Reserve Bank of Fiji
Payment Service Provider Supervision Policy
Statement No: 1

MINIMUM REQUIREMENTS FOR RISK MANAGEMENT FRAMEWORKS OF LICENSED PAYMENT SERVICE PROVIDERS IN FIJI

NOTICE TO LICENSED PAYMENT SERVICE PROVIDERS

Reserve Bank of Fiji
February 2025

PART 1: PRELIMINARY

1.0 Introduction

1.1 This Policy outlines the Reserve Bank's minimum requirements for risk management for payment systems and is issued pursuant to sections 5(a) and 5(b) of the National Payment System Act 2021.

1.2 This Policy applies to all licensed Payment Service Providers (PSPs) in Fiji.

1.3 The Policy sets out the Reserve Bank of Fiji's ("Reserve Bank") minimum requirements for the establishment of a Risk Management Framework (RMF) within all licensed PSPs, outlining sound risk management principles and practices to be applied, and covers the roles and responsibilities of the board of directors ("board or board proxy in case of branch operations[1]") and the senior management of PSPs and its internal control functions[2].

1.4 The minimum standards reflected in this Policy have been aligned to international standards, including those advocated by the International Organization for Standardization (ISO) and practices implemented by other jurisdictions.

2.0 Background

2.1 An adequate RMF is essential in the sustainability of the operation of a payment system provider which in turn encourages customer trust. Therefore, it is vital that a PSP establishes and maintain a robust internal risk management and control system.

2.2 Some key risks that PSPs are generally exposed to include operational risk, systemic risk, reputational risk, liquidity risk, general business risk, settlement risk, money laundering risks, financial risk and legal risk.

2.3 The Reserve Bank recognises that risk management differ between licensed entities, depending on a range of factors including size, complexity of operation, organisational structure, ownership structure, nature and scope of financial activity, corporate strategy and the risk profile. Nonetheless, the Reserve Bank expects every licensed PSP to establish and implement an appropriate and sound risk management framework, operate with a high degree of integrity, and work under a strong risk culture.

3.0 Objective of the Policy

3.1 The objective of this policy is to ensure that PSPs have in place a comprehensive and effective risk management framework that identifies, measures, monitors and mitigates risks, commensurate with the size, nature, complexity, and risk profile of their business operations.

[1] Foreign incorporated licensed payment service provider must appoint a board proxy (whether a director or senior executive or a committee) outside the Fiji operations, with delegated authority from the board who will be responsible for overseeing the Fiji branch operations.

[2] Refer to definition on page 17

PART 2: MINIMUM REQUIREMENTS

4.0 Risk Management Framework

4.1 A PSP must establish and maintain an effective RMF that identifies, measures, monitors, and controls risks that can arise during provision of payment services.

4.2 The size, nature, scope, complexity and risk profile of the licensed payment service provider must be considered in the development of its RMF.

4.3 The board or proxy of PSPs is ultimately responsible for the sound and prudent management of the RMF.

4.4 All PSPs must ensure that their RMF is reviewed at least once in three years or as and when the risk profile of the PSP changes.

4.5 The RMF includes all structures, systems, policies, processes, risk management strategy, risk culture and people that the PSP employ for its risk identification, measurement and assessment, monitoring, mitigation, control and reporting of risk.

5.0 Risk Culture

5.1 PSPs must adopt and maintain an effective risk culture, as part of its RMF through relevant policies, proper communication, continuous training, and should include an adequate ‘tone from the top’ that fosters ethical and responsible business behaviour and attitude towards risk management.

5.2 The risk culture should be communicated and implemented effectively across all levels within the PSPs and that all staff responsible for risk management process must be fully aware of it and be held accountable for their actions.

5.3 A PSP must develop appropriate processes to evaluate the current state of the risk culture of the PSP, for example, by means of self-assessment techniques or internal surveys, and where deficiencies in risk cultures are noted, the PSP should adopt well defined and timely actions to address these deficiencies.

6.0 Risk Management Strategy

6.1 A PSP must create and implement a well-documented Risk Management Strategy (RMS) that has been approved by its board or proxy. The RMS must reflect the PSP's approach to identifying, measuring, monitoring, reporting, and controlling or mitigating the major risks of its operation. Furthermore, the RMS should explain the policies and procedures for risk identification, measurement, monitoring, reporting, and control.

6.2 The RMS must be accessible and communicated to all staff on a regular basis, and any changes to the RMS must be approved by the board or proxy.

7.0 Risk Management Policy

7.1 As part of its RMF, a PSP must establish and implement a well-documented policy that outlines the PSP's approach in managing risk and the process involved.

7.2 The policy must be approved by the board, accessible and communicated to all staff on a regular basis and reviewed at least annually. Any amendment to the policy must be approved by the board or proxy.

7.3 The policy must include, at a minimum, the following:

a) clear defined roles, responsibilities and reporting structure;
b) clear defined risk, risk appetite and tolerance level for the PSP;
c) processes for identification, assessment, monitoring, mitigation, and reporting of risk;
d) clear adequate controls for the management of risk;
e) processes that ensure compliance with all applicable laws and prudential regulatory requirements; and
f) processes that ensure adequate oversight of the risk management function.

7.4 The PSPs must ensure the risks are assessed and managed from both customer level and company level. Risks should be categorised and prioritised based on their potential impact, likelihood of occurrence, and the organization's risk appetite. This process will enable the development of effective risk mitigation strategies.

8.0 Governance and Oversight

8.1 Organisational Structure

8.1.1 Each PSP must specify the organisational structure for risk management and ensure that all staff understands their specific roles, responsibilities, and reporting lines. All risk management procedures must be understood and carried out correctly.

8.1.2 Although the board or proxy is ultimately in charge for oversight[3] of risk management, it is crucial that:

a) the PSP's staff is clear on their specific roles in the risk management process; and
b) to facilitate the identification and reporting of risk-related issues to the appropriate parties, a proactive risk culture is established.

8.2 Roles and Responsibilities of Board

8.2.1 The responsibilities of the board include, but are not limited to:

a) promoting a strong risk culture that is communicated across all levels;
b) determining risk appetite and tolerance levels that are communicated to all staff;

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

c) ensuring that an effective risk management system is in place that adequately manage risks and that the RMF is documented and reviewed regularly;
d) ensuring the PSP is structured appropriately and has an adequate internal controls;
e) recognise the key inherent risks that are part of its company and are familiar with the risk management framework;
f) approving policies, procedures and conduct for the evaluation and management of risks;
g) ensuring that the internal audit unit performs an efficient and thorough evaluation of the operational risk management frameworks;
h) ensuring proper due diligence is undertaken by senior management prior to outsourcing any function; and
i) ensuring the risk management policy is implemented and maintained by senior management.

8.3 Roles and Responsibilities of Senior Management

8.3.1 The responsibilities of the senior management[4] include, but are not limited to:
a) implementing risk appetite and tolerance levels, strategies and policies;
b) develop, implement and report detailed policies and procedures for managing risks in all business activities, processes and systems;
c) assess the appropriateness of the management oversight process of the risk management function;
d) promoting, together with the board a strong risk culture across all levels;
e) maintain appropriate standards of conduct and adequate internal control;
f) ensuring implementation and compliance to risk management policies, procedures, regulations and other relevant laws;
g) monitoring compliance with all applicable laws, prudential regulatory requirements and internal risk management policies;
h) providing advice on changes in regulatory, legal or market conditions that may impact the PSP's operations;
i) provide the Board with a thorough report on the risk management policy in a timely manner;
j) developing strategic, policies and procedures that identify, measure, manage and monitor risks; and
k) notify the Board of material changes or exceptions from established policies and procedures that could affect the risk management framework.

8.4 Roles and Responsibilities of the Risk Management Function

8.4.1 The PSP must establish an independent risk management function commensurate to the size, nature, complexity and risk profile of its operations.

8.4.2 The role of the function is to assist the board and senior management to develop, implement, and maintain the risk management framework.

8.4.3 The responsibilities of the function include, but are not limited to:

[4] Senior Management include those persons whose conduct has a significant impact on the sound and prudent management of the licensed PSPs operations, which include senior managers, senior executives, General Managers/Chief Executive Officer.

a) assisting senior management in developing the risk management framework;
b) providing report on incidence situations/events where risk events exceed the PSPs' board approved risk tolerance/ appetite levels;
c) identifying and analysing potential risks and the impact of losses to the PSP's operations;
d) driving and strengthening risk culture in the PSP and managing risks proactively through best practices;
e) maintaining a risk register as part of its risk management process; and
f) providing regular reports on the performance of the function to the board.

8.4.4 The function may also include ensuring compliance with the PSP's internal risk management policies and procedures, this policy statement and Fiji's National Payment System regulatory and legal requirements.

9.0 Establishment of Risk Management Process

9.1 Risk Identification, Assessment and Measurement

9.1.1 A PSP must have in place documented processes that identify, measure and assess risks that could adversely affect its operations and must establish and maintain adequate controls mechanisms to mitigate and control identified risks.

9.1.2 A licensed PSP must ensure that its risk management framework should address the following types of risks:
a) operational risks including IT risk, business continuity risk, cyber risk, internal and external fraud, and agent risk;
b) systemic risk;
c) financial risk;
d) money laundering/terrorism financing risk;
e) reputational risk;
f) legal risk; and
g) any other significant risk that may arise from time to time.

9.1.3 PSPs must conduct a comprehensive risk assessment to identify potential risks associated with their payment services. This assessment should consider internal and external factors, such as technological vulnerabilities, operational weaknesses, regulatory compliance, fraud, financial risks or any business decision that will have an impact on their operations.

9.2 Risk Mitigation and Controls

9.2.1 The control mechanisms must be independent, quantifiable, audited and include, at a minimum, the following:
a) appropriate segregation of duties;
b) clear defined roles and responsibilities;
c) clear defined verification and approval processes, authorisation and reporting lines;
d) activity controls for each division or department;
e) a system of approvals, limits, authorisations and reporting lines;

f) reviews by the Board, Board Risk Committee, Senior Management and Internal Audit; and
g) physical controls that are in place.

9.2.2 The PSP should identify the threats and vulnerabilities applicable to its IT environment, including information assets that are maintained or supported by third party service providers. Examples of security threats that could have a severe impact on the PSP and its customers include wire transfers, system disruptions and data theft.

9.2.3 PSPs must establish robust controls and procedures to mitigate identified risks. These controls should encompass preventive, detective, and corrective measures, and should be regularly reviewed and updated as necessary.

9.2.4 Adequate security measures must be implemented to safeguard customer data, transactions, privacy, and storage of confidential data internationally and within national borders. This may include encryption, strong authentication mechanisms, intrusion detection systems, and incident response plans.

9.2.5 The PSP should perform an analysis of the potential impact and consequences of the threats and vulnerabilities on the overall business and operations. The PSP should take into consideration financial, operational, legal, reputational and regulatory factors in assessing technology risks.

10.0 Monitoring and Reporting Risk

10.1 A PSP must establish an effective monitoring process for the early detection of risk, and adopt and maintain an effective and timely reporting process for the escalation of risk management matters to the senior management and board.

10.2 Regular monitoring and reporting of risks should be carried out to ensure timely detection and mitigation of emerging threats. Incident response plans must be in place to manage and mitigate any security breaches or operational disruptions.

10.3 Collaboration with relevant stakeholders, such as banks, regulatory bodies, and technology providers, is crucial to ensure alignment with industry best practices and to address emerging risks effectively.

10.4 The PSP must ensure that data used for reporting are complete and accurate and must notify the Reserve Bank of any material risk incident (refer to Appendix 2) or when requested by the Reserve Bank for any other information.

10.5 Risk Mitigation and Controls

10.5.1 A risk register should be maintained to facilitate the monitoring and reporting of risks. Significant risks should be monitored closely and reported to the board of directors and senior management. The frequency of monitoring and reporting should be commensurate with the level of risk.

10.5.2 To facilitate risk reporting to management, a risk matrix should be developed to highlight business activities and their corresponding risk exposure. In determining the risk matrix, the PSP should take into account risk events and audit observations, as well as applicable regulatory requirements.

10.6 Compliance

10.6.1 PSPs must adhere to all applicable laws, regulations, and industry standards governing payment services. This includes compliance with data protection and privacy laws, anti-money laundering (AML) and counter-terrorist financing (CTF) regulations, and consumer protection requirements.

10.6.2 All PSPs must have in place a compliance register that ensures all applicable legislations are adhered to. This will enhance the monitoring of any breach occurring from any line of payment services business and allow for business continuity purposes.

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

10.6.4 Compliance programs should be established to monitor and ensure adherence to regulatory requirements. Regular internal audits, statutory audits, and assessments should be conducted to evaluate the effectiveness of compliance measures on an annual basis.

10.6.5 Each PSP 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 at least once in three years or depending on the level of risk the PSP is exposed to.

10.6.6 Any non-compliance with rules and regulations must be immediately reported to senior management and the Board or proxy.

11.0 Key Operational Risk Areas

11.1 Outsourcing

11.1.1 Pursuant to section 21 of the National Payment System Act 2021, the Reserve Bank’s approval is required prior to outsourcing any operational function.

11.1.2 Prior to entering into any outsourcing arrangement, a thorough risk assessment shall be conducted to evaluate the potential risks associated with the outsourced activities, including security, operational, reputational, legal, and compliance risks. Third party service providers should have adequate business continuity arrangements in place, and this should form part of the “due diligence” process undertaken by PSPs, when entering into an outsourcing arrangement.

11.1.3 Each PSP is required to develop an outsourcing policy that has been approved by the Board or proxy. This policy outlines the PSP's approach to outsourcing

significant business operations and includes a comprehensive framework for monitoring outsourcing arrangements.

11.1.4 To the same extent as if the services were provided in-house, the PSPs retains complete responsibility, legal liability, and accountability for all tasks that they may outsource to a third party provider.

11.1.5 PSPs are required to ensure that every outsourcing agreement is supported by a written, legal binding contract that is signed prior to the outsourced arrangement starting.

11.1.6 The third party service provider's BCP and DRP test results should be requested by PSPs 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.

11.1.7 The PSP shall ensure that all outsourced activities comply with applicable laws, regulations, and industry standards, including but not limited to data protection, anti-money laundering, and consumer protection policies.

11.1.8 The outsourcing agreement must make allowance for the Reserve Bank of Fiji to access the third party service provider's documentation and pertaining to the outsourcing arrangement when need be.

11.1.9 PSPs shall provide regular updates to the Reserve Bank of Fiji on vendor performance, incidents, compliance, and any material changes to the outsourcing arrangement.

11.1.10 The Reserve Bank of Fiji reserves the right to take necessary actions on a PSP's outsourcing arrangement. These actions include but are not limited to supervisory assessments and the ability to request information directly from the outsourcing provider by the Reserve Bank of Fiji of the PSPs' outsourcing arrangements, and their compliance with the Reserve Bank of Fiji requirements.

11.2 Agent and Merchant Risk

11.2.1 All PSPs have the responsibility to ensure their respective agents and merchants are in compliance with all relevant legislations. PSPs must conduct regular spot checks on agent and merchant operations in relation to payment services. PSPs must also carry out regular trainings to their agents and merchants to ensure they are updated on new ways of fraudulent activities taking place, to be able to detect and report any suspicious transactions taking place.

11.2.2 All PSP must ensure that thorough due diligence is conducted prior to on-boarding any agents or merchants, including their financial stability, technical capabilities, security measures, and compliance with regulations.

11.2.3 PSPs should develop adequate Agent and Merchant Oversight Programs to maintain consistency in terms of supervision and risk awareness for both parties.

11.3 IT Security and Control Risk

11.3.1 The PSP should ensure they have an Information and Communication Technology (ICT) and security risk management policy in place, and it should have the Board or proxy approval. Roles and responsibilities for information security risk management and other ICT activities should be clearly defined by the PSP. The Board or proxy should approve and review the ICT and security risk management policy at least once per year.

11.3.2 The ICT and security risk management policy should at minimum include processes in place to:

a) assess the ICT and security risks to which a PSP is exposed;
b) identify mitigation measures, including controls, to mitigate ICT and security risks;
c) keep track of the success of these measures as well as the quantity of reported incidents, including those affecting ICT related activities, and act to adjust the actions as required; and
d) recognise and evaluate any ICT and security risks that may arise as a result of significant changes to ICT systems, services, processes, or protocols, as well as following significant operational or security incidents.

11.3.3 The following should be guaranteed in relation to IT and security systems used by PSPs in the delivery of payment services:

a) assure the accuracy, dependability, and completeness of all information processed, saved, or transmitted.
b) confidentiality and integrity and non-repudiation of customer information and transactions;
c) reliability of services delivered via channels and devices with minimum disruption to services;
d) appropriate authentication of users or devices and authorisation of transactions;
e) adequate audit trail and monitoring of suspicious transactions;
f) establish and keep proactive measures to identify and stop fraudulent transactions, phishing scams, and the compromise of application systems and data as well as policies, procedures, systems, and controls for managing fraud; and
g) encrypt electronic customer records and information when transferring data over private and public networks to protect customer data.

11.3.4 PSPs must ensure confidentiality by having a user access management in place. The PSP should be able to provide patch management and updates to fix any bugs or issues in the system.

11.4 Network Resilience

11.4.1 A PSP must stage a testing platform before production deployment to ensure the products are high quality in terms of security and reliability. Additionally, all systems must be monitored 24/7 by the relevant networking team for any issues that may arise depending on the proportionality and size of the business.

11.4.2 All PSPs must carry out periodic vulnerability assessment tests and penetration tests to their system security to assess their protection level and determine if perpetrators will be able to infiltrate it based on proportionality and size of business, and if vulnerable, strengthen their security levels as soon as possible at least once in three years or depending on the level of risk the PSP is exposed to.

11.4.3 The PSP needs a dependable, expandable, and secure network that can accommodate all of its business operations, including long-term expansion plans.

11.4.4 The PSP is responsible for making sure that enough and pertinent network device logs are kept for the time period specified in the system for forensic and investigative reasons.

11.5 Cybersecurity

11.5.1 This applies to all employees, contractors, vendors, and third-party partners of all licensed PSPs who have access to its systems, data, or networks. It encompasses all aspects of cybersecurity, including but not limited to information security, network security, application security, and incident response.

11.5.2 All PSPs must have a cybersecurity strategy in place and must, at a minimum include:

a) implement robust access control mechanisms to ensure that only authorized individuals have access to sensitive systems and data;
b) encrypt sensitive data both in transit and at rest to protect it from interception and unauthorized access;
c) deploy firewalls and intrusion detection/prevention systems to monitor and block unauthorized network traffic;
d) regularly update and patch all software and systems to address known vulnerabilities;
e) cybersecurity training to all employees to raise awareness of potential threats and best practices;
f) develop and maintain a comprehensive incident response plan to address security breaches promptly and effectively; and
g) evaluate and manage the cybersecurity risks associated with third-party vendors and partners.

11.5.3 The use of third-party services must not in any way result in any weakening of the cybersecurity control environment of the licensed PSP, or the assurance over its effectiveness.

11.5.4 Third-party agreements must include clauses that reserves the right of the PSP and the Reserve Bank, or an agency authorized by the Reserve Bank to conduct reviews, including on-site examination of the activities, systems, sites, and facilities that are relevant to the provision of the contracted services.

11.5.5 To ensure that cybersecurity is implemented and operated in accordance with the PSP's policies and procedures, the following minimum security audit and testing requirements are to be observed:

a) conduct security audits and tests, including but is not limited to vulnerability scans and penetration tests, at regular intervals at a minimum for high risk systems and processes, and before such systems are introduced;
b) internal audit function to perform security audits and tests which is commissioned by the Board at regular intervals according to their independent risk assessment; and
c) ensure that the internal audit function is sufficiently resourced, at a minimum to effectively assess the tests' planning, execution and reporting.

11.6 Settlement Risk, Complaints and Dispute Resolution

11.6.1 A PSP must have policies in place to mitigate settlement risks prevalent to transactions taking place either domestic or international. PSPs must maintain sufficient liquidity reserves to meet settlement obligations promptly.

11.6.2 Each PSP including its agents and merchants must establish liquidity management policies and procedures to monitor and manage cash flows effectively and must develop contingency plans to address liquidity shortfalls or unexpected payment volume fluctuations.

11.6.3 Complaints may be lodged in writing, or verbally, by any reasonable means (for example, letter, telephone, email, or in person). Complaints can also be lodged by filling a payment service providers prescribed complaint form. Complaints registered online should be also registered on the main complaints register kept at the head/main office.

11.6.4 A PSP must endeavour to resolve complaints received no later than twenty-one working days unless legal proceedings are required.

11.6.5 For complaints lodged, the PSP may require complainants to enclose photocopies of originals and full disclosure of supporting documents. The twenty-one working days timeline begins from the date when the payment service provider receives full documentation from the complainant.

11.6.6 When complaints are resolved, the PSP must convey the decision in writing to the customer or authorised customer representative within five working days.

11.6.7 PSP complaints team must maintain Complaints Registers and records of complaints received. The registers should include, but not be limited to the following:

a) date complaints received;
b) name and contact details of the complainant;
c) name of staff receiving and recording the complaints;
d) brief description of the complaints;
e) appropriate person(s) and business unit(s) handling the complaints;
f) progress on the complaints; and
g) settlement amount and date.

11.6.8 Head/main offices must maintain a Master Register of all complaints for record keeping, reporting and transparency purposes for the past seven years.

11.6.9 PSPs must establish internal reporting mechanism on complaint resolution process, effective procedures to monitor complaints, and produce regular reports to senior management for review. All complaints reports must be recorded via signoff ensuring that it is read by senior management.

11.6.10 Should there be any suspected person that is being monitored for their e-money activities for suspicious transactions, they must not be in any way tipped off which may hinder finding a potential fraudster.

11.7 Incident Reporting and Investigation

11.7.1 The board or proxy should approve the PSPs' development of an incident management policy that guarantees an efficient response to any potential incidents. The incident management strategy needs to be reviewed on a regular basis or based on the lessons discovered during incidents.

11.7.2 The incident management policy should include processes in place to:

a) identify the incident, analyse to ascertain its cause and vulnerabilities it exploited;
b) identifying and prioritizing types of incidents, i.e. define severity levels, and targeted timeframe for response and resolution of the incident;
c) incident handling and escalation procedures;
d) tactics for containing the incident;
e) corrective actions to repair and prevent reoccurrence;
f) report the incident to Reserve Bank of Fiji;
g) communication plan to inform the affected parties; and
h) recording of any evidence, such as digital evidence, physical evidence, original evidence and copies of evidence.

11.7.3 The PSPs should establish a post incident analysis strategy to identify corrective measures to avoid repeat incidents and must be reported to the Reserve Bank of Fiji.

11.7.4 The PSP should regularly compile and evaluate the post-incident data. The Board or proxy must formally approve any adjustments made to the incident management policy as a consequence of the post-incident review.

11.7.5 PSPs are required to maintain detailed records of all incidents incurred for reference purposes and report to the Reserve Bank of Fiji on a quarterly basis.

11.8 Disaster Recovery and Business Continuity

11.8.1 A reliable backup system or a disaster recovery site should be ready to re-route payment operations during downtime or unexpected outage. Where a PSP uses an outsourced cloud computing platform or an offshore data recovery site to transfer and process heavy loads of transactions as and when required, proper due diligence must be undertaken by the PSP prior to any such engagements.

11.8.2 Each PSP must appropriately document its Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) procedures to manage risk associated with system interruption or data loss and must ensure that appropriate oversight, data security review and proper backup arrangements of data are regularly performed.

11.8.3 The BCP and DRP of each PSP 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 utilise these resources in order to run IT and normal operations in the event the primary operational site is unavailable;
c) a communication and public notice for all customers if the provider's BCP or DRP is invoked;
d) trainings to provide understanding of the roles, duties and responsibilities of the PSPs' employees and persons relevant to the BCP or DRP; and
e) outsourcing arrangements or contract with a critical third-party service provider should address business continuity plan and IT recovery.

11.8.4 Offsite 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 where applicable.

11.8.5 BCP and DRP must be tested and audited annually based on organizational risk assessments, regulatory requirements, and the criticality of the systems being protected.

12.0 Audit Function

12.1 Audit plays an important role to assess the effectiveness of the controls, risk management and governance process in the PSP. The PSPs should ensure IT audit is performed to provide the board or proxy and senior management an independent and objective opinion of the adequacy and effectiveness of the PSPs risk management, governance and internal controls relative to its existing and emerging technology risks.

12.2 The board should establish an internal audit function and ensure its effectiveness in performing an independent assessment of the adequacy of the internal control systems covering all relevant risks of the licensed entity.

12.3 The internal audit function should have a direct reporting line and unfettered access to the board or its audit committee, to ensure its operational independence and prompt direct reporting of its findings.

12.4 It is important to identify a comprehensive collection of technology risk auditable areas so that an efficient risk assessment can be carried out during audit planning. All IT activities, functions, and processes ought to be included in the auditable areas.

12.5 The importance and risk presented by the IT information asset, function, or process should be taken into consideration when determining the frequency of IT audits.

12.6 All PSPs should ensure that its IT auditors possess the necessary degree of competency and skills to accurately assess and evaluate the suitability of IT policies, procedures, processes, and controls put in place.

12.7 Apart from IT audits, the PSP must also ensure there is a company-wide audit also done both internally and with an external party to give assurance on the organizational structure, reporting systems, operational side of the business and AML protection in relation to financial services provided.

13.0 Review of the Risk Management Processes and Controls

13.1 A licensed PSP must have in place a documented process for the regular review of the risk management processes and control mechanism to evaluate its effectiveness.

13.2 This Risk Management Policy should be reviewed at least once in a year to ensure its continued relevance and effectiveness. Changes in regulatory requirements, industry practices, and emerging risks should be considered during policy updates.

13.3 In the event where deficiencies in the processes and controls are noted during the review, the PSP should adopt well defined and timely actions to address these deficiencies.

13.4 The result of the review should be recorded and reported to the board or proxy. The Reserve Bank must be consulted in the event where the review noted a significant development.[5]

PART 3: OVERSIGHT AND IMPLEMENTATION ARRANGEMENTS

14.0 Oversight by the Reserve Bank of Fiji

14.1 For the purpose of this Policy, all licensed PSPs are required to provide to the Reserve Bank their initial Risk Management Policy within 12 months after the effective date of this Policy**.** In the event of major changes made to risk management policy, a copy of the revised policy must be submitted to the Reserve Bank within 30 days after changes have been approved by the PSP's board or proxy.

14.2 The Reserve Bank will assess the compliance of each PSP with the requirements of this Policy in the normal course of its supervision.

14.3 Compliance with this Risk Management Policy is mandatory for all employees and stakeholders involved in mobile payment services.

[5] Examples of such development include: establishment of new roles, major upgrade to the operations and controls of the PSP.

14.4 A licensed PSP that fails to comply with the requirements of this Policy will be subject to sanctions as specified in Section 24(6) of the National Payment System Regulations 2022.

14.5 The Reserve Bank may adjust or exclude a specific requirement in this Policy by providing a written notice.

15.0 Implementation Arrangements

15.1 This Policy applies to all payment service providers licensed under the National Payment System Act 2021.

15.2 This Policy becomes effective from 31 March 2025 with full compliance required within one year from the effective date.

Reserve Bank of Fiji
February 2025

Appendix 1

Definition:

Agent: means a person that has been contracted by a payment service provider to provide a payment service on behalf, and in the name, of the payment service provider in the manner specified in the Act.

Board: means the board of directors of the payment service provider.

Complaint: means the expression of customer dissatisfaction arising from potential financial loss or poor services to the customer including those caused by error or negligence on the part of the PSP.

Control Functions: means the functions that have responsibilities independent from management to provide objective assessment, reporting and/or assurance. This includes the risk management function, the compliance function and the internal audit function.

Credit Risk: means the risk that a counterparty, whether a participant or other entity, will be unable to meet fully its financial obligations when due, or at any time in the future.

Electronic Fund Transfer: means any transfer of funds initiated by a person by way of instruction, authorisation or order to a bank to debit or credit an account maintained with that bank through electronic means, and includes point of sale transfers, automated teller machine transactions, direct deposits and the withdrawal of funds and transfers initiated by telephone, mobile network operators, internet, card or other devices.

Electronic Money: means electronically, including magnetically, stored monetary value as represented by a claim on the issuer, which is issued on the receipt of funds for the purpose of making payment transactions and which is accepted as a means of payment by the person to whom the payment is being made to.

Financial Risk: means the risk that PSP customers lose access to the funds entrusted to it.

General Business Risk: means the risks related to the administration and operation of a PSP as a business enterprise, excluding those related to the default of a participant or another entity, such as a settlement bank, global custodian, or another PSP.

Incident: means any current or past disruptive events the occurrence of which would have an adverse effect on critical operations of the PSP**.**

Legal Risk: means the risk of the unexpected application of a law or regulation, usually resulting in a loss.

Liquidity Risk: means the risk that a counterparty, whether a participant or other entity, will have insufficient funds to meet its financial obligations as and when expected, although it may be able to do so in the future.

Material Risk Incident: means those risks that are recognised by senior management that has the potential to materially impact the licensed industry's business operations.

Money laundering/terrorism financing risks: risks relating to e-money accounts and transactions being used to launder criminals' money and/or to finance terrorist activities

Operational Risk: means the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by a PSP.

Outsourcing: means a licensee's use of a third party to perform activities on a continuing basis that would normally be undertaken by the licensee.

Payment Service: means a service enabling cash deposits or withdrawals, the execution of payment transactions, the issuance or acquisition of payment instruments and any other service functional to the transfer of money, including the issuance of electronic money, electronic money instruments and electronic money services provided by a mobile network and other operators, but does not include the provision of solely online or telecommunication services or network access.

Payment Service Provider: means an entity providing a payment service.

Payment Systems: means any system or arrangement for the processing, clearing or settlement of funds, but does not include—

(a) a clearing house recognised under any other written law;
(b) an in-house system operated by a person solely for the person's own administrative purposes that does not transfer, clear or settle funds for third parties; and
(c) such other systems or arrangements as may be prescribed under this Act or any regulations made under this Act;

Reputational Risk: means the potential harm to brand image and status due to negative public perception, customer dissatisfaction, or adverse incidents.

Risk Appetite: means the aggregate level and types of risk a licensed industry is willing to take, decided in advance and with its risk capacity, to achieve its strategic objectives and business plan.

Risk Culture: means a licensed industry's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risk they assume.

Risk Management: means the process established to ensure that all material risks and associated risk concentrations are identified, measured, limited, controlled, mitigated and reported on a timely and comprehensive basis.

Risk Management System: means a systematic approach to identifying, assessing, and mitigating potential risks to minimise their impact on an organization.

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

Risk Tolerance: means the acceptance level of the outcome of a risk that a licensed industry is willing to accept, should a risk occur.

Risk Strategy: means the structured approach that a licensed industry use for the management of its risks.

Senior Management: means officers holding senior management responsibilities that may materially affect the whole or a substantial part of the licensed industry's business or financial standing.

Settlement: means the act of discharging obligations by transferring funds or securities between 2 or more persons**.**

Settlement Risk: means the risk that settlement in a payment system will not take place as expected. This risk can involve both credit and liquidity risk. It can also arise as a result of operational risk.

Systemic Risk: means the risk that the failure of one participant in the financial system to meet its required obligations will cause other PSPs to be unable to meet their obligations when due.

Technology Risk: means the risk for mobile operators to the potential challenges and uncertainties related to the use and deployment of technology in their operations.

Appendix 2

Reserve Bank of Fiji									
RBF Form IRPS INCIDENT REPORTING									
TO BE COMPLETED BY ALL OFC's									
		As At:							
	(insert name of PSP)						**(day)**	**(month)**	**(year)**
Deadline : to be submitted to RBF, within 24 hours of an incident being identified.									
I/we, the undersigned officer(s), do hereby declare that this Return has been prepared in conformance with official instructions issued by the Reserve Bank of Fiji and is true to the best of my/our knowledge and belief. **Submission of false information may be grounds for remedial measures as provided in the RBF Act 1985.**									
PERSON TO CONTACT FOR QUERIES									
Primary Contact Person:			***Email***				***Telephone***		
Title of Contact Person:			***Signature:***						
Secondary Contact Person:			***Email***				***Telephone***		
Title of Contact Person:			***Signature:***						
1.0	**Fraud, Theft , Robbery and Similar Incidents**								
1.1	**Incident Reference Number:**								
1.2	**Incident type:**								
1.3	**Date of occurrence:**								

1.4	**Date of detection or reported:**	
1.5	**Amount Involved**	
1.5.1	**Amount Lost**	
1.5.2	**Amount Recovered**	
1.6	**Summary of the incident:**	

Reserve Bank of Fiji									
RBF Form IRPS INCIDENT REPORTING									
TO BE COMPLETED BY ALL OFC's									
		As At:							
	(insert name of PSP)						**(day)**	**(month)**	**(year)**
Deadline : 1500hrs of the 7th working day of the month after each reporting month									
I/we, the undersigned officer(s), do hereby declare that this Return has been prepared in conformance with official instructions issued by the Reserve Bank of Fiji and is true to the best of my/our knowledge and belief. **Submission of false information may be grounds for remedial measures as provided in the RBF Act 1985.**									
PERSON TO CONTACT FOR QUERIES									
Primary Contact Person:			***Email***				***Telephone***		
Title of Contact Person:			***Signature:***						
Secondary Contact Person:			***Email***				***Telephone***		
Title of Contact Person:			***Signature:***						
1.0	**Fraud, Theft , Robbery and Similar Incidents**								
1.1	**Incident Reference Number:**								
1.2	**Incident type:**								
1.3	**Date of occurrence:**			**1.3.1**	**Date closed:**				
1.4	**Date of detection or reported:**								

1.5	**Amount Involved**	
1.5.1	**Amount Lost**	
1.5.2	**Amount Recovered**	
1.6	**Name(s) and profile of person(s) involved (NB. Including institutions):**	
1.7	**Name(s) of Person(s) charged or apprehended**	
1.8	**How fraud was perpetrated:**	
1.9	**Remedial action taken:**	

1.10	**Any other relevant information:**
2.0	**Service Interruption**
2.1	**Nature & Details of service interruption:**
2.2	**Number of system outages more than 2 hours:**
2.3	**Date(s) and time (including number of hours) service was interrupted:**
2.4	**Cause(s):**
2.5	**Corrective action taken:**

2.6	**Any other relevant information:**
3.0	**Cyber Incident**
3.1	**Nature & Details of Incident:**
3.2	**Status of Incident**
3.3	**Date(s) and time (including number of hours) service was interrupted (If applicable):**
3.4	**Cause(s):**
3.5	**Corrective action taken:**
3.6	**Any other relevant information:**