Reserve Bank of Fiji
Banking Supervision Policy Statement No. 16

NOTICE TO LICENSED FINANCIAL INSTITUTIONS UNDER THE BANKING ACT 1995

MINIMUM REQUIREMENTS FOR THE MANAGEMENT OF OPERATIONAL RISK FOR LICENSED FINANCIAL INSTITUTIONS IN FIJI

1.0 Introduction

1.1 This policy is issued under Section 14(3) of the Banking Act 1995 as part of the Reserve Bank of Fiji's standards governing the conduct of banking business in the Fiji Islands.

1.2 In preparing the requirements of this policy, reference has been made to the recommendations of the Basel Committee on Banking Supervision and other international sound practices and standards. The Reserve Bank of Fiji has also taken into account the nature of licensed financial institutions (LFIs)[1] operating in Fiji and consulted with the industry[2].

1.3 Operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events[3]. Operational risk event types that have the potential to result in losses include:

a) internal and external fraud;
b) employment practices and workplace safety issues;
c) failure to meet client obligations, or in the nature or design of products;
d) damage to physical assets;
e) business disruption and system failures;
f) transaction processing and/or process management failures; and
g) legal risk[4]

2.0 Objective of the Policy

2.1 The objective of the policy is to ensure that each LFI has in place a comprehensive and effective operational risk management framework that is commensurate with the size, complexity, nature and scale of its operations.

2.2 Effective management of Operational Risk is integral to the nature of business the LFIs perform and to its roles as financial intermediaries. Although Operational Risk is not new, deregulation and globalization of financial services, together with growing sophistication of financial

1 LFIs include banks and credit institutions licensed under the Banking Act 1995.

2 Association of Banks in Fiji and Finance Companies Association.

3 Strategic risk and reputational risk are not included in this definition. This definition includes legal risk.

4 Legal risk includes, but is not limited to, exposure to fines, penalties or punitive damages resulting from supervisory actions, as well as ordinary damages in civil litigation, related legal costs and private settlements.

technology, and new business activities, are making LFIs' operational risk more complex.

2.3 This policy is developed to outline the Reserve Bank of Fiji's minimum requirements for the operational risk management framework of LFIs, licensed to conduct banking business. In developing this policy, the Reserve Bank of Fiji recognizes the differences in approaches to the management of operational risk.

3.0 Establishment of an Operational Risk Management Framework

3.1 Operational Risk Management Framework

3.1.1 Each LFI is required to establish a comprehensive and effective Operational Risk Management Framework (ORMF). This is the responsibility of the Board of Directors and the Senior Management. Risk management is the process of identifying, assessing, controlling and monitoring inherent operational risk in the conduct of banking business.

3.1.2 The ORMF is the totality of systems, structures, processes and people that address the operational risk management process. The ORMF sets the scope for the entire operational risk management process and determines how the process can be established and maintained within the LFI. The Framework consists of a fully documented Operational Risk Management Policy and Operational Risk Management Strategy.

3.2 Operational Risk Management Policy

3.2.1 In establishing the ORMF, each LFI is required to document its policy on managing operational risk. The policy is to ensure that the LFIs approach to Operational Risk Management will cover operational risk management standards and objectives for all key underlying business and support processes.

3.2.2 The documented Operational Risk Management Policy must be Board approved and appropriately designed for the size, nature, complexity and scale of risk and activity undertaken. The policy must reflect the internal and external environment within which each LFI's activities take place.

3.2.3 The Policy must be clearly communicated to all employees on a regular basis, to ensure that it is fully understood by the people responsible for managing these risks; and awareness levels are maintained and are consistently applied.

3.2.4 The Policy must facilitate the monitoring, measurement and management of such activities and needs to be subject to regular review and update to ensure they continue to reflect the environment within which the LFIs operate.

3.2.5 The areas, at a minimum, that Operational Risk Management Policies should cover include; Human Resources, Internal Controls, Compliance, Internal Audit, Administration, Outsourcing, Information Technology, Business Continuity Planning, Fraud, New Product Development and Change Management.

3.3 Operational Risk Management Strategy

3.3.1 The establishment of a successful framework also includes the development of strategies for LFIs. This could be separately documented or contained within the Operational Risk Management Policy.

3.3.2 The Reserve Bank of Fiji requires each LFI to develop an Operational Risk Management Strategy (ORMS) that is documented, easily understood, auditable, accessible to all staff and reflective of the size, complexity and nature of the LFI's operational risk profile and exposure.

3.3.3 To establish an effective ORMS, the LFIs need to identify stakeholders involved and what is required of them. This facilitates the identification of key business drivers and objectives.

3.3.4 In developing its strategy, each LFI should consider its strategic challenges in delivering those objectives and the consequences of not doing so. The ORMS should be reviewed continuously.

4.0 Governance of Operational Risk Management

4.1 Organizational Structure for Operational Risk Management

4.1.1 Each LFI is required to define an organizational structure for operational risk management and clearly communicate individual roles and responsibilities and reporting lines. All operational risk management activities must be clearly understood and executed.

4.1.2 Whilst the ultimate responsibility for operational risk management resides with the Board, it is essential that:

a) staff of the LFI understand their individual role in the risk management process clearly; and
b) a proactive risk culture is created to support the identification and reporting of operational risk related issues to relevant parties.

4.2 Role and Responsibilities of Board

4.2.1 The Board of an LFI is required to:

a) recognise operational risk as a distinct risk category;
b) recognise the major operational risks inherent in its business and understand the risk management framework for this;

c) approve assigned authority, responsibility and reporting relationship developed by Senior Management;

d) receive reports that enable it to understand the overall risk profile and focus on the material and strategic implications;

e) ensure that Senior Management is actively monitoring the effectiveness of risk controls, where such review should be carried out at least once a year;

f) ensure that the operational risk management framework is subject to an effective and comprehensive review by the internal audit unit.

4.2.2 For branch operations in Fiji, the Board of each LFI is required to declare who is delegated responsibility for the oversight[5] of operational risk in the Fiji branch through formalized Terms of Reference (TOR) or Charter, which should be regularly reviewed.

4.3 Role and Responsibility of Senior Management[6]

4.3.1 Senior Management should ensure the ORMF approved by the Board is implemented consistently throughout the LFI, and all levels of staff should understand their responsibilities with respect to operational risk management.

4.3.2 Senior Management of each LFI is required to:

a) develop, implement and verify detailed policies and procedures for managing operational risk in all business activities, processes and systems;

b) assess the appropriateness of the management oversight process of the operational risk management function;

c) upon approval of the Board, clearly assign authority, responsibility and reporting relationship for the LFI to facilitate decision-making and ensure accountability;

d) communicate clearly the operational risk management policy to staff across all risk areas within LFIs' that incur material operational risks;

e) report comprehensively on operational risk management program to the Board on a timely basis; and

f) notify the Board of material changes or exceptions from established policies and procedures that could affect the operational risk management framework.

4.4 Independent Operational Risk Management Function

4.4.1 The LFIs should, at a minimum, establish an Independent Operational Risk Management Function. The role of this Function is to design,

5 Oversight refers to the function of a Board where it is able to satisfy itself that the management and operation of the regulated institution conforms to its strategy, direction and policies. CEO's are not to be delegated with this responsibility.

6 Senior Management' include those persons whose conduct has a significant impact on the sound and prudent management of the licensed financial institution's operations, which include senior managers, senior executives, General Managers /Chief Executive Officer.

implement and continuously develop the LFI's Operational Risk Management Framework and to assist Senior Management in meeting their responsibility for understanding and managing operational risk.

4.4.2 The Independent Operational Risk Management Function should at a minimum:

a) establish, maintain and monitor compliance arrangements, including processes and procedures that ensure compliance with the operational risk management framework;
b) define and document all roles, responsibilities and functions pertaining to the management of operational risk;
c) ensure consistent status reporting to the Board and Senior Management;
d) design and implement a monitoring and reporting system for operational risk;
e) identify and monitor emerging trends and issues; and
f) ensure consistent liaison with internal and external audit.

5.0 Establishment of Risk Management Process

5.1 Risk Identification, Measurement and Assessment

5.1.1 Each LFI is required to establish risk identification processes. These should focus on both current and future operational risks. The operational risk identification process should consider:

a) the full spectrum of potential operational risks;
b) the internal and external environment in which each LFI operates;
c) the LFI's strategic objectives;
d) the products and services the LFI provides;
e) the LFI's unique circumstances; and
f) the internal and external change and pace of that change.

The internal environment includes each LFI's structure, activities, quality of staff, organisational changes, employee turnover and its products and services. External environment includes technological advances, changes in industry and other market information that affects the achievement of the LFI's objectives.

5.1.2 Risk identification should consider potential causes of operational risks, such as transaction processing, sales practices, management processes, human resources, vendors and suppliers, technology, external environment, disasters and unauthorized/criminal activities.

5.1.3 The risk identification process should employ tools and processes to ensure that the full spectrum of potential operational risks is captured.

These include the use of key risk indicators, risk and compliance registers, risk maps and other tools.

5.2 Risk Mitigation and Controls

5.2.1 Each LFI must have appropriate control mechanisms in place to mitigate and control the identified risks. This is essential for effective operational risk management. Risk mitigation and control at a minimum should include;

a) establishing Board approved policies, processes and procedures to control and or mitigate material operational risks;
b) ensuring that established control processes and procedures have in place a system for ensuring compliance;
c) the use of appropriate procedures to control and/or mitigate, or bear all material risks identified. For those risks that cannot be controlled, the LFI should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely;
d) clear and effective internal control system in place with clear assignment of roles and responsibilities, appropriate segregation of duties, to avoid conflicts of interest;
e) assurance of the effectiveness and appropriateness of controls in relation to risks identified;
f) identification of areas of potential conflict which should be subject to independent monitoring and review by Senior Management; and
g) use of risk mitigation tools, models or programmes to reduce the exposure to, or frequency and /or severity of risks events.

5.3 Monitoring and Reporting Risk

5.3.1 The Senior Management of each LFI is required to implement a system to monitor operational risk profiles, material exposures, incidents and breaches, losses and key risk indicators on an on-going basis.

5.3.2 Senior Management is also required to incorporate regular reporting of operational exposures, loss experience, group risk, specialist functions and internal through its operational risk organisational structure and ultimately to the Board.

5.3.3 The reports should at the least contain internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should fully reflect any identified problem areas and should prompt timely and corrective action on outstanding issues.

5.3.4 Reports should be distributed to appropriate levels of management and areas of the LFI relevant to the issues/risks/deficiencies being reported.

5.3.5 Senior Management should establish an escalation process through the operational risk organizational structure for reporting and regularly monitor the timeliness, accuracy and relevance of reporting systems, and internal controls to ensure the usefulness and reliability of reports.

6.0 Requirements for Business Continuity Management

6.1 Business Continuity Management

6.1.1 Each LFI is required to develop a Board approved Business Continuity Management (BCM) Policy. This would allow the LFI to identify, assess and manage potential business continuity risks to be able to meet its financial and service obligations.

6.1.2 Each LFI should consider in its BCM policy different types of likely scenarios to which it may be vulnerable, and identify critical business functions including those where there is dependence on external vendors or other third parties for which rapid resumption would be essential.

6.1.3 At a minimum, the LFI's BCM should include Business Impact Analysis (BIA), Risk Assessment, Recovery Strategy, Business Continuity Plan (BCP) and Disaster Recovery Plan for IT (DRP), and a regular review, testing and maintenance of the BCM.

6.2 Business Impact Analysis

6.2.1 Each LFI is required to ascertain its key business functions, resources and infrastructure and the maximum downtimes for these before a disruption has a material impact on its operation.

6.2.2 The BIA must include mapping internal processes and/or their inter-relationships and should involve active participation by the Senior Management. It ensures an adequate representation from all potentially impacted business functions within the LFIs'.

6.2.3 At a minimum, the BIA should include:

a) assessment of the likely disruption to business operations in the event of a loss of a critical business process for defined periods of time;
b) determination of alternative sources of information/services available;
c) assessment of the financial and non-financial costs during business disruption and the probable recovery time for each critical business; and
d) identification of specific threats to the critical business processes, including assessment of geographic location of installations and the prevailing conditions.

6.3 Business Continuity Plan and Disaster Recovery Plan for IT Recovery

6.3.1 Each LFI is required to develop a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). The BCP and DRP will enable an LFI to:

a) respond to a material disruption to normal business operations and critical IT systems;
b) recover and continue critical business functions and IT systems in an orderly manner;
c) plan to return business and IT systems to normal operations after material disruption; and
d) consider wide area disruptions.

6.3.2 The BCP and DRP of each LFI should, at a minimum include:

a) the detailed procedures to be followed in response to a material disruption to normal business operations and critical IT systems;
b) a list of all resources needed and a plan to efficiently utilize these resources in order to run IT and normal operations in the event the primary operational site is unavailable;
c) a communication and public relations plan for contacting key internal and external stakeholders if the institution's BCP or DRP is invoked;
d) training and seminars to promote understanding of the roles, duties and responsibilities of the LFIs' employees and persons relevant to the BCP or DRP;
e) outsourcing arrangements or contract with a critical third-party service provider should address business continuity plan and IT recovery; and
f) important information about an institution's alternate operation site for the recovery of business and/or IT operations if this forms part of the institution's BCP/DRP.

6.3.3 Off-site copies of the BCP must be kept by a number of responsible senior managers who have designated responsibilities in terms of the BCP and should also be available at the alternate recovery site if applicable.

6.4 Review, Maintenance and Testing of BCM

6.4.1 LFIs should set clear procedures, and designate responsible persons to regularly, review, test and maintain the BCM components.

6.4.2 LFIs should stipulate appropriate and regular testing of the BCM by simulating real life situations and upon completion, the test results should be assessed by an internal auditor.

6.5 Recovery Strategy

6.5.1 Each LFI is required to develop and implement a Recovery Strategy based on the results of BIA and Risk Assessment. This may involve the use of the LFI's alternate operational site. A key risk to be mitigated when using an alternate operational site is that the primary operational site and alternate operational site are not unavailable simultaneously due to close physical proximity and/or shared critical infrastructure.

6.5.2 LFIs should consider critical data and specialist software, covering frequency of update, remoteness from the prime site, processing capability, responsibility for back-ups and the maintenance of adequate documentation on how to use the back-ups when establishing appropriate off-site storage.

7.0 Key Operational Risk Areas

7.1 Outsourcing

7.1.1 Each LFI must develop a Board approved outsourcing policy that sets out its approach to outsourcing of material business activities, including a detailed framework for managing outsourcing arrangements.

7.1.2 LFIs must ensure that procedures are in place to ensure that all relevant business units of the LFI, are aware of and comply with the outsourcing policy.

7.1.3 LFIs must ensure that all outsourcing arrangements are evidenced by a written, legally binding agreement, and this must be executed before the outsourcing arrangement commences.

7.1.4 The service provider's BCP and DRP test results should be requested by LFIs that rely on the services outsourced. These documents should be reviewed and assessed to provide a level of assurance that the service provider's plans and practices are adequate.

7.1.5 Service providers should have adequate business continuity arrangements in place and this should form part of the "due diligence" process undertaken by LFIs, when entering into an outsourcing arrangement.

7.1.6 Each LFI must consult with the Reserve Bank of Fiji prior to entering agreements to outsource material[7] business activities to service providers, who conduct their activities within and outside Fiji. An outsourcing agreement must include a clause which allows Reserve Bank of Fiji access to the Service Providers documentation and processes related to the outsourcing arrangement.

7 A material business activity is one that has the potential, if disrupted, to have a significant impact on the LFI's business operations or its ability to manage risks effectively.

7.2 Internal Audit

7.2.1 Each LFI should regularly check and evaluate how well the Bank's operational risk management system operates.

7.2.2 The Internal Audit Department should supervise the implementation of operational risk management policies and independently evaluate new operational risk management policies, processes and specific procedures.

7.2.3 The Internal Audit Department should report to the Board of Directors, through the Risk Subcommittee, the evaluation results of operational risk management system.

7.2.4 The Reserve Bank of Fiji may request the external auditor of the LFI, or an appropriate external expert, to provide an assessment of the risk management processes.

7.3 Compliance

7.3.1 Each LFI should affirm the importance of the compliance function by appointing senior personnel, or an appropriate unit to oversee compliance issues.

7.3.2 Each LFI should ensure that compliance officers are equipped with the necessary skills and expertise in line with the level of complexity of the LFI's products and activities.

7.3.3 Each LFI should ensure that compliance personnel, among other responsibilities, provide advice and training on regulatory requirements and standards of professional conduct to staff, and conduct periodic reviews to assess compliance with policies, procedures, and regulatory requirements.

7.3.4 Each LFI is required to report to senior management any non-compliance with rules or guidelines.

7.4 Fraud

7.4.1 Each LFI should have in place proper financial accounting controls and adequate monitoring. It should include red flags that can quickly identify potential fraudulent activities.

7.4.2 Each LFI should ensure that regular management reports should cover not only amounts and types of fraud, but the trend analysis of the particular fraud.

7.4.3 The Reserve Bank may undertake a risk assessment and where necessary, seek expert support.

7.4.4 Each LFI should ensure that staff are trained on the potential sources of fraud and controls used in fraud risk management.

7.5 Internal Controls

7.5.1 Each LFI must have in place internal controls that are adequate for the size and complexity of their business. These should include clear arrangements for delegating authority and responsibility, separation of the functions that involve committing the LFI, paying away its funds and accounting for its assets and liabilities, reconciliation of these processes and safeguarding the LFI's assets.

7.5.2 The internal control environment should be subject to appropriate independent internal audit and compliance functions to test adherence to these controls as well as applicable laws and regulations.

7.6 Information Technology

7.6.1 Each LFI should have adequate information systems for effective management and control of all aspects of its operations. This should be commensurate with the complexity and diversity of its operations. Systems support and operational capabilities should accommodate the activities in which it engages.

7.6.2 Each LFI should deploy the necessary resources to develop and maintain the operations and systems supporting its activities.

7.6.3 Each LFI should report on its information systems operations and this should be sent to management for review.

7.6.4 Each LFI should ensure that adequate policies and procedures are established in authorising, administering and regularly reviewing user access to the network. As a general principle, developers should not have access to the IT production environment.

7.6.5 Each LFI should ensure that its IT unit facilitate with respective personnel the induction, awareness, education, and training in business information security.

7.7 Intra-Group or Conglomerate Activities

7.7.1 Each LFI should establish policies and procedures that address all dealings with related parties. This should cover operational risks that could arise from intra group or conglomerate activities.

7.7.2 Each LFI should properly document all policies relating to the activities it engages in with its related entities[8].

8 Related entities refers to any holding company, any sister company (including their subsidiaries) and any subsidiaries (direct or indirect) of a Licensed Financial Institution. It includes all related commercial and financial enterprises and regulated and unregulated entities.

7.7.3 Policies and procedures should establish the requirement for staff to report directly to Senior Management and the Board any potential operational risk issues such as conflicts of interest that arise from intra-group and conglomerate activities.

7.7.4 Each LFI is required to report to the Reserve Bank of Fiji, at all times, any operational risk issues that arises in the activities it engages in with its intra group or conglomerate activities.

8.0 Oversight of the Reserve Bank of Fiji

8.1 For the purpose of this policy, all LFIs are required to provide to the Reserve Bank of Fiji, its initial ORMF including; it's ORMP and ORMS within 30 calendar days from the date of implementation, and thereinafter by 31 December each year. Furthermore, each LFI must provide a copy of the same whenever amendments are made, and this must be submitted to the Reserve Bank of Fiji within 30 days of Board approval.

8.2 Each LFI is required to report to the Reserve Bank of Fiji, any material operational risk incident no later than 24 hours of its occurrence.

8.3 The Reserve Bank of Fiji will assess the compliance of each LFI with the requirements of this Policy, in the course of its supervision. Non-compliance may result in sanctions as specified in Section 15 of the Act.

9.0 Implementation Arrangements

9.1 This guideline applies to Licensed Financial Institutions licensed under the Banking Act and will be effective from 30 June 2010 following consultation with the industry.

Reserve Bank of Fiji
June 2010