obligations of a Financial Institution.....	96
Meetings with the Appointed Auditor.....	96
Responsibilities of the Appointed Auditor	96
Special Purpose Engagements	97
Auditor Independence	97



Authority

This Prudential Statement is made under Section 3 (2) of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act.

Definitions

Financial Institution ó Financial Institution entity licensed under the Financial Institutions Act 1996.

General Requirements

1. A Financial Institution must obtain an annual certified financial audit in accordance with Samoa Company Law.
2. For the purposes of this Prudential Statement, a Financial Institution must appoint an auditor - the appointed auditor. The appointed auditor must be a member of the Samoa Institute of Accountants (SIA) and/or must have Temporary Certificate of Public Practice (TCPP) to do auditing in Samoa.
3. A Financial Institution must set out the terms of engagement of the appointed auditor in a legally binding contract between the Financial Institution and the appointed auditor. The Financial Institution must ensure the terms of engagement require the appointed auditor to fulfil the roles and responsibilities of the appointed auditor as specified in this Prudential Statement.
4. The costs of preparing and submitting reports, documents and other material required by this Prudential Statement, whether routinely or as part of a special purpose engagement, must be borne by the Financial Institution.

Fitness and Propriety of the Appointed Auditor

5. A Financial Institution must ensure that its appointed auditor:
 - a) is a fit and proper person in accordance with the Financial Institution's fit and proper policy as required by Prudential Statement ó Governance and Risk Management; and
 - b) satisfies the auditor independence requirements in this Prudential Statement.

Obligations of a Financial Institution

6. A Financial Institution, if requested by the CBS, must provide the CBS with the terms of engagement, other instructions or correspondence, as well as audit reports and management letters, prepared by the appointed auditor, in relation to the Financial Institution.
7. A Financial Institution must ensure that the appointed auditor has access to all data, information, reports and staff of the Financial Institution that the appointed auditor reasonably believes is necessary to fulfil its role and responsibilities under this Prudential Statement.
8. A Financial Institution must ensure that its appointed auditor is fully informed of all prudential requirements applicable to the Financial Institution. Prudential requirements include requirements imposed by the Financial Institutions Act and prudential statements, conditions on authority and any other requirements imposed by CBS, in relation to a Financial Institution. In addition, the Financial Institution must ensure that the appointed auditor is provided with any other information CBS has provided to the Financial Institution that may assist the appointed auditor in fulfilling its role and responsibilities under this Prudential Statement.
9. A Financial Institution must ensure that the following are provided to its Board or Board Audit Committee:
 - a) reports provided by the appointed auditor in accordance with this Prudential Statement, and any associated assessments and other material provided by an appointed auditor to the Financial Institution on request;
 - b) commentary or responses provided by the CBS to the Financial Institution on reports provided by the appointed auditor, and any associated assessments and other material; and
 - c) any commentary or response on the reports, associated assessments and other material provided by the appointed auditor that are given to the CBS by the Financial Institution.

Meetings with the Appointed Auditor

10. The CBS and an appointed auditor may meet, at any time, on a bilateral basis at the request of either party.
11. Where a Financial Institution is a subsidiary of a foreign financial institution, the CBS may meet with the head entity external auditor and internal auditor.
12. It is also the responsibility of the appointed auditor to supply all information and documents requested by the CBS relevant to the Financial Institution.

Responsibilities of the Appointed Auditor

13. Appointed Auditors must within 3 months of the annual balance date of a Financial Institution, provide simultaneously to the CBS and the Financial Institution's Audit Committee, a report up to the latest balance date detailing the auditor's opinions as to whether:

- a) the Financial Institution has observed all prudential statement requirements;
- b) the statistical and financial data provided by the Financial Institution to the CBS are reliable; and
- c) any matters which, in the auditor's opinion, may have the potential to prejudice materially the financial condition of the Financial Institution.

Special Purpose Engagements

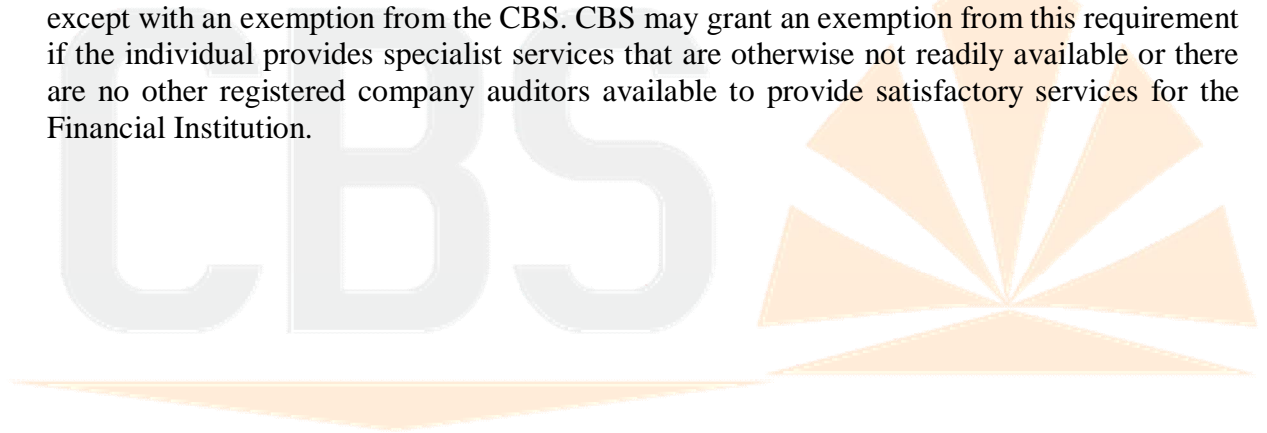
14. The CBS may require a Financial Institution, by notice in writing, to appoint an auditor, who may be the existing appointed auditor or another auditor, to provide a report on an aspect of the Financial Institution's operations, prudential reporting, risk management systems or financial position. Such a special purpose engagement report will normally be requested following consultation with the Financial Institution. However, the CBS may request such a report without prior consultation with a Financial Institution.

Auditor Independence

15. The Board of the Financial Institution must undertake steps to satisfy themselves that the appointed auditor is independent of the Financial Institution and that there is no conflict of interest that could compromise, or be seen to compromise, the independence of the appointed auditor.
16. As part of the process of ascertaining the independence of the appointed auditor, a Financial Institution must obtain a declaration from the auditor to the effect that the auditor is independent, both in fact and appearance, and has no conflict of interest, and that there is nothing to the auditor's knowledge (either in relation to the individual auditor or any audit firm or audit company of which the auditor is a member or director) that could compromise that independence.
17. For the purposes of this Prudential Statement, a conflict of interest situation exists in relation to a Financial Institution at a time, if because of circumstances that exist at that time:
- a) the appointed auditor is not capable of exercising objective and impartial judgement in relation to the conduct of the work that is undertaken for the Financial Institution in relation to the Financial Institutions Act, Prudential Statements or the prudential reporting requirements; or
 - b) a reasonable person, with full knowledge of all relevant facts and circumstances, would conclude that the appointed auditor is not capable of exercising objective and impartial judgement in relation to undertaking the work for the Financial Institution for the purposes of the Financial Institutions Act, Prudential Statements or the prudential reporting requirements.
18. A person, who was a partner of an audit firm or a director of an audit company, and who served in a professional capacity in the audit of a Financial Institution in relation to the Financial Institutions Act, Prudential Statements or the prudential reporting requirements,

cannot be appointed to the role of director or senior manager of that Financial Institution until at least two years have passed since they served in that professional capacity.

19. A person, who was an employee of an audit company and who acted as the lead auditor or review auditor in the audit of a Financial Institution in relation to the Financial Institutions Act, Prudential Statements or the prudential reporting requirements, cannot be appointed to the role of director or senior manager of that Financial Institution until at least two years have passed since they acted as the lead auditor or review auditor.
20. A person cannot be appointed as a director or senior manager of a Financial Institution if there is already another person employed as a director or senior manager of the Financial Institution who was a director of the audit company or a member of the audit firm, at a time when the audit company or audit firm undertook an audit of the Financial Institution at any time during the previous two years.
21. An individual who plays a significant role in the audit of a Financial Institution in relation to the Financial Institutions Act, Prudential Statements or the prudential reporting requirements, for five successive years, or for more than five years out of seven successive years, cannot continue to play a significant role in the audit until at least a further two years have passed, except with an exemption from the CBS. CBS may grant an exemption from this requirement if the individual provides specialist services that are otherwise not readily available or there are no other registered company auditors available to provide satisfactory services for the Financial Institution.



Prudential Statement 10

Foreign Exchange Risk

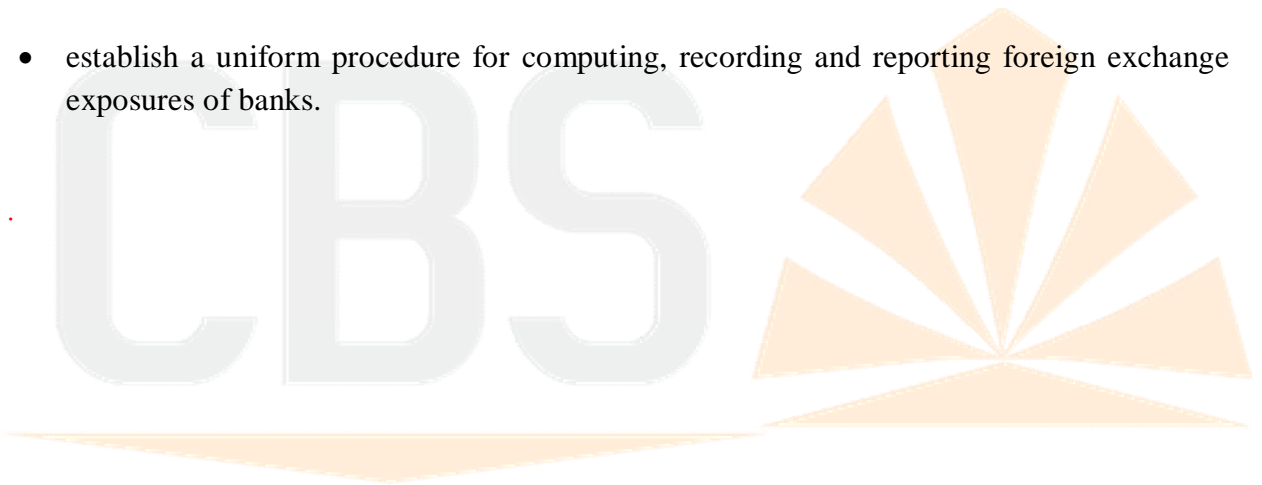


Objectives and key requirements of this Prudential Statement

This Prudential Statement provides the guidelines on the management of foreign exchange risk and settlement risk; and sets out the maximum limits for foreign currency net open positions; and reporting requirements in relation to prudent management of foreign currency exposures of licensed commercial banks.

The key requirements of this Prudential Statement are that a Financial Institution must:

- closely monitor foreign exchange risk within prudent limits on its overnight net open positions in foreign currencies.
- ensure that they have in place adequate foreign exchange risk management systems, appropriate operational guidelines and internal controls intended to identify, measure, monitor and mitigate foreign exchange risk and settlement risk; and
- establish a uniform procedure for computing, recording and reporting foreign exchange exposures of banks.



Contents

Authority.....	102
Application.....	102
Definitions	102
Board Responsibilities.....	103
Senior Management Responsibilities	103
Foreign Exchange Risk Management Framework.....	104
Foreign Exchange Risk Management Policy.....	104
Risk Measurement and Reporting Systems	105
Control of Foreign Exchange Activities	106
Foreign Exchange Limits.....	106
Measurement of Foreign Currency Net Open Positions.....	107
Limits on Net Open Positions in Foreign Currencies.....	108
Foreign Exchange Settlement Risk Management	108
Internal Audit	109
Contingency Plan	110

Authority

This Prudential Standard is made under Section 3 (2) of the Financial Institutions Act 1996 (the Financial Institutions Act).

Application

This Prudential Statement applies to all institutions licensed under Financial Institutions Act.

Definitions

Financial Institution ó bank entity licensed under the Financial Institutions Act 1996.

‘Foreign Exchange Risk’ means the risk of financial loss to a bank arising from adverse movements in foreign exchange rates.

‘Foreign Exchange Settlement Risk’ the risk of financial loss to a bank when it pays the currency it sold but does not receive the currency it bought in a foreign exchange transaction.

‘Foreign Currency Open Position’ means for an individual foreign currency, assets denominated in that currency minus liabilities denominated in that currency. A foreign currency position of zero is referred to as a closed foreign currency position. A positive or negative foreign currency position is referred to as an open foreign currency position.

‘Intra-day’ means between the opening of any business day until the close of business of that same day.

‘Long Position’ means an open currency position for an individual currency where assets denominated in that currency exceed liabilities denominated in that currency, plus the impact of off-balance sheet items

‘Overall Foreign Currency Open Position’ means the higher in absolute terms of either the sum of all short foreign currency positions or the sum of all long foreign currency positions.

‘Overnight Net Open Position’ means the holdings of any net open positions in foreign currencies of a bank at the close of each business day.

‘Short Position’ means an open foreign currency position for an individual foreign currency where liabilities denominated in that currency exceed assets denominated in that currency, plus the impacts of off-balance sheet items.

Board Responsibilities

1. The board has the ultimate responsibility for ensuring that the bank has in place a foreign exchange risk management policy. The responsibilities of the Board or its proxy, at the minimum include:
 - a) approve policies, processes and procedures on foreign exchange risk management;
 - b) approve risk appetite and set limits for foreign exchange exposures and activities;
 - c) ensure that the bank has in place adequate internal audit coverage of the foreign exchange operation;
 - d) ensure the selection and appointment of qualified and competent management to administer the foreign exchange function; and
 - e) determine the report submission intervals and frequency by senior management on foreign exchange activities and the management of exposure to foreign exchange risk.

Senior Management Responsibilities

2. While the ultimate responsibility for foreign exchange risk management lies with the board, the senior management of the bank is responsible to formulate policies, processes and procedures, and implement these upon board approval. The responsibilities of the senior management should, at the minimum:
 - a) develop and document appropriate foreign exchange risk management policies, processes and procedures for approval by the board;
 - b) ensure that foreign exchange risk is managed and controlled within the approved foreign exchange risk framework;
 - c) establish prudent limits on the bank's exposure to foreign exchange risk;
 - d) develop and implement techniques to address the bank's exposure to foreign exchange risk and its foreign exchange gains and losses;
 - e) ensure effective segregation of duties between trading, risk measurement and monitoring, settlement and accounting functions;
 - f) establish and implement procedures governing the conduct and practices of foreign exchange dealers;
 - g) develop lines of communication to ensure timely dissemination of foreign exchange risk management policies, processes and procedures to officers involved in foreign exchange activities and foreign exchange risk management process;
 - h) provide reports on foreign exchange activities and foreign exchange risk management to the Board, at the frequency as determined by the Board. However, senior management

should inform the Board promptly should any large losses occur or are likely to occur from foreign exchange exposures; and

- i) ensure that officers involved in foreign exchange operations have the necessary knowledge and expertise to undertake their duties.

Foreign Exchange Risk Management Framework

3. Managing foreign exchange risk is a fundamental component in the safe and sound management of all banks that have exposures in foreign currencies. It involves the prudent management of foreign currency positions in order to control, within set parameters, the impact of changes in exchange rates on the financial positions of banks.
4. The frequency and direction of exchange rate changes, the extent of the foreign currency exposure and the ability of counterparty to honor their obligations to the banks are significant factors in foreign exchange risk management. It is therefore essential that each bank puts in place a comprehensive foreign exchange risk management framework, taking into account the nature and complexity of their foreign exchange activities.
5. The foreign exchange risk management framework must comprise the following:
 - a) sound and prudent foreign exchange risk management policies, procedures and prudent limits;
 - b) appropriate and effective foreign exchange risk management systems, processes and internal controls; and
 - c) effective oversight by the board and senior management.

Foreign Exchange Risk Management Policy

6. Each bank is required to develop and document an in-house policy for the management of its foreign exchange risk. This policy must be approved by the bank's board, and subject to annual review.
7. The banks should take into account its ability to absorb potential losses when developing an in-house foreign exchange risk management policy; and at the minimum, should include the following:
 - a) clear objectives and strategies for foreign exchange risk management;
 - b) procedures and mechanisms for managing foreign exchange activities; proportionally to the size, complexity and frequency of the bank's foreign exchange activities;
 - c) scope of trading activity authorised and types of services offered;
 - d) trading and credit limits, and limit exception approval and reporting procedures;
 - e) clear standards for trading with affiliated entities including members of the board and employees;

- f) clear, prudent and detailed limits of the bank's foreign exchange risk exposure, compatible with the bank's operational and financial abilities, and the risk levels that the bank is willing to accept, related to individual overnight and intra-day limits for each currency and total overnight and intra-day limits for all foreign currencies;
 - g) in-house policy limits on overnight open positions for single foreign currency position and the overall foreign currency position, which must not exceed the limits prescribed under section 23;
 - h) clearly defined delegation of authority and separation of duties regarding foreign exchange operations and risk management;
 - i) accounting methods and operational procedures; and
 - j) a contingency plan and framework for stress testing.
8. The policies, procedures and limits should be properly documented, drawn up after careful consideration of the foreign exchange risk associated with the different types of products, reviewed by management at appropriate levels, and approved by the board, and circulated to all relevant departments and units.
9. Banks should supplement these policies and procedures with ethical rules and standards which employees engaged in foreign exchange trading should observe. These rules and standards should address issues concerning potentially problematic trading practices, such as spreading of rumors and false information.

Risk Measurement and Reporting Systems

10. Banks should have foreign exchange risk measurement systems that encompass all significant causes of such risk. The systems should evaluate the effect of foreign exchange rate changes on profitability and capital adequacy meaningfully, and accurately within the context and complexity of the bank's foreign exchange activities.
11. Measurement systems should:
- a) evaluate all foreign exchange risk by maturity, on both a gross and net basis, arising from the full range of the bank's assets, liabilities and off-balance sheet positions, including instruments with embedded or explicit foreign exchange options;
 - b) have accurate and timely data, in relation to exchange rates, embedded options and other details on current FX positions;
 - c) enable banks to identify and measure accurately their foreign exchange settlement risk incurred both intraday and overnight, and monitor settlement exposures in real-time (or close to real-time) in order to ensure that settlement limits will not be exceeded;
 - d) document the assumptions, parameters and limitations on which the measurement systems are based. Material changes to assumptions should be documented, well supported and approved by senior management; and,

- e) include other relevant measures that the bank deems useful and relevant in line with the complexities of its foreign exchange activities.

Control of Foreign Exchange Activities

12. Controls of foreign exchange activities may vary among banks, depending on the nature and extent of their foreign exchange activities. However, the key element of a bank's foreign exchange controls should govern the following:
 - a) organisational controls to ensure clear and effective segregation of duties between those persons who approve foreign exchange transactions and those persons responsible for operational functions such as arranging settlement, exchanging and reconciliation of confirmations foreign exchange activities;
 - b) procedural controls to ensure that transactions are fully recorded in the records and accounts of the bank, are promptly and correctly settled and that unauthorized dealing is promptly identified and reported; and
 - c) controls to ensure that foreign exchange activities are monitored frequently against the bank's foreign exchange risk, counterparty and other limits, and ensure that any breach of these limits should be promptly reported.
13. The use of hedging techniques is one means of managing and controlling foreign exchange risk. However, banks may not need the full range of hedging techniques or instruments, therefore, banks must consider which hedging techniques are appropriate for the nature and extent of their foreign exchange activities, the skill and experience of trading staff and management, and the capacity of foreign exchange rate risk reporting and control system. Banks must also ensure that the financial instruments used for hedging meet their specific needs in a cost-effective manner.
14. New hedging or risk management initiatives that are not already covered by the bank's foreign exchange risk management policy should be approved in advance by the board, or the Asset and Liability Management Committee prior to implementation.
15. In assessing the effectiveness of hedging activities, banks must make sure that the assessment is not solely based on the technical attributes of the individual transaction, but the overall risk exposure of the bank resulting from a potential change in asset-liability mix and other risk exposures such as credit, interest rate and position risks is also considered.

Foreign Exchange Limits

16. Banks are required to establish explicit and prudent foreign exchange limits. They should consider their current business strategies, liquidity/volatility of the individual currencies and loss exposure related to capital when setting the internal limits. At the minimum, a bank's foreign exchange risk policy should include limits with respect to:
 - a) net open position by currency, and aggregate;
 - b) overnight net open position by currency, and aggregate;

- c) maturity distribution of foreign currency assets, liabilities and contracts;
- d) individual customer and bank lines;
- e) total FX contracts outstanding;
- f) credit limits for FX counterparties and settlement limits; and
- g) if actively trading, maximum loss by trader/desk/branch

17. Foreign exchange risk limits need to be set within the bank's overall risk profile, which should reflect factors such as capital adequacy, liquidity, credit quality, investment risk and interest rate risk.

18. The Central Bank sets maximum limits on the following:

- É Overnight Single Foreign Currency Net Open Position; and
- É Overnight Overall Foreign Currency Net Open Position.

Measurement of Foreign Currency Net Open Positions

19. The calculation of foreign currency open position in a single currency should be made by summing up the following items:

- a) The net spot position (that is, all asset items less all liability items, including accrued interest, denominated in the currency in question);
- b) The net forward position (that is, all amounts to be received less all amount to be paid under forward foreign exchange transactions, including currency futures and the principal on currency swaps not included in the spot position);
- c) Guarantees (and similar instruments) that are certain to be called and likely to be irrecoverable; and
- d) Net future income/expenses not yet accrued but already fully hedged (at the discretion of the reporting bank).

20. Foreign currency position can be either open or closed:

- a) Where the amount of the bank's assets and liabilities are equal in each type of currency, the foreign currency position is considered as 'closed' and
- b) Where the amounts of the bank's assets and liabilities are not equal in each type of currency, the foreign currency position is considered as 'open'

21. By type of foreign currency, a bank's single foreign currency open position can be either 'long' or 'short'

- a) Where the bank's assets exceed its liabilities, within the same type of foreign currency, an open position is considered as 'long' and

- b) Where the bank's assets are less than its liabilities, within the same type of foreign currency, an open position is considered as "short"

Limits on Net Open Positions in Foreign Currencies

22. Banks are required to monitor and manage their end-of-day foreign currency positions on a daily basis, to comply with the limits set out in section 23 below. At this stage, no formal limits are being imposed on intra-day positions in foreign currencies and each bank is required to manage its intra-day position in a prudent manner.
23. Banks are required to comply with the overnight foreign currency net open positions limits specified below:
24. Limit on Single Foreign Currency Net Open Positions, irrespective of short or long position, shall not exceed 12.5% of Total Capital; and
25. Limit on Overall Foreign Currency Net Open Positions, shall not exceed 25% of Total Capital.
26. The above limits are maximum limits; however, banks are required to comply with its in-house policy limits where they are lower than the limits specified in this Statement.
27. Banks may sell any excess of foreign currencies to the Central Bank at end of day to minimize foreign exchange exposure.

Foreign Exchange Settlement Risk Management

28. Foreign exchange settlement risk involves both credit risk and liquidity risk. In a transaction that fails to settle, a bank faces the possibility of losing the full principal value of the transaction. The unsettled funds may expose the bank to liquidity pressures if such funds are needed to meet other expenses.
29. Foreign exchange settlement failures can arise from counterparty default, operational problems, market liquidity constraints and other external factors.
30. Banks should ensure that there are prudent limits to control the settlement risk of individual counterparties. Foreign exchange settlement exposures should be subject to an adequate credit control process, including credit evaluation of the maximum exposure that the bank is willing to accept for a particular counterparty (foreign exchange settlement limit).
31. Foreign exchange settlement limit should be subject to the same procedures used for deciding limits on other credit exposures of similar duration and size to the counterparty. For example, if the foreign exchange settlement exposure to a counterparty that lasts for a night, the limit may be assessed in relation to the bank's willingness to lend directly to this counterparty on an overnight basis. Limits should be based on the level of credit risk that is prudent and should not be set at an arbitrary or high level, solely for the purpose of facilitating trading with a counterparty.

32. Any planned excesses of settlement limits should be subject to approval by the appropriate credit management personnel in advance.
33. Banks must take steps to avoid any under-estimation of the risk they incur both intra-day and overnight, given the full size and duration of their remaining foreign exchange settlement exposures.
34. Recognizing that some of settlement obligations may last for more than one day, affected by factors such as time zone differences, banks must measure accurately the size and duration of their settlement exposures by identifying explicitly both the unilateral payment cancellation deadline for individual transactions and the time needed for checking the receipt of funds for the currency bought.
35. For effective management of foreign exchange settlement risk, banks are required to have, at the minimum:
- a) clear senior level responsibility and authority for managing foreign exchange settlement exposures with individual counterparties, and appropriate daily management procedures for these exposures;
 - b) institution-wide business policies that provide for the choice of settlement methods through appropriate risk measurement and cost-benefit analyses, with adequate incentives and controls for individual business units to follow the policies;
 - c) systems that monitor closely any limit excesses and unusual settlement activity;
 - d) stress tests to evaluate capacity to withstand stressed situations such as settlement delay, individual counterparty failures and disruption of payment systems (stress-testing scenarios must be appropriate to the nature and complexity of the bank's foreign exchange operations); and
 - e) procedures including contingency plans for dealing with settlement failures and other problems.

Internal Audit

36. The Internal Audit Unit of each bank is required to conduct regular reviews of the internal control and risk management process for foreign exchange risk (including settlement risk) in place, to ensure its integrity, accuracy and reasonableness.
37. The internal audit function is required to present the internal audit assessment report to the board on a timely basis, and must promptly inform the bank's senior management of any irregularities in trading patterns or trends, frequent excesses of limits or issues concerning controls in the trading area.

Contingency Plan

38. Contingency planning should be an integral part of a bank's foreign exchange and settlement risk management process and should at the minimum:
- a) document general procedures and processes for the continuity of its foreign exchange operation in the event that the main area becomes unusable;
 - b) incorporate specific procedures in addressing failed transactions or other settlement problems to ensure timely access to key information and to obtain information and support from correspondent banks; and
 - c) test the plan periodically to assess its adequacy.
39. The Central Bank reserves the right at any time to review and revise the approved limits for each bank and to withdraw approval for such amounts to be held in foreign currencies, at its discretion.



Prudential Statement 11

Cybersecurity



Objectives and Key Requirements

This Prudential Standard aims to ensure that licensed financial institutions (LFIs) have in place a cybersecurity governance and risk management framework commensurate with the LFI's inherent cybersecurity risk, so as to ensure the business impact from the occurrence of cybersecurity vulnerabilities or cybersecurity incidents are kept to a minimum and are within the LFI's risk tolerance levels.

Key requirements of this Prudential Standard are that the Board of an LFI is ultimately responsible for ensuring prudent and comprehensive cybersecurity risk management of the institution, and that the LFI must:

- establish and maintain a comprehensive and effective cybersecurity risk management framework;
- clearly define the cybersecurity-related roles and responsibilities of the Board, senior management, governing bodies and individuals;
- maintain a cybersecurity capability commensurate with the size and extent of threats to its information assets;
- implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls; and
- minimise the likelihood and impact of cybersecurity incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third-parties.

Contents

Introduction.....	114
Applicability	114
Definition of Terms	114
Governance	116
Human Resources.....	119
Asset Management.....	120
Access Control.....	121
Cryptography	122
Physical and Environmental Controls	123
Operations Security	124
Communications Security.....	126
Systems Acquisition and Development Lifecycle	127
Third-Party Relationships.....	128
Incident Management	128
Security Audit and Testing	128
Cybersecurity Considerations of Business Continuity Management.....	129
Regulatory Reporting	129
Compliance with <i>Financial Institution Prudential Standard - Cybersecurity</i>	129
Appendix 1.....	130

Introduction

In preparing the requirements of this Prudential Standard, reference has been made to the recommendations of international financial sector supervisory standard setters and international sound practices and standards on cybersecurity.

Applicability

This Prudential Standard applies to all entities licensed under the Financial Institution Act 1996

Definition of Terms

Availability ó timely and reliable access to and use of information

Confidentiality ó access being restricted only to those individuals, entities or processes authorised

Criticality ó the degree of importance to potential loss of availability

Cybersecurity ó controls and processes to preserve the confidentiality, integrity and availability of information assets

Cybersecurity capability ó the totality of resources, skills and controls which provide the ability and capacity to maintain information security;

Cybersecurity control ó a prevention, detection or response measure to reduce the likelihood or impact of an information security incident;

Cybersecurity incident ó an actual or potential compromise of the confidentiality, integrity or availability of an institution's system or data

Cybersecurity policy framework ó the totality of policies, standards, guidelines and procedures pertaining to information security;

Cybersecurity threat ó a circumstance or event that has the potential to expose an information security vulnerability;

Cybersecurity vulnerability ó weakness in an information asset or information security control that could be exploited to compromise information security;

Data at rest ó data held or stored on some form of storage system

Data in transit or motion ó means data being transferred over some form of communication link.

Data in use ó means data that is being accessed or used by a system at a point in time.

Firewall ó system or combination of systems that enforces a boundary between two or more networks typically forming a barrier between a secure and an open environment such as the Internet;

Information asset ó information and information technology, including software, hardware and data (both soft and hard copy);

Integrity ó completeness, accuracy and freedom from unauthorised change or usage;

Sensitivity ó the potential impact of a loss of confidentiality or integrity.

Malware ó a collective term used to describe a variety of malicious programs (including viruses, worms, Trojan horses, ransomware, spyware, adware, shareware etc.) designed to spread and replicate from computer to computer through communications links or through sharing of electronic files to interfere with or damage computer operation.

Material activities ó activities of such importance that have a significant impact on the banking institution's business operations or its ability to manage risks effectively should such activities be disrupted;

Need to know basis ó the restriction of sensitive data using a tight security method in which information is only given to those who need it, to do a particular task

Penetration testing ó the practice of testing a computer system, network or web application for security weaknesses or vulnerabilities that might potentially be exploited

Software System End of Life ó with respect to a software product, indicating that the product is in the end of its useful life

Vulnerability assessment ó the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system

Governance

Cybersecurity Risk Management

1. Financial Institutions (FIs) must have in place a framework for cybersecurity risk management (CSRMF) and this should be an integral part of the FI's enterprise risk management framework. A comprehensive and effective CSRMF must at a minimum include:
 - a) clear definition of the elements of cybersecurity governance such as organisation structures, roles and responsibilities and reporting lines;
 - b) a formally documented statement of the Board's cybersecurity risk tolerance;
 - c) cybersecurity risk assessment methodology and tools;
 - d) cybersecurity processes which considers identification, protection, detection, response and recovery functions;
 - e) process for reviewing the effectiveness of the framework, and continuous improvement and learning process; and
 - f) three lines of defense risk management for cybersecurity.
2. A FI's CSRMF must be documented and approved by the Board. The CSRMF must be reviewed regularly.
3. FIs must have a designated cybersecurity risk management function, that, at a minimum:
 - a) is responsible for assisting the Board, board committees and senior management of the institution to maintain CSRMF;
 - b) is appropriate to the size, business mix and complexity of the FI;
 - c) has independent reporting lines to the Board, board committees and senior management of the institution, so to conduct its risk management activities in an effective and independent manner;
 - d) is resourced with staff who possess appropriate experience and qualifications to exercise their responsibilities;
 - e) is headed by a person designated as the Chief Information Security Officer (CISO) or an equivalent senior officer of the FI;
 - f) includes a formally documented statement of the Board's cybersecurity risk tolerance;
 - g) includes risk assessment methodology and tools;
 - h) includes cybersecurity processes which considers identification, protection, detection, response and recovery functions;

- i) includes process for reviewing the effectiveness of the framework, and continuous improvement and learning process; and
 - j) includes three lines of defense risk management for cybersecurity.
4. FIs which are subsidiaries or branches may adopt the CSRMF of their parent, but the minimum requirements of this standard must be complied with on a standalone entity basis.

Cybersecurity Strategy

5. FIs must develop and document an enterprise wide cybersecurity risk strategy, approved by the Board.
6. The strategy must:
- a) outline the cybersecurity risk concept and the cybersecurity challenges facing the FI;
 - b) explain the FI's overall approach to cybersecurity risk management and how this aligns to the FI's business strategy;
 - c) include key elements of the FI's cybersecurity risk management objectives, principles and implementation;
 - d) be aligned with the Board's established and documented cybersecurity risk tolerance;
 - e) establish a plan for cybersecurity risk management to identify, assess and control cybersecurity threats covering people, process, technologies and policies.
7. FIs must conduct regular reviews of its cybersecurity strategy to ensure the strategy remains relevant and current to the FI's overall business strategy and risk tolerances.

Policy Framework

8. FIs must have in place a cybersecurity policy framework commensurate with its exposures to vulnerabilities and threats, covering policies and procedures for cybersecurity risk identification, measurement, monitoring and control.
9. Cybersecurity policies and procedures must cover requirements arising from the FI's business strategy, regulatory framework and the current and projected cybersecurity threat environment.
10. The cybersecurity policy framework should cover, inter alia:
- a) information asset management;
 - b) access control;
 - c) physical and environmental security;
 - d) end user management;
 - e) cryptography;
 - f) operations security;
 - g) communication;
 - h) system development;

- i) third-party relationships;
- j) incident management;
- k) business continuity; and
- l) regulatory compliance.

11. FIs should review and update cybersecurity policies and procedures at least annually or when major changes occur in its security environment.

Roles and Responsibilities

12. The Board and senior management of an FI must ensure that a sound and robust CSRMF is established and maintained.

13. The Board of an FI is ultimately responsible for the institution's CSRMF and is responsible for the oversight of its operation by management, and must, inter alia:

- a) approve the CSRMF;
- b) approve the institution's cybersecurity strategy (CSS);
- c) set and formally document the cyber security risk tolerance;
- d) approve cyber security policies and procedures;
- e) ensure receipt of information on the cyber security risk profile of the institution, including significant cyber security incidents; and
- f) ensure the CSRMF is subject to effective and comprehensive audits and testing.

14. Senior management of an FI is responsible for implementing and maintaining the CSRMF consistent with the Board's cybersecurity risk tolerance, and must, inter alia:

- a) ensure sufficient resources are available for effective operation of the cyber security risk management framework;
- b) develop and maintain a comprehensive cyber security policy framework, and ensure that policies and procedures are clearly communicated throughout the institution;
- c) maintain a process of continuous assessment of the institution's cyber security risk profile and associated periodic reporting;
- d) periodically review, assess and enhance the effectiveness of the CSRMF; and
- e) establish the institution's cybersecurity strategy (CSS).

15. The Chief Information Security Officer (CISO) (or equivalent) of an FI is responsible for:

- a) managing the CSRMF;
- b) developing and enhancing the CSRMF;
- c) ensuring the consistent application of policies and standards across all technology projects, systems and services;
- d) providing leadership to the FI's cybersecurity organization;

- e) partnering with business stakeholders across the company to raise awareness of cybersecurity risk management concerns;
 - f) assisting with the overall FI's technology planning, providing a current knowledge and future vision of technology and systems.
16. The internal auditor of an FI is responsible for conducting periodic cybersecurity risk assurance audit of the FI and this should include testing of the cybersecurity environment of the FI.
17. The compliance manager of an FI is responsible for conducting compliance assessment on the cybersecurity risk policy framework of the FI.

Human Resources

Screening and Background Checks

18. FIs must have a comprehensive screening and background checking process for prospective employees and contractors that covers relevant laws, regulations and ethics.
19. FIs must have in place documented policy and controls regarding recruitment and hiring of personnel (including employees and suppliers), identity and access management, and segregation of duties, employee mobility, transfer and leave.
20. The screening and background checking process of the FI should be proportional to the business requirements, sensitivity of the information to be handled and the perceived risks.

Necessary Competence

21. FIs must have employment guidelines to ensure that all employees hired for cybersecurity related roles have the necessary skills and experience to perform the role in a trusted, competent manner.

Security Awareness Program

22. FIs must have a cybersecurity awareness and training program to ensure that all employees and contractors are aware of their responsibilities for cybersecurity and how those responsibilities are to be discharged.
23. The cybersecurity awareness and training program must encompass the entire range of target audiences, including employees, managers, developers, system and infrastructure administrators, external entities, suppliers and customers.
24. Cybersecurity awareness training should be conducted at least annually.
25. The cybersecurity awareness and training should be conducted when employees are transferred to a new position or roles with substantially different cybersecurity requirements and during the onboarding of employees.

Contractors

26. FIs must have a policy and associated written guidelines on engaging contractors to critical information technology operations and cybersecurity functions. The guidelines at a minimum must include:
- a) screening and background checks;
 - b) communication protocols;
 - c) terms and conditions of the engagement;
 - d) compliance to FI's code of conduct;
 - e) confidentiality and non-disclosure agreements; and
 - f) fit and proper criteria.

Assessment Management

Asset Inventory and Ownership

27. FIs must ensure that all information, information processing and communication assets are identified and inventoried. The inventory of these assets should be drawn up, maintained accurately and kept up to date.
28. Ownership of information assets maintained in the inventory must be appropriately assigned. The asset owners should:
- a) define protection requirements for the assets owned, be accountable for these protection requirements and ensure regular review ; and
 - b) identify assets critical to the continued operation of the institution to ensure commensurate protection.

Information Classification

29. FIs must define and have in place a Board approved information asset classification scheme. The classification scheme, at a minimum, must:
- a) include confidentiality, integrity, and availability requirements for each category; and
 - b) have institution wide applicability.
30. Information assets that are in the highest protection category, at a minimum, should be labelled regardless of their format (physical or electronic).

Media Handling

31. FIs must have appropriate policies and procedures in place to prevent unauthorised access, modification, removal or destruction of media used for the storage of information assets.

Access Control

Principles of Access Control

32. FIs must establish, document and implement relevant policies and procedures to control access to information assets and information processing and transmitting facilities.
33. The policies must align to international best practice standards and at a minimum include:
- a) information dissemination and authorisation (for example the 'need to know' and 'default deny' principles, information security levels and classification of information);
 - b) application of segregation of duties principles commensurate with the size and complexity of the institution and the risk level of the operations and functionalities involved; and
 - c) clearly defined roles and responsibilities.

User Access Management

34. FIs must establish, document and implement relevant policies, and procedures to address the following:
- a) user identification (ID) (account) lifecycle management including creation, modification, suspension and deletion of user identities;
 - b) access rights lifecycle management, including requesting, approving, granting, changing and revoking access rights;
 - c) appropriate recording of audit trails for all access rights related activities;
 - d) user IDs and access rights activities must be regularly (at least annually) reviewed and any discrepancy with policies promptly followed up, resolved and appropriately reported;
 - e) requirements for secret authentication information for all user IDs compliant with defined and enforced complexity requirements and expiration times, that effectively mitigate the risk of uncovering them;
 - f) requirements for privileged access rights assigned to user IDs different from those used for regular business or ICT related activities must include:
 - i. the number of user IDs with privileged access rights must be kept at the minimum possible;
 - ii. to the extent possible privileged user ID must be set up with strong (i.e. two-factor or three-factor) authentication; and
 - iii. activities performed using privileged access rights should be subject to close monitoring.
 - g) requirements for the use of generic administration user IDs limiting usage to the extent possible.

Cryptography

Use of Cryptography to Protect Sensitive Data

35. FIs must have a comprehensive policy on the use of cryptography for protection of confidentiality, authenticity and integrity of information. The policy at a minimum must include:
- a) senior management's approach towards the use of cryptographic controls across the institution;
 - b) use of encryption (e.g. end-to-end encryption) and authentication measures on a risk-based basis to safeguard data during transmission across open and public networks as per the institution's classification scheme on criticality and sensitivity of information;
 - c) the use of encryption for protection of information transported through devices and equipment;
 - d) methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised and damaged keys; and
 - e) vetting functions involving cryptographic algorithms and crypto-key configurations for deficiencies and loopholes.

Key Management

36. FIs must have a key management policy to ensure that cryptographic Keys are secure through their whole life cycle. The policy at a minimum to include:
- a) methods for generating keys for different cryptographic systems and different applications and disposal of materials used in the generation of Keys;
 - b) hardware security modules and keying materials are physically and logically protected;
 - c) procedures for issuing and obtaining public Key certificates;
 - d) storing Keys, including how authorised users obtain access to Keys;
 - e) procedures on exchanging or updating Keys upon expiry, including rules when Keys should be changed and how this will be done;
 - f) dealings with compromised Keys, revoking Keys, lost Keys and backing up or archiving Keys; and
 - g) when cryptographic Keys are being used or transmitted, the FI should ensure that these keys are not exposed during usage and transmission.
37. Cryptographic Keys should be used for a single purpose to reduce the impact of an exposure of a Key.

38. FIs should consider and decide the appropriate lifetime (validity period) of each cryptographic Key.

Physical and Environmental Controls

Physical Security of Information Processing Facilities

39. FIs must define security perimeters to protect areas that contain sensitive or critical information and information processing facilities.
40. Physical and logical access to data centre and systems should be permitted only for individuals who are identified and authorised, and authorisation should be limited only to those with a legitimate business need for such access according to job responsibilities.
41. Physical access of staff to the data centre should be revoked immediately if it is no longer required.
42. FIs must ensure that there is proper notification of and approval for third-parties who requires temporary access to the data centre to perform maintenance or other approved work.
43. FIs must ensure that visitors or third-parties are accompanied at all times by an authorised employee while in the data center.
44. FIs must ensure that the data centre building, facility, and equipment room are physically secured and monitored at all times and deploy security systems and surveillance tools, as appropriate.

Physical Entry Controls

45. FIs must ensure secure areas are protected by effective entry controls that only allow access to authorised personnel at all times.
46. FIs must maintain a physical log book for recording physical movements in the data centre for all personnel access, including information technology personnel, visitors and third-parties.
47. The log book should be reviewed regularly for suspicious access.
48. The access rights to data centre should be regularly reviewed and updated and revoked when necessary.
49. FIs should conduct spot checks on the physical security of the information processing facilities of the institution.
50. FIs must verify that adequate physical security measures are implemented at third-party payment kiosks, which accept and process the FI's payment cards.

Equipment Protection

51. FIs must have adequate controls in place for equipment and devices issued to employees to prevent loss, damage, theft or compromise of equipment and devices and interruption to the institution's operations.
52. FIs should also have adequate controls in place for:
- a) maintenance of the equipment and devices;
 - b) removal of equipment and devices;
 - c) security of equipment and devices off-premises;
 - d) secure disposal or re-use of equipment and devices; and
 - e) unattended user equipment and devices.

Clear Desk Policy

53. FIs must have and implement a clear desk policy for all personnel that includes papers and removable storage media.
54. FIs must have a clear screen policy for at least the information processing facilities.

Operations Security

Operational Procedures and Responsibilities

55. FIs must have formal documented procedures for operational activities relating to information processing and communication facilities; including:
- a) computer start-up and close-down procedures;
 - b) equipment maintenance;
 - c) operation and management of media; and
 - d) mail management.
56. Operational procedures should clearly identify management responsibilities and controls over all changes relating to information processing and communication facilities.
57. FIs must implement appropriate monitoring systems for the use of all information technology resources, to ensure effective operational control of information processing and communication facilities.
58. To ensure sufficient operational capacity, FIs must monitor the volume of use of information processing and communication facilities and project and manage future capacity requirements.
59. Commensurate to the level of risks inherent in an information system, LFIs must ensure that there is an adequate segregation and separation of duties for systems development, testing and operational environments.

Malware Protection

60. FIs must ensure that all information processing and communication facilities have up-to-date malware protection mechanisms.

Backup

61. FIs must maintain information backup facilities ensuring that significant information and software can be recovered following an operational failure, disruption or disaster.

62. FIs must ensure backup duplicates of data, applications, and system images are taken and tested regularly in accordance with documented and approved backup policy and procedures.

63. FIs must ensure that the backup policy and procedures are based on defined data loss tolerances and recovery requirements and address retention and protection requirements.

64. FIs backups must be accessible at a remote location that is unlikely to be affected by the same operational failure, disruption or disaster event as the main processing site.

65. In cases of critical assets, backups must cover all information necessary for a comprehensive recovery in the event of an operational failure, disruption or disaster.

Logging and Monitoring

66. FIs must keep and regularly review event logs that record user activities (including system administrators), exceptions, faults and information security events.

67. Event logs must:

- a) be protected against unauthorised access, tampering, and data loss (including by system administrators); and
- b) be subject to privacy controls.

68. FIs must ensure all clocks of data processing and communication services are automatically synchronized to a single reference time source.

Software Installation

69. FIs must have in place documented policies and procedures to control changes to software on operational systems.

70. All installation and systems upgrades and updates must be assessed, approved, implemented and reviewed in a controlled manner, in accordance with documented policies and procedures.

71. FIs must have stated strategies and plans for Software System End of Life in the institution.

72. FIs must adopt and enforce policies to control types of software and updates users may install.

Vulnerability Management

73. Information about technical vulnerabilities of information systems must be obtained in a timely fashion.
74. FI's exposure to such security vulnerabilities are to be evaluated and appropriate measures are to be implemented to address the associated security risks.
75. FIs must establish the roles and responsibilities associated with vulnerability management, including vulnerability monitoring, vulnerability risk assessment and the installation of security updates.
76. FIs should install all relevant security updates to software on operational systems without undue delay and prioritizing high risk systems.
77. FIs must test and evaluate security updates before installation on critical systems for effectiveness and undesired side effects.
78. If installing a security patch would result in side effects that cannot be tolerated, or a security update is not available, then compensating controls must be implemented to mitigate the resulting exposure.

Communications Security

79. FIs must have in place controls to ensure the security of information in networks and the protection of connected services from unauthorised access, including:
 - a) documented and approved responsibilities and procedures for the management of networks;
 - b) controls to ensure confidentiality and integrity of data transmitted over networks not controlled by the institution, or wireless networks;
 - c) restrictions on system connections to the networks; and
 - d) authentication of systems on the network.
80. Network services' security mechanisms, service level requirements and required management services, must be identified and be subject to documented service level agreements, whether services are provided internally or outsourced.
81. FIs deploying Wireless Local Area Networks (WLAN) within the institution must take measures to mitigate the risks associated in this environment, such as having secure communication protocols for transmissions between access points and wireless clients.
82. Groups of users and information systems must be segregated based on an assessment of the security requirements of each group.
83. Access between such segregated groups and between the institution's network and any third-party network must be controlled and restricted on a business need basis.

84. Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities, in particular electronic messaging.

Systems Acquisition and Development Lifecycle

85. FIs must ensure that information security related requirements are considered when acquiring new information systems or enhancing existing information systems.
86. FIs must have in place effective controls to ensure that information (such as payments, internet banking or mobile banking apps) are protected from fraudulent activities, contract dispute and unauthorised disclosure and modification.
87. Rules for the development of software and systems, including mandatory security requirements, must be established by the FIs and applied to developments within the institution.
88. Secure system engineering principles, coding standards and programming techniques must be adopted by the FIs and used in the system development process.
89. FIs must ensure that changes to systems within the development lifecycle are controlled by the use of formal change control procedures and the modifications to software packages are limited to necessary changes under a strict control environment.
90. FIs should establish and appropriately protect secure development environments that cover the entire system development lifecycle. In addition, FIs should supervise and monitor outsourced system development activities.
91. During the systems development phase, testing of security functionality should be carried out.

Third Party Relationships

92. The use of third-party services must not in any way result in any weakening of the cybersecurity control environment of the institution or the assurance over its effectiveness.
93. FIs must develop and implement a third-party relationship policy that mandates cybersecurity controls to address the risk posed by third-party access to its information assets.
94. FIs must review the security policies, procedures and controls of third-parties that have access to its information assets, on a regular basis, including commissioning or obtaining periodic expert reports on the adequacy of the cybersecurity control environment and compliance to applicable regulation.
95. The third-party relationship policy must, at the minimum include:
- a) appropriate due diligence processes for the appointment of a third-party service provider to determine its viability, reliability, credential and financial position;

- b) limited third-party access with time limitations ; and
 - c) management of changes to the provision of services by third-parties taking it into account the criticality of business information, systems and processes involved and reassessment of risks.
96. FIs must establish an effective service level agreement for any services provided by third-parties that in any way requires or provides access to the FI's information assets.
97. The service level agreement must include provisions in relation to cybersecurity that ensures the effectiveness of the FI's cybersecurity controls are maintained.
98. Third-party agreements must include clauses that reserves the right of the FI and the Central Bank to conduct audits, including on-site inspections of the activities, systems, sites, and facilities that are relevant to the provision of the contracted services.

Incident Management

99. FIs must have a cybersecurity incident management process governed by documented policy and procedures with the objective of restoring normal service as quickly as possible following an incident, and with minimal impact to the its business operations.
100. The cybersecurity incident management policy and procedures must at a minimum:
- a) define what constitutes a cybersecurity incident and the criteria for incident categorization, including criteria for categorizing an incident as a crisis;
 - b) prioritize resolution based on defined severity levels;
 - c) address clear accountability and communication strategies to limit the impact of information security incidents ;
 - d) address evidence collection and preservation;
 - e) address the testing of the incident management process;
 - f) address employees' requirements to notify on incidents or indicators of possible incidents; and
 - g) clear and effective coordination with supervisory body, police and national cybersecurity organizations.

Security Audit and Testing

101. FIs are required to ensure that its approach to managing information security and its implementation, including the objectives, controls, policy, processes and procedure for information security, are reviewed independently at planned intervals or when significant changes occur.

102. FIs must ensure that an operationally independent and adequately resourced internal audit function covers review of the CSRMF.
103. To ensure that cybersecurity is implemented and operated in accordance with the FIs policies and procedures, the following minimum security audit and testing requirements are to be observed:
- a) conduct security audits and tests, including vulnerability scans and penetration tests at regular intervals at a minimum for high risk systems and processes, and before such systems are introduced (put in production);
 - b) internal audit function to perform or commission security audits and tests at regular intervals (at least annually) according to their independent risk assessment; and
 - c) ensure that the internal audit function is sufficiently resourced, at a minimum to effectively assess the audits and tests planning, execution and reporting.

Cybersecurity Considerations of Business Continuity Management

104. Information security continuity must be embedded in the FIs business continuity management system and at a minimum should include the following requirements:
- a) determine their requirements for cybersecurity and the continuity of cybersecurity risk management in adverse situations, e.g. during a crisis or disaster; and
 - b) establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for cybersecurity during an adverse situation.

Regulatory Reporting

105. FIs are required to provide the following reports on cybersecurity:
- a) Quarterly reporting on all cybersecurity incidents in the format prescribed attached as *Appendix 1*
106. FIs must notify the Central Bank as soon as possible but not later than sixty minutes after becoming aware of an information security incident that materially affects or has the potential to materially affect financially or non-financially the institution or the interests of depositors.

Compliance with Financial Institution Prudential Standard – Cybersecurity

107. Non-compliance with the requirements of this Prudential Standard will be subject to corrective actions as provided by the Central Bank and the administrative penalties outlined in the Financial Institutions Act 1996.

Form QCR

Quarterly Report on Cybersecurity Risk Incidents

Reporting Institution Name			Reporting Quarter			
Cyber security root cause Areas	Event		Incident			
	Number	Value of Loss	Number	Value of Loss	No. Unresolved from prior period	No. Resolved this Qtr.
Asset Management						
Access Controls						
Operations Security						
Communication Security						
System Acquisition, Development & Maintenance						
Third Party relationships						
Information Sec. BCM						
Human Resource						
Cryptography						
Physical & Environmental						
Total						