Bank of Namibia

CYBERSECURITY IN THE NATIONAL PAYMENT SYSTEM (NPS)

OBSERVANCE OF CPSS-IOSCO1 PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES (PFMI) AND CYBER RESILIENCE OF FMI

ACCRA – GHANA

02 FEBRUARY 2024

Bank of Namibia

CONTENT

NATIONAL PAYMENT SYSTEM DEPARTMENT (NPSD) MANDATE

- To ensure the **safe, secure, efficient** and **cost-effective** operation of NPS.
- To determine standards to ensure that **bank fees** and **charges** payable by customers are the public interest; promote competition; efficiency; and cost-effectiveness

NPSD supports the following objectives of the Bank:

- **Safeguard and Enhance Financial Stability**
- Optimize **Organizational Efficiency** and **Cost-Effectiveness**
- Promote **Financial Sector Development**
- Promote **Regional Integration**

THE REGULATORY ENVIRONMENT

Legal Framework	Bank of Namibia Act, 2020 (No. 1 of 2020)
	Payment Systems Management Act (No. 14 of 2023)
	Banking Institutions Act, 1998 (No.2 of 1998), as amended

Regulatory Framework (Determinations)

- PSD-1 Payment Instruments
- PSD-3 E-Money
- PSD-4 Conduct of Cards
- PSD-5 Basic Bank Account & Cash Deposit Fees
- PSD-6 Access & Participation
- PSD-7 Efficiency in the NPS
- PSD-8 Administrative Penalties
- PSD-9 EFT Transactions
- PSD-10 Fees and Charges
- PSD-11 Card Interchange
- **PSD – 12 Operational & Cyber Security**

Bank of Namibia

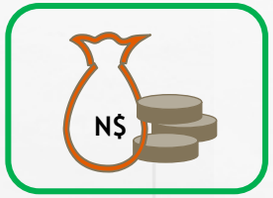
THE REGULATORY ENVIRONMENT

- PSD-12 - **Operational & Cyber Security**
  - **This Determination provides the principles and key risk indicators for the risk management of cyber security and operational resilience in the National Payment System.**
  - **Governance - Role of the Board and Senior Management – Framework**
  - **Vulnerability Management – Identification, Protection, Detection, Response and Recovery**
  - **Risk-Based Risk Indicators and Tolerance Levels**

THE NPS PAYMENTS LANDSCAPE AND ARRANGEMENTS

Customers i.e., individuals, businesses, institutions etc.

ATMs, POS Devices, Mobile Apps, USSD, Agents, Branches etc.



Banks

Banks and Non-Banks

FMIs and Service Providers

Rules, Standards etc.

Laws, Regulations, Policies etc.

Bank of Namibia

CYBER SECURITY ASSESSMENT: 2019

Regulatory Guidance	Institutions in scope
Determination on Information Security (BID-30)	— Bank Windhoek Limited — First National Bank Namibia Limited — Nedbank Namibia Limited — Standard Bank Namibia Limited — Namclear (Pty) Ltd
COBIT 5	
Information security principles of the Payment Card Industry Data Security Standard (PCI DSS)	
Principle 17 of the Principles for Financial Market Infrastructures (PFMI)	— Namclear (Pty) Ltd

Ongoing Cyber Security Interventions

- The Committee on Payments and Market Infrastructures (CPMI) “toolkit” to support central banks that wish to reduce the risk of wholesale payments fraud related to endpoint security in their institutions and jurisdictions.
  - Operator assessed the seven (7) elements designed to address areas relevant to preventing, detecting, responding to, and communicating wholesale payment fraud.
  - Action plan developed in conjunction with industry to address gaps.
- Cyber Security Council (Council) established in 2023:
  - The Cybersecurity Council Working Group (WG) aims to identify, assess, and recommend solutions to the industry's cybersecurity challenges.

Ongoing Cyber Security Interventions

- Cybersecurity Assessments – Started 2023, and to continue in 2024 (IMF technical resource supports Banking Supervision. Payments system resource accompanying for capacity building)
- PFMI Assessment on Namclear to be conducted during 2024. Ongoing attempts to source resources to engage IMF to support cyber security assessment.
- National CSIRT setup ongoing. Led by Communications Regulatory Authority in Namibia, with input from the financial sector. Discussion on sectorial CSITs is ongoing.

Challenges

- Challenges
  - Capacity of the overseers
  - Resource constraints
  - Knowledge at regulatory level and governance of participant board level


THANK
YOU