Bank of Namibia

National Payment System Oversight Policy Framework

National Payment System and Financial Surveillance Department

14 April 2024

TABLE OF CONTENTS

1. ABBREVIATIONS

BIS	-	Bank for International Settlement
CPSS	-	Committee on Payment and Settlement Systems
CSP	-	Critical Service Providers
EFT	-	Electronic Funds Transfer
EMV	-	Europay, MasterCard and Visa
FIC	-	Financial Intelligence Centre
FMD	-	Financial Market Department
FMI	-	Financial Market Infrastructure
IOSCO	-	International Organisation of Securities Commissions
KRI	-	Key Risk Indicator
NAMFISA	-	Namibia Financial Institutions Supervisory Authority
NPS	-	National Payment System
NISS	-	Namibia Inter-Bank Settlement System
PFMI	-	Principles for Financial Market Infrastructures
PIRPS	-	Prominently Important Retail Payment System
PS	-	Payment System
PSP	-	Payment Service Provider
RMS	-	Risk Management System
RTGS	-	Real-Time Gross Settlement System
SIPS	-	Systematically Important Payment System
SIRPS	-	Systematically Important Retail Payment System
SWIFT	-	Society for Worldwide Interbank Financial Telecommunications
VASP	-	Virtual Asset Service Providers
ORPS	-	Other Retail Payment Systems

2. DEFINITIONS

1.1. In this Framework, unless the context otherwise indicates, the words and expressions used herein shall have the same meaning assigned to them in the *Payment System Management Act, 14 of 2023, (PSM Act)*, and cognate expressions shall have corresponding meanings:

a) **“Financial Market Infrastructure”** is defined as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions.

b) **“Payment Services”** means services relating to the facilitation of payment instructions, the issuance and acquiring of payment instruments or electronic money and any other services incidental to executing payments or transferring of funds, as specified under the Schedule of the PSM Act.

c) **“Payment Service Provider”** means a person, including a banking institution, licensed under the PSM Act to provide payment services as specified under the Schedule of the PSM Act.

d) **“Prominently Important Retail Payment Systems (PIRPS)”**, based on the criteria highlighted in this Framework, refers to retail payment systems characterised by the fact that they play a prominent role in the processing and settlement of retail payments and that their failure could have major economic effects and undermine the confidence of the public in payment systems. Examples are card, Electronic Fund Transfer, and electronic money.

e) **“Systematically Important Payment Systems (SIPS)”** means a system that has a significant impact on the national payment system and which system is capable of triggering or transmitting disruptions among system participants or to the entire national payment system if it is not sufficiently protected against risk.
f) **“Systematically Important Retail Payment Systems (SIRPS)”**, based on the criteria highlighted in this Framework, refers to retail payment systems characterised by the fact that a failure of such systems could potentially endanger the operation of the whole economy. Examples are card, Electronic Fund Transfer, and electronic money.
g) **“Payment system operators”** means a person authorised under the PSM Act to operate a payment system.

3. PURPOSE

3.1 The legal authority of the Bank of Namibia (the Bank) to regulate and oversee the National Payment System (NPS) is firmly established under the *Bank of Namibia Act, 1 of 2020* (BoN Act), the *Payment System Management Act, 14 of 2023* (PSM Act) and the Virtual Assets Act, 10 of 2023 (Virtual Assets Act). The BoN Act empowers the Bank to perform functions and exercise powers related to the NPS as assigned or conferred by the PSM Act. The PSM Act further delineates the Bank's powers and functions concerning the NPS, providing a clear framework for regulatory oversight. In addition, the Bank has been designated as the regulatory authority to administer the *Virtual Assets Act, 10 of 2023 as* published in Government *Gazette* No. 8148, General Notice No. 219 dated 25 July 2023.

3.2 The National Payment System Oversight Policy Framework (Framework) serves as the cornerstone document outlining the Bank's objectives and approach to regulating and overseeing the NPS. The Bank has revised the existing Framework to update its regulatory approach to focus on activity-based authorisations and licensing, entity-based compliance monitoring, and aligning oversight efforts with international standards such as the PFMI requirements, with a significant emphasis on adopting a future-centric approach to the oversight of the NPS. This forward-thinking strategy ensures not only effective risk management and adaptation to the evolving payments ecosystem but also proactive anticipation and preparation for future developments and challenges within the NPS landscape.

3.3 The revised Framework puts the Bank in a position to proactively adopt advanced technologies to effectively license and supervise participants in the NPS. This is crucial to ensure that the Bank is not left behind the curve by its regulated populous that continues to innovate and introduce new services that challenge the current reporting and supervision process.

3.4 The revised Framework communicates the Bank’s approach to regulation which entails seeking to fully digitise its licensing process (from submission, and assessment, to communicating the decision), as well as fully automating and digitising its regulatory reporting and supervisory efforts. This will allow the Bank to shift from reactive supervision to proactive supervision.

4. OBJECTIVES OF THE FRAMEWORK

4.1 The primary objective of the Framework is to inform the NPS industry on how the Bank performs its licensing, oversight, and policy functions as it relates to the NPS in order to:

a) Promote a safe, secure, and efficient NPS.
b) Identify, monitor, and manage risks within the NPS.

c) Enhance transparency, innovation, and fair competition within the NPS.

4.2 In achieving the above objectives, the Bank aims to ensure that the NPS ecosystem contributes to the following:

a) **Financial Stability**: Mitigating systemic risks and promoting smooth NPS operations.
b) **Financial Inclusion**: Facilitating universal access to affordable and user-friendly payment services, especially for the underserved and unbanked demographics.
c) **Enable Innovation**: Supporting fintech advancements in the development of new financial products and services, and promote differentiation strategies, while managing associated risks and promoting competition.
d) **Financial Integrity**: Maintaining accurate transactional records and enforcing regulatory compliance.
e) **Financial Sustainability**: Promoting long-term economic growth and equitable access to financial products and services.
f) **Climate Change and Sustainability**: Fosters sustainability and adopt measures to mitigate the effects of climate change within the national payment infrastructure.

5. SCOPE

5.1 This Framework is applicable to the entire NPS. The following participants and payment activities fall within the scope of this Framework:

a) Retail Payment Systems (e.g. EFT, Card, etc),
b) Large Value Payment Systems (e.g. NISS),
c) Financial Market Infrastructure (e.g. Namclear)
d) Central Securities Depositories (CSD),
e) Payment System Operators,
f) Payment Service Providers,
g) Virtual Asset Service Providers, and
h) Payment Instruments.

5.2 The above-mentioned participants and payment activities will be directly overseen by the Bank or supervised in conjunction with other regulatory authorities (e.g. NAMFISA, FIC, etc). Additionally, the Bank will monitor payment activities, services, and systems according to the PSM Act, following an activity-based oversight [1]approach to ensure the payments ecosystem functions smoothly. In summary, **Figure 1** depicts the regulatory landscape which further highlights the scope of this Framework.

[1] Activity-based oversight and regulation of the NPS require licensing and authorisation to be such that regulatory requirements are uniformly applied to all types of entities involved in a specific payment activity in scope, i.e. same activity – same risk - same regulation.

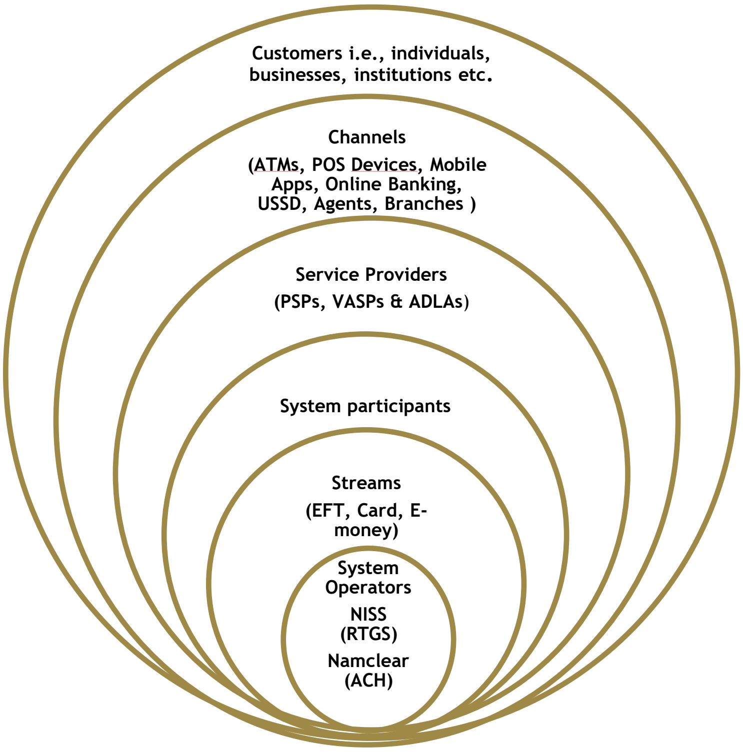

Figure 1: NPS Regulatory Landscape

6. NPS REGULATORY FUNCTION

In fulfilment of its regulatory function for the NPS, the Bank follows a three-step regulatory process to execute its mandate. This is to ensure that participants and payment activities within the NPS adhere to the Bank's regulatory framework and are subject to ongoing monitoring. In doing so, this enables the Bank to formulate appropriate and fit for purpose policy interventions. The following sections outline the Bank's three-step approach to effectively execute its regulatory function:

6.1. LICENSING

6.1.1. The Bank is empowered to license and authorise payment service providers to offer payment services as listed in the Schedule of the PSM Act, inclusive of virtual assets service providers and payment system operators in terms of section 9, section 10 and section 11 of the PSM Act. In addition, section 7, section 8 and section 9 of the *Virtual Assets Act* confers powers to the Bank to license virtual assets service providers. Leveraging digital tools, the Bank facilitates the licensing and regulation process through online portals, enabling the digital submission of applications thereby streamlining the submission, assessment and feedback process. By employing these digital tools, the Bank strives to improve the efficiency, transparency, and effectiveness of its licensing and regulatory processes for participants. As such, the Bank performs its regulatory functions for the respective participants as provided below:

a) Payment Service Providers

The PSM Act grants the Bank the authority to license and authorise payment service providers offering services outlined in the Schedule of the PSM Act, in adherence to specified subordinate legislation. The *Determination on the Licensing and Authorisation of Payment Service Providers in Namibia* (PSD-1) outlines comprehensive licensing and compliance requirements for payment service providers, encompassing both banking institutions and non-bank financial institutions. These requirements are designed to uphold consumer protection by ensuring adherence to regulatory requirements and safeguarding both funds and personal information of consumers. PSD-1 aims to bolster financial stability by mandating robust risk management frameworks and controls, thereby mitigating the potential for system failures that could jeopardize customers and the national payment infrastructure. Additionally, it reinforces legal adherence, particularly concerning anti-money laundering legislation, to deter illicit financial activities. This regulatory structure promotes interoperability between different payment systems. In essence, the licensing process plays a crucial role in nurturing a secure, resilient, and reliable financial environment.

b) Payment System Operators

The PSM Act empowers the Bank to authorise payment system operators and endorses system participants who intend to access and participate in payment systems. *The Determination for the Authorisation of Payment System Operators and System Participants in the Payment, Clearing and Settlement Systems* (PSD-6) outlines the application requirements, regulatory requirements and the terms and conditions for payment system operators and system participants as stipulated in the PSM Act. PSD-6 aims to ensure the stability and security of payment systems by providing requirements for safeguarding against fraud, cyber threats, operational risks, and other vulnerabilities that could undermine the reliability and integrity of payment systems and their participants. Furthermore, section 25 of the PSM Act empowers the Bank to designate that payment system as a designated payment, clearing or settlement system in the NPS, if the Bank is of the opinion that a payment system is a systemically important system.

c) Virtual Asset Service Providers

The Virtual Assets Act stipulates that the Bank is responsible for overseeing the licensing and regulation of virtual asset service providers. This crucial mandate aims to safeguard consumer interests, combat market abuse, and mitigate the risks of money laundering, financing terrorism, and proliferation activities associated with virtual asset markets. The Bank fulfils this mandate by implementing detailed subordinate legislation that outlines the licensing and compliance requirements for virtual asset service providers.

6.1.2. Conclusively, the Bank undertakes the above functions to ensure that its licensing regime fosters sustainability and mitigates the effects of climate change within the national payment infrastructure, such as incorporating climate-related stress tests into its regulatory requirements among its participants, in accordance with section 4.2(f) of this Framework. These tests assess how participants would fare under various climate change scenarios, helping to identify and mitigate potential risks to financial stability. In summary, the licensing process plays a pivotal role in cultivating a secure, resilient, and credible financial environment.

6.2. OVERSIGHT

6.2.1. The Bank is empowered to oversee the NPS in terms of section 3.2 (b) of the PSM Act. Oversight of the NPS comprises offsite oversight and onsite oversight efforts to ensure compliance with the Bank regulatory framework. Considering the ever-growing digital payment landscape, oversight will transition from reactive to proactive supervision, incorporating advanced monitoring mechanisms and data analytics capabilities. This includes optimising data collection, validation, storage, and reporting processes, as well as leveraging superior Artificial Intelligence techniques for proactive oversight, risk assessment and regulatory compliance validation.

6.2.2. In its oversight efforts, the Bank will conduct dynamic risk assessments in the NPS. Dynamic risk assessment is vital for timely intervention, employing advanced scanning tools to extract real-time data on payment trends. The Bank intends to use automated compliance validation and fraud detection mechanisms to maintain regulatory compliance and safeguard against risk. The Bank's primary focus is on mitigating a range of payment and settlement risks within the NPS to safeguard against systemic disruptions and failures. These risks encompass credit, cyber, fraud, liquidity, legal, operational, reputational, settlement, and systemic risks among NPS participants. The Bank also addresses potential market failures within the NPS, including:

a) **Coordination Failures**: Ineffective coordination hindering optimal networking and system integration.
b) **Non-contestable Monopolies**: Risks associated with monopolistic practices and lack of innovation, potentially leading to economic inequalities.
c) **Information Asymmetry**: Risks stemming from insufficient transparency and information on system design and services.
d) **Underinvestment in Safety Mechanisms**: Lack of internalisation of risks by participants, leading to inadequate safety measures.
e) **Faster Payment Errors**: Risks associated with automation and digital transformation, including incorrect payments and irreversible transactions.

6.2.3. Approach to Oversight

A. Off-site Oversight

The Bank leverages advanced regulatory data analytic tools and techniques to collect, validate and assess data to derive insights and make informed decisions, which allows for adequate and real time oversight. This ensures that participants are continuously compliant with the Bank's regulatory framework. Information relating to NPS operations is gathered digitally from various sources including electronic regulatory returns, reports, market intelligence, social media, consumer complaints, and other relevant sources, for effective risk profiling and monitoring of key risk indicators. The Bank further intends to leverage tools and techniques such as:

a) Automated and real-time data collection via automated push and pull techniques which integrate with the industry participants' systems. This proactive stance will enable the participants to automatically submit accurate data in real time.

b) Automated and real-time data validation to expedite data validation and increase consistency and standardisation of data to ensure data quality.

c) Appropriate data governance mechanisms over the stored data and secured access to safeguard data integrity and privacy.

d) Advanced business intelligence reporting tools and visualisation analytical tools to optimise the data reporting processes. The processed data is made available to the industry participants and relevant stakeholders.

e) Utilising real-time monitoring tools integrated with industry participant security operation centres and system availability monitoring tools to facilitate real-time notification and alerts of cyber security incidents and system downtimes.

f) Automated scanning tools to collect market intelligence in real-time from social media, websites, and internet records. By tapping into these sources of informal feedback, the Bank can take a proactive stance in identifying and addressing risks within the NPS.

g) Employing advanced analytics to analyse the instant payment transactional data, user behaviour, and network patterns in real-time to identify anomalies, suspicious patterns, hidden relationships and connections and potential threats within the payment industry.

B. On-site Assessment

Section 33 of the PSM Act empowers the Bank to conduct inspections and access information necessary to enable the effective discharge of its functions. Onsite oversight involves supervisory activities that are conducted in person, typically at the physical location of the regulated activity and entity. This can include inspections, audits, interviews, and direct observations of operations, facilities, and processes. The Bank leverages advanced technologies in executing its oversight function with automated validation of compliance with the Bank's regulatory framework. Onsite oversight is typically a result of offsite monitoring where imminent risks are identified, categorised, and assessed, but it can also be ad-hoc if a major event happens at the regulated entity. The Bank conducts the following types of inspections:

a) **Pre-opening** inspections are conducted to determine whether the prospective PSPs and system operators have met the Bank's regulatory requirements.

b) **Risk-based** inspection is focused and targeted to an individual PSP or system operator that is informed by offsite monitoring efforts. These types of inspections are planned on an annual basis, to be conducted for the following year. However, an ad-hoc Risk-Based inspection can be triggered by a high-risk incident such as a pandemic, financial crisis, spike in fraud incidents, etc. The rating model for this type of assessment is informed by **Annexure 1**: Risk Model.

c) **Thematic** inspections are targeted to more than one PSP or system operator with a focus on a specific theme. These types of inspections are planned on an annual basis for the following year and are informed by offsite monitoring efforts. However, an ad-hoc thematic inspection can be triggered by high-risk incidents such as pandemics, financial crises, spike in fraud incidents, etc.

6.2.4. Application of the Principles for Financial Market Infrastructures (PFMI)

Central banks, market regulators, and other relevant authorities have five key responsibilities for Financial Market Infrastructures (FMIs) as per the Principles for Financial Market Infrastructures. These are regulation, supervision, and oversight of FMIs; regulatory, supervisory, and oversight powers and resources; disclosure of policies with respect to FMIs; application of the PFMI; and cooperation with other authorities. These responsibilities need to be observed to achieve policy objectives and ensure the safety and stability of financial markets.

In overseeing FMIs, the Bank is guided by the PFMI. FMIs are required to adopt the PFMI, and the supporting CPSS-IOSCO *Guidance note on cyber security and resilience for FMI*. The PFMIs are designed to ensure that the infrastructure supporting global financial markets is robust and secure, and thus well-placed to withstand financial shocks. The applicability of the twenty-four PFMIs is demarcated according to the Bank's criteria for SIPS, PIRPS and ORPS in the NPS. PFMIs will also apply to the retail payment systems. The rating model for this type of assessment is informed by **Annexure 2**: PFMI Assessment Model.

6.3. POLICY

6.3.1. Policy Formulation for the NPS & Virtual Assets

The Bank is responsible for conducting policy research on various aspects within the NPS and virtual assets. Considering the ever-evolving payments landscape, this policy research results in the formulation of regulatory frameworks that are both fit-for-purpose, forward-looking and align with the Bank's objectives to modernise the NPS, enhance financial inclusion, safeguard consumer interests, and maintain the efficiency, safety, security, and cost-effectiveness of the NPS. The Bank, in line with section 3(2)(j) of the PSM Act, can issue any determination, directive, guideline, standard, circular, specifications, order or notice to govern the operations of the NPS. These regulatory frameworks are obligatory for payment service providers, payment system operators, and virtual asset service providers, who are required to comply with them diligently.

The Bank employs a range of methodologies for policy research, which encompass desktop research, benchmarking visits, and engagements with other central banks and the NPS industry participants among others. The policy research is further complemented by the statistical data that is outlined in the Data Analytics section.

6.3.2. Data Analytics

The Bank leverages statistical data collected through electronic regulatory returns and other sources to support policymaking, enhance regulatory oversight, and enhance the efficiency and security of the NPS ecosystem. In terms of data analytics, our approach involves:

a) Maintaining and routinely updating a central digital database encompassing statistical information from NPS participants, and other stakeholders.

b) Performing stress testing simulations using various tools such as the Bank of Finland Payment System Simulator aligned with the NISS Simulation Framework. These simulations cover liquidity risk, settlement risk, operational risk, and others, contributing to the Bank's financial stability and macroprudential mandates.

c) Gathering ad-hoc data from entities that are operating outside of the Bank’s regulatory scope within the NPS ecosystem to evaluate their impact and penetration into the economy to mitigate against hidden risks that these entities could introduce in the NPS.

d) Developing policy reports as well as reports that aim to provide an understanding of the interactions of the various NPS ecosystem players and the impact of the Bank's regulation in achieving the desired objectives.

Going forward the Bank will explore advanced data analytics tools such as machine learning algorithms, predictive modelling, and data visualisation techniques to extract valuable patterns and trends within the NPS. These advanced data analytics tools will enable in-depth analyses of various aspects within the NPS, including transaction volumes, consumer behaviour, risk factors, and emerging market trends, among others.

7. INDUSTRY EXPECTATIONS/RESPONSIBILITIES

7.1. The Bank expects continuous compliance from the industry with existing regulations, encompassing adherence to the Bank's regulatory framework. The timely and accurate provision of information, including operational data, transactional records, cyber resilience posture data, compliance reports, and other relevant data, is required to facilitate effective oversight and regulatory decision-making. While engaging with industry stakeholders, the Bank emphasizes that the NPS stakeholders should not impede its oversight rights, which include monitoring, assessing, and intervening in the NPS to execute its mandate. Through open communication channels and collaborative efforts, industry stakeholders can contribute to enhancing the efficiency, security, and innovation of the national payments ecosystem in alignment with regulatory objectives and mandates.

7.2. In terms of furnishing the Bank with confidential information and the controls used by the Bank to protect such information, in terms of section 76 of the BoN Act read with section 34 of the PSM Act, the Bank may request information or data (from the NPS stakeholders) it requires in order to perform its powers and functions. Staff members of the Bank are further obligated to maintain strict confidentiality regarding any information or data gathered while exercising powers or performing functions of the Bank in terms of section 77 of the BoN Act read with section 42 of the PSM Act.

8. GENERAL

This policy framework is not exhaustive and may be supplemented and/or amended from time to time.

9. ENQUIRIES

All enquiries related to this policy framework must be directed to:

Director: National Payment System and Financial Surveillance Department
Bank of Namibia
P.O. Box 2882
71 Robert Mugabe Avenue

This National Payment System Oversight Policy Framework is duly approved by:

Barbara Dreyer
DIRECTOR

Date: 14 April 2024

ANNEXURE 1: RISK MODEL

In determining the severity of risks associated within the NPS, a three-step process is followed.

Step 1: Determine the Level of **Inherent Risk**
Step 2: Determine the Strength of the **Risk Management Systems**
Step 3: Determine the **Residual Risk**

Step 1: Model for Determining the Level of Inherent Risk

Table 1 is used for rating **Inherent Risk** and is based on a 4 x 4 risk level matrix. **Inherent Risk** may be characterized as "Low", "Medium Low", "Medium High" or "High".

		Likelihood			
		Low	**Medium Low**	**Medium High**	**High**
Impact	**Low**				
	Medium Low				
	Medium High				
	High				

Table 1: Model for determining Inherent Risk

Step 2: Model for determining the strength of the Risk Management Systems

The Bank assesses the quality and adequacy of the Risk Management Systems (RMS) based on **Table 2** below by considering the following 4 risk management assessment factors:

1. Active Board and Senior Management Oversight.
2. Adequate Policies, Procedures and Thresholds for managing business activities.
3. Adequate Risk Management, Monitoring and Management Reporting Systems; and
4. Comprehensive Internal Controls including an effective Internal Audit Function.

Individual RMS factors as highlighted above may be characterized as "Adequate" or "Not Adequate". The overall rating for RMS may be characterized as "strong", "acceptable", "needs improvement" or "weak".

Risk Management Systems (RMS)				Score	Overall Rating for RMS
Board & Senior Management	**Policies & Procedures**	**Management Information Systems**	**Internal Audit & Internal Controls**		
Adequate	Adequate	Adequate	Adequate	1	Strong
Adequate	Adequate	Adequate	Not Adequate	2	Acceptable
Adequate	Adequate	Not Adequate	Not Adequate	3	Needs Improvement
Adequate	Not Adequate	Not Adequate	Not Adequate	4	Weak

Table 2: Model for Determining the Strength of Risk Management Systems

Step 3: Model for determining Residual Risk

Determining Residual Risk is accomplished by balancing the **Inherent Risk** rating with the overall strength of the **RMS** rating for each major risk area. The Residual Risk may be characterized as "High", "Medium High", "Medium Low" or "Low". The model in **Table 3** overleaf is used to determine Residual Risk and it correlates to **Table 4** in terms of the treatment thereof, as per the colour coding.

Strength of Risk Management Systems		Level of Inherent Risk			
		L	ML	MH	H
		1	2	3	4
Strong	1	Low	Low	Medium Low	Medium High

Acceptable	2	Low	Low	Medium Low	Medium High
Needs Improvement	3	Low	Medium Low	Medium High	High
Weak	4	Low	Medium Low	Medium High	High

Table 3: Model for determining Residual Risk

Description of Risk Assessment Report Rating

The descriptions of the risk assessment reporting ratings highlight the action required by the management of the participant to manage the risk.

High (4)	Considering the RMS in place or lack thereof, the risk has the potential to become systemic and has a high impact on the smooth operations of the NPS. This is unacceptable. A different approach is required. Priority management attention is required.
Medium High (3)	Considering the RMS in place or lack thereof, the risk may not become systemic and has a high impact on the smooth operations of the NPS. A different approach is required. Additional management attention is required.
Medium low (2)	Considering the RMS in place or lack thereof, the risk may not become systemic and has a moderate impact on the smooth operations of the NPS. A different approach may be required. Additional management attention may be required.
Low (1)	Considering the RMS in place, the risk may not become systemic and has a low impact on the smooth operations of the NPS. Minimal oversight effort is needed to ensure risk remains low

Table 4: Risk Assessment Reporting Rating

ANNEXURE 2: PFMI ASSESSMENT MODEL

The results of the PFMI assessment are made in accordance with the following:

Fully Observed (FO)	Payment system fully complies with the principle.
Broadly Observed (BO)	There are minor irregularities that do not significantly affect the system's security and/or efficiency.
Partially Observed (PO)	There are major irregularities and/or risks affecting the system's security and/or efficiency, but they can be removed by the service provider within a short period of time.
Not Observed (NO):	The payment system does not comply with the principle.
Not Applicable (NA):	The principle is not applicable to the payment system being assessed.

Table 5: PFMI Risk Assessment Model