Bank of Namibia

Risk-Based Oversight Policy Framework

Payment and Settlement Systems Department

Payment and Settlement Systems

29 November 2019

Table of Content

DEFINITIONS

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, 2003 (Act No. 18 of 2003 as amended) and cognate expressions shall have corresponding meanings:

1. **"Closed-Loop System Payment Instruments"** means payment instruments which can be used for the purchase of goods and services and are redeemable by the holder at a group of a clearly identified merchant.
2. **"Central Securities Depository"** is defined as entity that provides securities accounts, central safekeeping services, and asset services, which may include the administration of corporate actions and redemptions, and plays an important role in helping to ensure the integrity of securities issues (that is, ensure that securities are not accidentally or fraudulently created or destroyed or their details changed).
3. **"FMI"** 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.
4. **"Open-Loop System Payment Instruments"** means payment instruments which can be used for the purchase of goods and services and are redeemable by the holder at any card or non-card accepting merchant locations.
5. **"Payment Institution"**, means a person which provides payment services such as facilitating deposits and withdrawals from bank accounts, executing direct debits and standing orders, money remittance and certain services provided through mobile phones or other digital and IT devices.
6. **"Payment Scheme"** means is the set of functions, procedures, arrangements, rules and devices that enable a holder of a payment instrument (i.e. card or non-card) to effect a payment and/or cash withdrawal transaction with a third party other than the payment instrument issuer.
7. **"Prominently Important Retail Payment Systems (PIRPS)"**, based on the criteria highlighted in section 5 of the Framework, are 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 and in the currency in general. Such systems have alternatives.
8. **"Securities Settlement System"** is an entity that enables securities to be transferred and settled by book entry according to a set of predetermined multilateral rules. Such systems allow transfers of securities either free of payment or against payment.
9. **"Systematically Important Payment Systems (SIPS)"**, based on the criteria highlighted in section 5 of the Framework, are characterised by the fact that a failure of such systems could potentially endanger the operation of the whole economy. Such systems have no alternatives.
10. **"Systematically Important Retail Payment Systems (SIRPS)"**, based on the criteria highlighted in section 5 of the Framework, are characterised by the fact that a failure of such systems could potentially endanger the operation of the whole economy. However, such systems have alternatives.

ABBREVIATIONS

BoN	-	Bank of Namibia
BSD	-	Banking Supervision Department
BIS	-	Bank for International Settlement
CPSS	-	Committee on Payment and Settlement Systems
COBIT	-	Control Objectives for Information and related Technology
CRAN	-	Communications Regulatory Authority of Namibia
CSD	-	Central Securities Depositories
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
MNO	-	Mobile Network Operator
NaCC	-	Namibia Competition Commission
NAMFISA	-	Namibia Financial Institutions Supervisory Authority
NPS	-	National Payment System
NISS	-	Namibia Inter-Bank Settlement System
PAN	-	Payments Association of Namibia
PCI DSS	-	Payment Card Industry Data Security Standards
PCI PA-DSS	-	Payment Card Industry Payment Application Vendors
PCI PED	-	Payment Card Industry PIN Entry Devices
PFMI	-	Principles for Financial Market Infrastructures

PIRPS	-	Prominently Important Retail Payment System
PSM Act, 2003	-	Payment System Management Act No. 18 of 2003, as amended
PSSD	-	Payment and Settlement Systems Department
RMS	**-**	Risk Management System
RTGS	-	Real-Time Gross Settlement System
SARB	-	South Africa Reserve Bank
SIPS	-	Systematically Important Payment System
SIRPS	-	Systematically Important Retail Payment System
SWIFT	-	Society for Worldwide Interbank Financial Telecommunication

PAYMENT AND SETTLEMENT SYSTEMS OVERSIGHT POLICY FRAMEWORK

1. Introduction

One of the key roles of central banks is the oversight of payment and settlement systems in their areas of jurisdiction. This role is significant because the efficient functioning of payment systems allows safe, secure and timely completion of financial transactions and therefore makes a vital contribution to overall economic performance and financial stability. Central Bank's oversight of payment and settlement systems is consequently one aspect of its broad responsibility for monetary and financial stability. According to the CPSS-IOSCO PFMIs, *"payment system oversight is a public policy activity principally intended to promote the safety and efficiency of payment systems and to reduce systemic risk"*. Furthermore, while the primary role of Oversight is focused on the system (i.e. systemically and prominently important systems), it also places its focus on the efficiency and safety of the individual participants in such systems.

Oversight of payment systems complements the financial stability work of banking supervision. However, the scope of oversight differs from that of banking supervision. With banking supervision, the concerned is with the solvency and liquidity of individual financial institutions and requires the following:

- The supervision of banks and non-bank deposit-taking financial institutions;
- It is carried out by the central bank or other supervisory authority;
- It is carried out on grounds of detailed legal and prudential regulations; and
- The performance of detailed examination in the supervised institutions.

Oversight, on the other hand, seeks to promote the safety and efficiency of payment systems and requires the following:

- Analysing and examining the design and operation of systems, and related products and services, such as payment instruments;
- Ensuring efficient functioning of payment systems;
- It is not limited to banks and other institutions directly supervised by the central bank; and
- It is carried out solely by central banks.

Notwithstanding their differences, oversight and supervision share important similarities which include:

- The development and application of internationally accepted principles and standards;
- Identification and management of risks in the financial system;
- Promotion of fair access and competition;
- Assessing internal controls and operational risks in banks;
- Cooperating with other central banks and relevant international authorities in the monitoring of cross border banking and payments; and
- Overseeing the settlement of financial market trades.

From the above, it is clear that whereas financial supervisors are concerned with the soundness of banks and non-bank financial institutions, the overseer of the payment and settlement system has its focus on the smooth functioning of the payment infrastructure as a whole. Oversight and supervision, however, share the same goals of ensuring safety, soundness, reliability and stability of the financial system of a given country, including the effectiveness and efficiency of monetary settlement.

The Bank has a statutory responsibility for the payment and settlement systems in Namibia enshrined in the PSM Act 2003, as amended. In ensuring the safe, secure, efficient and cost-effective operation of the NPS, the Bank is tasked with the authorisation of participants in the clearing and settlement systems, endorsement of service providers, designation of payment instruments and also to oversee, inspect and monitor the NPS, system participants, service providers and non-bank payment institutions.

Furthermore, in terms of section 3 (1) of the PSM Act "The Bank and banking institutions must cause to be established by a constitution a juristic person to be known as the Payment System Management Body with the object of managing the national payment system, and organizing, setting technical standards, regulating the participation of its members in the national payment system and all matters affecting payment obligations and the clearing and netting of payment obligations."

In terms of this section, the Payment Association of Namibia (PAN) manages the conduct of its members in relation to all matters affecting the payment system and the Bank is tasked to oversee, inspect and monitor the operation of PAN.

PAN's mission is to maintain a world-class payment system that meets domestic, regional and international requirements. PAN has the responsibility to manage the Namibian payments inter-bank clearing system in order to:

- support the Bank in its role as overseer of the payment system by ensuring compliance for its members;
- provide the Namibian community with safe and efficient facilities to exchange payments;
- protect the safety and integrity of the payment system;
- manage the clearing and settlement risks in the payment system;
- authorise and facilitate access of participants and prospective participants to the payment system on a fair and equitable basis;
- facilitate communication between participants; and
- enable proper understanding of the system and the rules applicable to it.

2. Objectives of Oversight of Payment and Settlement Systems

Oversight is focused on two goals that contribute to financial stability. The first is preventing systemic risk to the extent it may arise from payment and settlement systems. This is also known as infrastructure-related systemic risk. The second goal is promoting the smooth operation of payment and settlement systems. This encompasses security and efficiency and maintaining public confidence.

- **Systemic Risk**
  Systemic risk occurs if a crucial settlement system fails or if a participant in a payment system cannot meet its obligations, thus setting off a chain reaction that puts other system participants in difficulty. This domino effect can have adverse consequences for the financial markets and the broader economic development of the country.

- **Smooth Operation of Payment and Settlement Systems**
  The second goal of oversight is to manage risks that may affect the smooth operation of payment systems even if there is no systemic risk. The failure or incorrect operation of retail payment systems or payment products can have significant economic and social consequences and, in the end, damage public confidence in the payment system. This could be the case, for example, if there are no alternative methods of payment or if they are limited or inefficient. It is important that such retail payment systems operate properly, and so oversight addresses their reliability, security and continuity. Smaller-scale problems, such as fraud with payment instruments or the temporary unavailability of instruments, may also arise and can also damage consumer confidence even though their financial effects are smaller.

There could be a trade-off between safety and efficiency e.g. there would be no significant gains from implementing a payment system that would have numerous safety features but would be extremely costly or difficult to use, as this would only result in the payment traffic going to less safe alternatives. With this in mind, the Bank works closely with service providers, system participants and non-bank payment institutions by encouraging efforts to adopt new processing techniques to improve safety without diminishing efficiency.

3. Scope of Oversight Activities

The payment and settlement systems oversight activities of the Bank cover the following types of systems and entities. While the list below covers a wide array of systems and entities, oversight will be guided by those risks that pose the highest risk to the NPS and the wider financial sector i.e. financial stability. The following two principles are to guide and inform the Oversight efforts and focus, as these may have a potential and material impact on the Oversight goal concerned with systemic risk:

3.1 SIPS (e.g. NISS) and PIRPS (e.g. Namswitch);
3.2 Designated Financial Market Infrastructures (FMIs e.g. NISS and Namclear); and
3.3 Payment systems that are of a systemic nature, as may be determined by the Bank, taking into account their collective effect on the payment and settlement systems and the extent to which their operations will affect public confidence in the payment systems e.g. closed and open-loop payment schemes and instruments i.e. card and non-card payment schemes. These include SIRPS e.g. EFT, Card etc.
3.4 Securities settlement systems (e.g. CSD);
3.5 Providers of critical services e.g. network service providers (e.g. Telecom, SWIFT etc.) in consultation with the relevant regulatory authorities; and
3.6 Cross-border payments and related systems, as they may be categorised under 3.1, 3.2 or 3.3 above.

As soon as the Bank has decided to oversee a new system, the decision is published on the Bank's website: *https://www.bon.com.na/*.

4. Types of Payment and Settlement Risks

The Bank's risk-based oversight policy framework is organised around the objective of the Bank's oversight — "*to assess and, if necessary, promote the mitigation of those risks within the NPS that could have adverse effects on the financial sector and the wider economy"*. In essence, the Bank seeks through its oversight to reduce systemic risks that could arise from and be propagated by payment systems. At the same time, the Bank recognises that designing and operating a payment system to minimise systemic risks would be counter-productive if the system thereby becomes so inefficient or impractical to use, such that payment traffic is migrated to less safe alternatives.

Oversight of payment systems includes the identification, management, containment and reduction of payment risks in the NPS, thus the Bank will focus on the mitigation of the following types of payment and settlement risks in order to prevent systemic disturbances and failure of the NPS:

- **Credit Risk**: The risk that a counterparty within the system will not be able to fully meet its financial obligation either when due or at any time in the future.
- **Cyber Risk:** This denotes criminal activity perpetrated using the internet, other computer networks or any other inter-connected infrastructure. In the context of payments, the term covers crimes such as phishing, card-not-present fraud, denial-of-service attacks etc. this may result in fraud risk and general business risks.

- **Fraud Risk:** Risks that materialise as a result of cyber-crime (cyber risks) or crimes which do not involve the internet, such as traditional activities used to exploit payment instruments, systems and related information.
- **General Business Risk:** The risk of the financial failure of a privately-owned service provider.
- **Liquidity Risk:** The risk that a counterparty within the system will not have sufficient funds to meet financial obligations as and when expected, although it may be able to do so at some time in the future.
- **Legal Risk:** When existing laws or regulations do not support the rules and arrangements of the system this could create uncertainties which could lead to unexpected losses resulting in credit and liquidity risks**.**
- **Operational Risk**: The risk that human error, failure of software or hardware or breakdown in communications systems or networks may bring about financial losses.
- **Reputational Risk:** Reputational risk can be defined as the risk arising from negative perception on the part of customers, counterparties, shareholders, investors or regulators that can adversely affect either a system participant or service provider's ability to maintain existing, or establish new, business relationships and continued access to sources of funding (e.g. through the interbank etc.).
- **Settlement Risk:** The risk that a settlement in a transfer system will not take place as expected.
- **Systemic Risk:** The risk that the inability of one or more participants to perform as expected will cause other participants to be unable to meet their obligations when due.

The Bank will also concern itself with preventing possible market failures in payment and settlement systems among which are:

- **Coordination failures:** it is necessary to have effective coordination between competing institutions providing payment services in order to achieve optimal networking of systems and integration. This encourages the introduction of new systems that are more efficient than if there were no coordination.
- **Non-contestable monopolies:** the network effect of payment systems infrastructure often leads to monopolies which may be counter-productive. There is the potential risk of abuse of monopoly power when a payment system service provider fails to introduce cost-saving measures as well as invest in new and improved technologies.
- **Information asymmetry:** lack of transparency in the design of systems and the weaknesses therein in addition to inadequate information on services for participants and customers create risks.
- **Underinvestment in safety mechanisms in payment and settlement systems**: Participants of the system may fail to internalize the effect of their own failures on other system participants, the financial system and the whole economy and therefore, not take appropriate steps to address inherent risks.

5. Approach to Oversight Activities

The Bank will pursue a risk-based approach in the oversight of payment systems in that it will conduct assessments and classifications based on systemic importance,

with the objective of focusing the oversight activities and resources on the systems that pose the highest risk to the stability of the system. A risk-based approach will allow for the identification and coordination of strategies to treat payment systems related risks. These risks can ultimately develop into systemic risk which, if left uncontrolled, can incapacitate the entire system and by extension the economy in general.

For the purpose of its oversight activities, the Bank will use the criteria below among others to determine the importance of the respective payment systems:

- Value and volume of payments executed in the system;
- The size and concentration of financial risks within the payment system;
- The payment system's market share;
- The share of critical participants;
- Interoperability of a system;
- Interdependence with other payment systems or markets;
- Use in monetary policy operations;
- Visibility of a system;
- The degree of substitutability;
- Impact on the national economy; and
- The markets on which the payment system is active.

Should a payment system be considered systemically important, the Bank will consider such systems to be FMI's in terms of the PFMIs. Such systems will then be required to comply with the PFMIs as well as any other oversight requirements set by the Bank. See **Annexure 10.1**.

6. Guiding Principles for Oversight Activities

The payment system's oversight activities would be guided by the following principles:

- **Transparency:** The Bank will publicly declare its oversight policies and standards for the various payment systems.
- **International Standards:** The relevant internationally recognized standards would be adopted for payment and settlement systems oversight activities.
- **Exercise of Statutory Authority:** The Bank will use its authority under the relevant laws to compel participants to conduct themselves in the interest of the national payment system. However, the Bank will as much as possible, dialogue with participants in the various payment systems to conduct their affairs in a manner that will promote the safety and efficiency of the NPS. The Bank will only evoke its statutory powers to compel participants to comply when dialogue fails.
- **Consistency:** oversight standards would be applied consistently to comparable payment and settlement systems.
- **Cooperation in oversight:** The Bank will cooperate with other relevant central banks (i.e. SARB, Central Bank of Lesotho, Central Bank of Swaziland, etc.) and other local supervisory authorities including the NAMFISA, NaCC, CRAN and relevant Departments in the Bank (e.g. BSD,

FIC and FMD) to promote safety and efficiency of the payment and settlement systems.

7. Standards

In addition to system rules, user guidelines, payment product standards[1] among others, the Bank will use internationally approved payment system standards and best practices to conduct the oversight activities. Regarding international standards, the Bank expects that service providers of payment systems comply with the **24 PFMIs** (April 2012) issued jointly by BIS-CPSS-IOSCO where applicable. These principles are set out on the BIS website as in http://www.bis.org/publ/cpss101a.pdf. Regarding best practices for the management of information and related technologies, the Bank will expect service providers, system participants and non-bank payment institutions to comply with processes of COBIT 5.

COBIT 5 provides an end-to-end business view of the governance of enterprise IT, reflecting the central role of information and technology in creating value for enterprises of all sizes. COBIT 5 is the only business framework for the governance and management of IT. One of the reasons that the Bank adopted COBIT 5 was that COBIT gives a holistic view of the IT computing environment, starting with management issues to operational issues, what controls management needs to implement which cascade to operational goals. Furthermore, the principles, practices, analytical tools and models found in COBIT 5 embody thought leadership and guidance from business, IT and governance experts around the world.

IT value management and IT business alignment emphasise on the need for IT resources to be aligned to business strategies. COBIT 5 provides a clear road map from planning of the risk assessment up to fieldwork execution. COBIT 5 is specifically targeted at IT risk and assurance professionals i.e. supervisors, overseers etc. It is designed to enable efficient and effective development of IT risk and assurance initiatives, providing guidance on planning, scoping and executing risk and assurance reviews using a road map based on well-accepted risk and assurance approach. COBIT 5 also provides detailed standards on how to ensure the security of the IT systems underlying the payment systems as covered by processes 5 and 11 listed. This sufficiently guides overseers of payment systems on how to assess the security of these systems.

It should be noted that the Oversight of payments systems does not involve the provision of assurance services in the conventional audit sense.

The Bank's oversight function of payment systems, as well as system participants and non-bank payment institutions, will also be guided by the five key responsibilities for market regulators and central banks as stipulated in the PFMIs and as provided in section 6 above. All designated FMIs operating in the country are expected to comply with the applicable principles unless a service provider, system participant or

[1] Such as PCI DSS, EMV, PCI PED, PCI PA-DSS, etc.

non-bank payment institution has reasons that the overseer of the payment system deem compelling enough for partial compliance.

8. Oversight Process

8.1 Authorisation. Licensing and Endorsement

The Bank will grant authorisation to participants in the clearing and settlement systems, endorse the registration of payment service providers, designate payment instruments and FMIs, and authorise non-bank payment institutions in line with the mandate given by the PSM Act, 18, 2003 as amended. The objective of system participant authorisation, payment instrument designation and service provider endorsement (as per PAN's recommendation) is to bring them within the regulatory ambit of the Bank and disclose information that becomes the basis for their monitoring and risk assessment. Before granting authorisation and / or licensing or endorsement, the Bank must be reasonably satisfied that the operations of a prospective system participant, issuers of a payment instrument or a service provider would not harm or risk harming, the soundness, safety and efficiency of the national payment system.

8.2 Ongoing Monitoring

A payment system, as defined by the BIS, consists of a set of instruments, banking procedures and interbank funds transfer systems that ensure the circulation of money.

Well designed and managed payment systems help to maintain financial stability by preventing or containing financial crises and help to reduce the cost and uncertainty of settlement, which could otherwise act as an impediment to economic activity. Payment systems not only entail payments between banks, but encompass the total payment process, including systems, mechanisms, institutions, agreements, procedures, rules and laws. Payment systems also typically involve the settlement of substantial trade in financial instruments such as bonds, equities and derivatives.

Oversight of the payment system is therefore crucial in order to reduce or contain systemic risks that could result from legal, liquidity, credit, operational, settlement and reputational risk in the payment system.

Through on-going monitoring, the Bank gets a good understanding of how the payment and settlement systems function and interact, and how use of payment instruments evolves. The oversight process relies on off-site monitoring and onsite inspections.

Offsite monitoring is conducted on an on-going basis and is highly dependent on the following:

- Data / Returns from NPS participants i.e. banks and non-banks;
- Market Intelligence i.e. media, networks etc.;

- Other Departments i.e. Banking Supervision, FIC (Financial Intelligence Centre), Exchange Control etc.;
- PAN (Payments Association of Namibia); and
- Other institutions i.e. CRAN (Communications Regulatory Authority of Namibia), NAMFISA (Namibia Financial Institutions Supervisory Authority) etc.

The data and information collected above should be intelligently collated to draw up the necessary reports and to identify risks and trends in the NPS. Reports emanating from oversight or monitoring activities are listed in section 9

8.2.1 Onsite Inspections

Onsite inspections are based on the outcome of the ***Risk Register*** and other offsite monitoring efforts. As part of its ongoing monitoring oversight activities, the Department conducts risk assessments on banks, non-bank financial institutions, payment instrument issuers, system participants and FMIs as guided by the COBIT 5 and regulation. Onsite inspections may be:

- **Pre-Opening Inspections:** This is conducted on new participants, who will be operating in the payments and settlements space, in relation to COBIT 5 and in terms of compliance with directives and determinations issued under the PSM Act, 2003, as amended. Where applicable, the Bank will have engagements with new participants between 12 – 18 months after the pre-opening inspection to discuss outstanding findings and any other relevant matters. The nature and extent (meetings, onsite or offsite monitoring) of the engagements / interventions will be informed by a risk assessment; and

- **Risk-Based Inspections:** This inspection is risk-based and focuses on areas of concern for a participant or industry as a whole. Thematic inspections based on specific determination(s), COBIT 5 processes and PFMI(s) will form part of Risk-Based inspections. The focus areas will emanate from the off-site activities conducted on the NPS and / or the participant itself. These inspections, for banks, will mostly be conducted by Banking Supervision department on the advise from the Payment and Settlement Systems Department

The assessment frequency for risk-based inspection:

- Periodic onsite inspections are based on the magnitude and nature of the risks identified from the on-going off-site activities. As part of the annual onsite inspection planning for the following year, participant risks will be assessed and prioritised as per the ***Risk Register***. Should there be no significant or material risks identified for a participant, an onsite will not be undertaken. The onsite inspection list will be approved by the appropriate structures within the Department, as part of the annual onsite inspection planning and where applicable, will be shared with the Banking Supervision Department to inform the overall onsite priority list for a particular year.
- Findings from the onsite inspections will be monitored through the off-site activities.

The above assessments shall be carried out in accordance with the planned activities and schedule of the Bank's unit in charge of payment and settlement systems oversight, as well as per the priority list for onsites as will be constructed by the Banking Supervision Department and as informed by the Oversight unit in PSSD. Each participant due for inspection for that year will be notified through official correspondence, which will provide details of the onsite inspection i.e. scope, timelines etc. Each onsite project is estimated to take a period of 3

months, depending on the nature of the engagements i.e. complexity, delays etc., which may lengthen the onsite period.

The Bank may also place reliance on independent reports i.e. assurance, internal / external audit reports etc.

8.3 Channels Through Which Payment Systems Risks are Spread

To operationalise the assessment of risks in the NPS, there are specifies three channels through which payment systems risks may have an adverse impact upon the financial sector and the wider economy:

- **Contagion:** A process whereby the financial or operational difficulties of one member of the payment system are transmitted through it to one (or more) other member(s) of the system;
- **Reputational:** A process whereby negative public opinion of a non-bank payment institution, system participant or a service provider would have on its current and prospective earnings and capital. This affects a non-bank payment institution, system participant or a service provider's ability to establish new relationships or services or continue servicing existing relationships; and
- **Disruption to Transactions:** A process whereby the financial or operational difficulties of the service provider(s), non-bank payment institution(s) or system participant (s) have so-called 'real economy' effects, by delaying, or even preventing, payments being made by financial institutions, businesses and/or consumers, or by requiring such payments to be made via materially less efficient or riskier methods than payers would freely choose.

8.4 Risk Types, Events and the Risk Register

To organise the landscape of risks in payment systems into a format which lends itself to consistent assessment and monitoring, the Bank's risk-based approach assigns risks to the payment systems risk types highlighted in section 4 above. The scope of the main risk types (and the more detailed categories of risks within each) has been defined to ensure, as far as possible, that they are all-encompassing. Within each risk type various (more granular) trigger events can give rise to settlement, reputational, general business, systemic, credit, liquidity or operational risks in a payment system. It is the basis of the analysis of such detailed events that the Bank seeks to assess the likelihood or probabilities and impacts of the various risks.

COBIT 5, as a comprehensive risk assurance framework for the management of IT risk, provides a proven and mature set of IT processes and practices suited for addressing payment systems related risks. In having a business orientation and linking business goals to IT goals, COBIT 5 provides metrics or KRIs appropriate for assisting in defining a standardised control environment for the payment systems.

8.5 Risk Assessment and Monitoring

Risk assessments are carried out against the list of risks highlighted in section 4. Greater precision in the Bank's risk assessment approach is achieved by using the available data to estimate how likely the risk might be and how much of an impact it might have. Since estimated likelihood and impacts, and supporting qualitative information, represent an assessment of risks only at a particular time, the Bank is careful to monitor existing risks and analyse new ones that may need to be reflected in future assessments. Such monitoring is facilitated by consideration of KRIs. These can be high-frequency data series which give an indication of trends in vulnerabilities, likelihood and/or impacts, based on observed events (e.g. operational performance statistics showing how many incidents of varying severity have been observed in a particular system during a particular time period). They can also take the form of qualitative information which highlights changes in a payment system's vulnerability to a specific risk and the quality of associated controls (e.g. indications from a system's audit reports that risk controls have improved or deteriorated). Monitoring such KRIs is an important part of the continual work of an overseer, and identification of a material change in a KRI can trigger a reassessment of the risk in question.

The risks identified in the ***Risk Register*** are reviewed by the Bank on an annual basis. The use of these risk estimates provides a rich set of management information which allows the Bank to monitor the risk mitigation efforts of system participants and non-bank payment institutions in a structured fashion and provides the basis for the Bank's oversight dialogue with individual system participants and non-bank payment institutions.

8.5.1 Risk Model

8.5.1.1 Assessment Guide

In determining the severity of risks associated with payment systems, 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**

8.5.1.2 Step 1 – Model for Determining the Level of Inherent Risk

Table 1 will be 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".

Impact \ Likelihood	Low	Medium Low	Medium High	High
Low				
Medium Low				
Medium High				
High				

Table 1: Model for determining Inherent Risk

8.5.1.3 Step 2 – Model for determining the strength of the Risk Management Systems

The Bank will assess 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

8.5.1.4 Step 3 - Model for determining Residual Risk

Determining Residual Risk is accomplished by balancing the **Inherent Risk** rating with the overall strength of **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

8.5.1.5 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 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 has may not become systemic and has a high impact on 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 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

8.6 Monitoring of Payment and Settlement Systems

For the purpose of monitoring the systems, information would be obtained from the non-bank payment institutions, system participants and FMIs covering various areas and through the following means:

- System design and architecture;
- Monitoring of system operations and their rules and procedures;
- Statistical data reporting forms e.g. returns;
- Questionnaires to gain relevant non-financial information;
- Onsite visits and inspections;
- Several activities and incident-related data, such as concentration ratios (for the top 3 participants), system availability rates, settlement data, custody data, depository data, etc.
- Information related to important system changes and new business developments;
- Information concerning the systems' risk exposures, if any;
- Financial data, including balance sheet and profit and loss data (for systems operated by the private companies);
- Periodic assessments of operating systems against international standards i.e. PFMI, COBIT 5 processes etc.;
- Cooperation with other financial regulatory authorities including NAMFISA, NaCC, CRAN, regional regulatory authorities i.e. SADC PSOC;
- Cooperation with other relevant bodies and stakeholders including PAN;
- Customer feedback;
- Legal opinions;
- Understanding Market practices;
- Information concerning governance and internal rules and procedures, such as board minutes, internal and external audit reports of the system participants, non-bank payment institutions and information from other financial institution regulators (like BSD etc.); and
- Bilateral and multilateral discussions.

8.7 Analysis of Information

In the course of analysing information on payment and settlement systems, attention would be paid to the following:

- Identification of risks and shortcomings in the design and operation of the payment systems i.e. system security design etc.;
- Review of systemically important and prominent payment systems against PFMI, CobiT 5 processes and the directives and determinations of the Bank;
- Assessment of changes to a system's design;
- Assessment of systems in the course of design; and
- Assessment of the system's performance and conduct i.e. activities, processing etc.

8.8 PFMI Compliance Assessment

On-going monitoring oversight activities will also include compliance assessments for PFMIs. The Bank will conduct these assessments on FMIs to determine their system's compliance with the international standards (i.e. CPSS-IOSCO PFMI), using the CPSS-IOSCO assessment methodologies. The FMIs that will be assessed, as may be appropriate, are as follows:

- NISS (Namibian Interbank Settlement System);
- Namclear; and
- CSD (Central Securities Depository).

The assessment of the FMIs will be supported and based on the PFMIs.

The assessment may be:

- **Full:** When the assessment of compliance is undertaken in relation to all or applicable principles of the proper functioning of payment systems. This assessment will be carried out for new FMIs. A full assessment can also be conducted if the Bank deems it necessary; or
- **Partial (Risk-Based**): When the assessment of compliance is undertaken in relation selected principles (but not all), based on specific areas of concern.

The above assessments of compliance shall be carried out in accordance with the plan of activities of the Bank's unit in charge of payment and settlement systems oversight. The FMI assessment will be conducted with the use of appropriate tools, methodology(ies) such as the CPSS-IOSCO Methodology, templates, as may be developed by the Bank.

The Bank may adopt the oversight expectations CSPs under the PFMI (Annexure F) and use appropriate tools i.e. CPSS-IOSCO Methodology. Compliance with the expectations may be achieved through communication by the Bank to the FMI serviced by the CSP, and the FMI obtains assurances from the CSP that it complies with the said expectations.

8.9 Description of Levels of the PFMI Compliance

The results of the PFMI assessment will be listed 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 affect significantly 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 3: PFMI - Levels of Compliance

8.10 Inducing Change

The Bank's tools to induce change include moral suasion and statutory powers, as a last resort. Having collected information through off-site monitoring and conducted onsite assessments, the Bank may in some cases conclude that the service provider, system participant or payment institution has a sufficient degree of safety and efficiency and that no further action is required. However, in other cases, it may conclude that legal and regulatory requirements or standards are not met, in which event it may decide it is necessary to induce change. In line with the Bank's philosophy of collaboration and partnership with the stakeholders, oversight seeks to promote dialogue with all payment system stakeholders with the view to creating consensus for policy choices.

This approach provides the Bank with the mechanism to exert moral suasion and to develop policy agenda by using feedback from the market and to assess the efficiency, reliability and fairness of the payment services. However, if moral suasion is not enough, the Bank may issue determinations and directives in accordance with PSM Act 18, 2003, as amended, to protect the integrity, effectiveness and security of the NPS. It may also suspend an authorisation and/or impose administrative penalties, as the law gives it the right to do so.

8.11 Cooperative Oversight

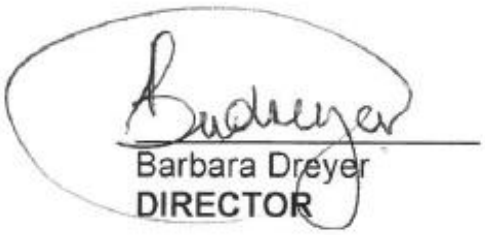
The Bank continues to work closely with other domestic and regional authorities as payment and securities settlement systems become more regionalized. Regular meetings on the oversight of regional payment systems are held with other central banks. Increasing attention is also being paid to prominent challenges and risks. These systems are overseen in co-operation with regional overseers. Co-operative oversight is led by a lead overseer, the authority with primary responsibility for overseeing the oversight subject. Co-operation is usually formalised in a Memorandum of Understanding (MoU). The frequency and depth of the oversight in terms of meetings and making assessments depend on the potential risks. Most agreements provide for a technical committee that meets relatively frequently and often reports to a high-level committee which in turn maintains contact with the managers of the system.

9. Reporting on Oversight Activities

The following reports emanating from oversight activities would be produced:

- Bi-Annual (Semester) Reports - Oversight and Fraud Reports;
- Monthly Updated System Participant and Non-Bank Payment Institution Risk Register;
- Onsite Reports;
- Financial Stability Report;
- Annual Report; and
- Other reports as may be determined from time to time.

This Payment and Settlement Systems Risk-Based Oversight Policy Framework is duly approved by:



29/11/2019.
Date

10. Annexure

10.1 System Participant, Service Provider and Non-Bank Payment Institution Risk Register

Risk Categorisation									Inherent Risk Assessment			Risk Management Systems					Residual Risk
Risk ID	Risk Type	Date Identified	Institution	Risk Event Description	Associated COBIT 5 Process / Regulation Impacted by Risk Event	Trigger (conditions that caused the risk to occur)	Reason for Likelihood	Reason for Impact	Inherent Risk Likelihood	Inherent Risk Impact	Matrix Score	Board & Senior Management	Policies & Procedures	Management Information Systems	Internal Audit & Internal Controls	Overall Rating for RMS	Residual Risk Likelihood
1	Cyber Risk	01/01/2019	BON	Cyber-attack led to online banking system to be offline.	Manage Security	Ransomware	Weak network	Mass-wide / public impact is significant, which also affects trade	Low	Medium High	Medium Low	Not Adequate	Not Adequate	Adequate	Adequate	Needs Improvement	High

10.2 Applicability of CPSS-IOSCO PFMI per Category of Payment Systems

Principles for Financial Market Infrastructures (PFMIs)

In its oversight and development work, a central bank uses the standards and guidelines published by the Bank for International Settlements (BIS)'s Committee on Payment and Settlement Systems (CPSS). These Principles are intended to be used as universal guidelines to encourage the design and operation of safer and more efficient systemically important payment systems world-wide as the safety and efficiency of payment systems are critical to the effective functioning of the financial system. Although systemically important payment systems are normally considered to be those that transmit large or high-value transactions, they include all systems that could, if they are not sufficiently protected from risk, transmit disruptions among participants and in the financial area more widely, particularly in times of market stress. Robust payment systems are, therefore, a key requirement in maintaining and promoting financial stability.

Several sets of standards and procedures were developed over time to promote the development and compliance of other financial market infrastructures internationally. These were developed by the BIS CPSS and the International Organisation of Securities Commissions (IOSCO) and included "Recommendations for Securities Settlement Systems" (November 2001), "Recommendations for Central Counterparties" (November 2004) and two consultative reports, "Guidance on the application of 2004 CPSS-IOSCO recommendations for central counterparties to OTC derivatives CCP's" and "Considerations for trade repositories in OTC derivatives markets" (January 2009). These sets of principles and standards were adopted by the IMF and World Bank as the standards by which FMI's were evaluated during Financial Sector Assessment Programmes in various countries around the world. Other reports that focussed further attention on the systemic nature of FMI's included the "Interdependencies of payment and settlement systems" (June 2008)[2].

The financial crisis of 2008 again drew the attention of authorities to the critical nature of FMI's and their potential to cause major disruptions in the financial world. Although FMI's performed well during the financial crisis, events highlighted important lessons for effective risk management. This led the CPSS and IOSCO to review and update the standards for FMI's. This was also in support of the Financial Stability Board (FSB) initiative to strengthen core financial infrastructures and markets. It was also decided that, rather than have separate documents, the principles and standards be combined into one report covering all FMI's.

Hence the new set of standards, known as "Principles for Financial Market Infrastructures" apply to systemically important payment systems, Central Securities Depositories (CSD's), Securities Settlement Systems (SSS), Central Counterparties (CCP's) and Trade Repositories (TR's). The new standards (called "principles") are designed to ensure that the infrastructure supporting global financial markets is more robust and thus well placed to withstand financial shocks. The following section provides an overview of the 24 principles contained in the document and the five responsibilities

[2] To view any of the documents mentioned please see www.BIS.org

of central banks, market regulators and other relevant authorities responsible for financial market infrastructures.

The principles for FMIs are divided into 5 categories, namely General Organisation; Credit Risk and Liquidity Management; Settlement; CSD and Exchange-of-Value Settlement Systems; Default Management; General business and risk management; Access, Efficiency and Transparency closing with Responsibilities. The principles are listed on the left with a brief overview of each, while the FMI that the principle is applicable to is indicated in the right-hand columns.

General organisation

Applicability to specific FMI's	PS	CSD	SSS	CCP	TR
Principle 1: Legal basis	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.					
Principle 2: Governance	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.					
Principle 3: Framework for the comprehensive management of risks	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks					

Credit and Liquidity risk management

Applicability to specific FMI's	PS	CSD	SSS	CCP	TR
Principle 4: Credit risk	**Y**		**Y**	**Y**	
An FMI should effectively measure, monitor, and manage its credit exposures to participants and those arising from its payment, clearing, and settlement processes. An FMI should maintain sufficient financial resources to cover its credit exposure to each participant fully with a high degree of confidence. In addition, a CCP that is involved in activities with a more-complex risk profile or that is systemically important in multiple jurisdictions should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would potentially cause the largest aggregate credit exposure to the CCP in extreme but plausible market					

conditions. All other CCPs should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would potentially cause the largest aggregate credit exposure to the CCP in extreme but plausible market conditions.					
Principle 5: Collateral	**Y**		**Y**	**Y**	
An FMI that requires collateral to manage its or its participants' credit exposure should accept collateral with low credit, liquidity, and market risks. An FMI should also set and enforce appropriately conservative haircuts and concentration limits.					
Principle 6: Margin				**Y**	
A CCP should cover its credit exposures to its participants for all products through an effective margin system that is risk-based and regularly reviewed.					
Principle 7: Liquidity risk	**Y**		**Y**	**Y**	
An FMI should effectively measure, monitor, and manage its liquidity risk. An FMI should maintain sufficient liquid resources in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate liquidity obligation for the FMI in extreme but plausible market conditions.					

Settlement

Applicability to specific FMI's	PS	CSD	SSS	CCP	TR
Principle 8: Settlement finality	**Y**		**Y**	**Y**	
An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real-time.					
Principle 9: Money settlements	**Y**		**Y**	**Y**	
An FMI should conduct its money settlements in central bank money where practical and available. If central bank money is not used, an FMI should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money.					
Principle 10: Physical deliveries		**Y**	**Y**	**Y**	
An FMI should clearly state its obligations with respect to the delivery of physical instruments or commodities and should identify, monitor, and manage the risks associated with such physical deliveries.					

Central securities depositories and exchange-of-value settlement systems

Applicability to specific FMI's	PS	CSD	SSS	CCP	TR
Principle 11: Central securities depositories		**Y**			
A CSD should have appropriate rules and procedures to help ensure the integrity of securities issues and minimise and manage the risks associated with the safekeeping and transfer of securities. A CSD should maintain securities in an immobilised or dematerialised form for their transfer by book entry.					
Principle 12: Exchange-of-value settlement systems	**Y**		**Y**	**Y**	
If an FMI settles transactions that involve the settlement of two linked obligations (for example, securities or foreign exchange transactions), it should eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other.					

Default management

Applicability to specific FMI's	PS	CSD	SSS	CCP	TR
Principle 13: Participant-default rules and procedures	**Y**	**Y**	**Y**	**Y**	
An FMI should have effective and clearly defined rules and procedures to manage a participant default. These rules and procedures should be designed to ensure that the FMI can take timely action to contain losses and liquidity pressures and continue to meet its obligations.					
Principle 14: Segregation and portability					**Y**
A CCP should have rules and procedures that enable the segregation and portability of positions of a participant's customers and the collateral provided to the CCP with respect to those positions.					

General business and operational risk management

Applicability to specific FMI's	PS	CSD	SSS	CCP	TR
Principle 15: General business risk	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should identify, monitor, and manage its general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that it can continue operations and services as a going concern if those losses materialise. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly					

wind-down of critical operations and services.					
Principle 16: Custody and investment risks	**Y**	**Y**	**Y**	**Y**	
An FMI should safeguard its own and its participants' assets and minimise the risk of loss on and delay in access to these assets. An FMI's investments should be in instruments with minimal credit, market, and liquidity risks.					
Principle 17: Operational risk	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.					

Access

Applicability to specific FMI's	PS	CSD	SSS	CCP	TR
Principle 18: Access and participation requirements	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should have objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access.					
Principle 19: Tiered participation arrangements	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should identify, monitor, and manage the material risks to the FMI arising from tiered participation arrangements.					
Principle 20: FMI links		**Y**	**Y**	**Y**	**Y**
An FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks.					

Efficiency

Applicability to specific FMI's	PS	CSD	SSS	CCP	TR
Principle 21: Efficiency and effectiveness	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should be efficient and effective in meeting the requirements of its participants and the markets it serves.					
Principle 22: Communication procedures and standards	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement, and					

recording.					

Transparency

Applicability to specific FMI's	PS	CSD	SSS	CCP	TR
Principle 23: Disclosure of rules, key procedures, and market data	**Y**	**Y**	**Y**	**Y**	**Y**
An FMI should have clear and comprehensive rules and procedures and should provide sufficient information to enable participants to have an accurate understanding of the risks, fees, and other material costs they incur by participating in the FMI. All relevant rules and key procedures should be publicly disclosed.					
Principle 24: Disclosure of market data by trade repositories					**Y**
A TR should provide timely and accurate data to relevant authorities and the public in line with their respective needs.					

Oversight Responsibilities of Central Banks, Market Regulators, and Other Relevant Authorities for Financial Market Infrastructures

Responsibility A: Regulation, Supervision, and Oversight of FMIs
FMIs should be subject to appropriate and effective regulation, supervision, and oversight by a central bank, market regulator, or other relevant authority.

Responsibility B: Regulatory, Supervisory, and Oversight Powers and Resources
Central banks, market regulators, and other relevant authorities should have the powers and resources to carry out effectively their responsibilities in regulating, supervising, and overseeing FMIs.

Responsibility C: Disclosure of Policies with Respect to FMIs
Central banks, market regulators, and other relevant authorities should clearly define and disclose their regulatory, supervisory, and oversight policies with respect to FMIs.

Responsibility D: Application of the Principles for FMIs
Central banks, market regulators, and other relevant authorities should adopt the CPSS-IOSCO Principles for financial market infrastructures and apply them consistently.

Responsibility E: Cooperation with Other Authorities
Central banks, market regulators, and other relevant authorities should cooperate with each other, both domestically and internationally, as appropriate, in promoting the safety and efficiency of FMIs.

(*Summarised from the publication "Principles for Financial Market Infrastructures", BIS. 2012*)