Observance of CPSS-IOSCO Principles for Financial Market Infrastructures (PFMI) and Cyber Resilience of FMI

Cyber Resilience for FMI

Tanzania - Experience

Friday, February 2, 2024

F. L. Kasole

Outline

- BOT Mandate
- NPS Structure
- Payment Systems Categories
- ICT Security Initiative
- ICT Security Governance
- Cyber Resilience
- Training and Challenges

Bank of Tanzania Mandate

BOT Act 2006

Sec 6

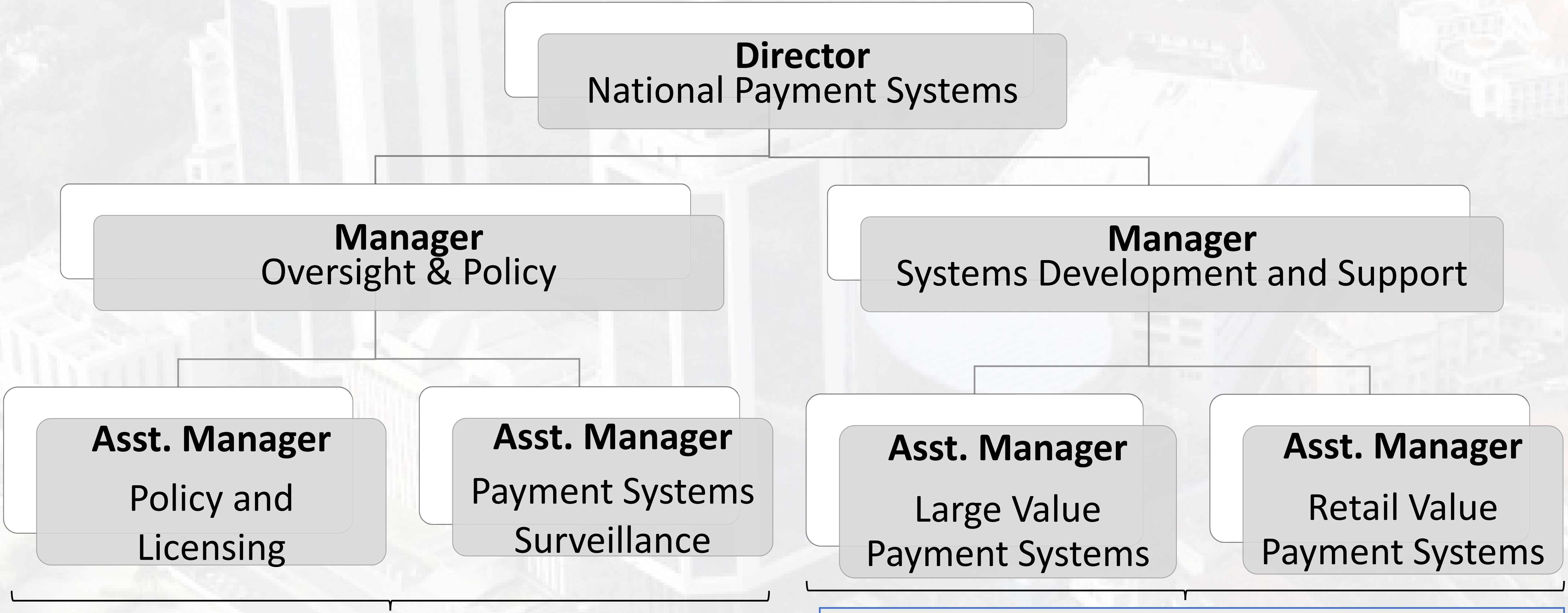
1. Regulate, monitor, and supervise the payment, clearing and settlement system including all products and services;
2. Conduct oversight functions on the payment, clearing and settlement systems in any bank, financial institution or infrastructure service provider or company;
3. Participate in any such payment, clearing and settlement systems;
4. Establish and operate any system for payment, clearing or settlement purposes;

NPS Act 2015,

Sec 4

1. Grant a licence and approval in accordance with this Act;
2. Regulate, supervise, investigate and oversee the operations of payment systems;
3. Provide settlement services to payment systems;
4. Provide settlement services to a clearing-house and a central securities depository;
5. Own and operate a real-time gross settlement system;
6. Co-ordinate payment systems activities with relevant stakeholders;
7. Participate in inter-bank clearing and settlement operations.

NPS: Directorate Structure:



Director
National Payment Systems

Manager
Oversight & Policy

Manager
Systems Development and Support

Asst. Manager
Policy and Licensing

Asst. Manager
Payment Systems Surveillance

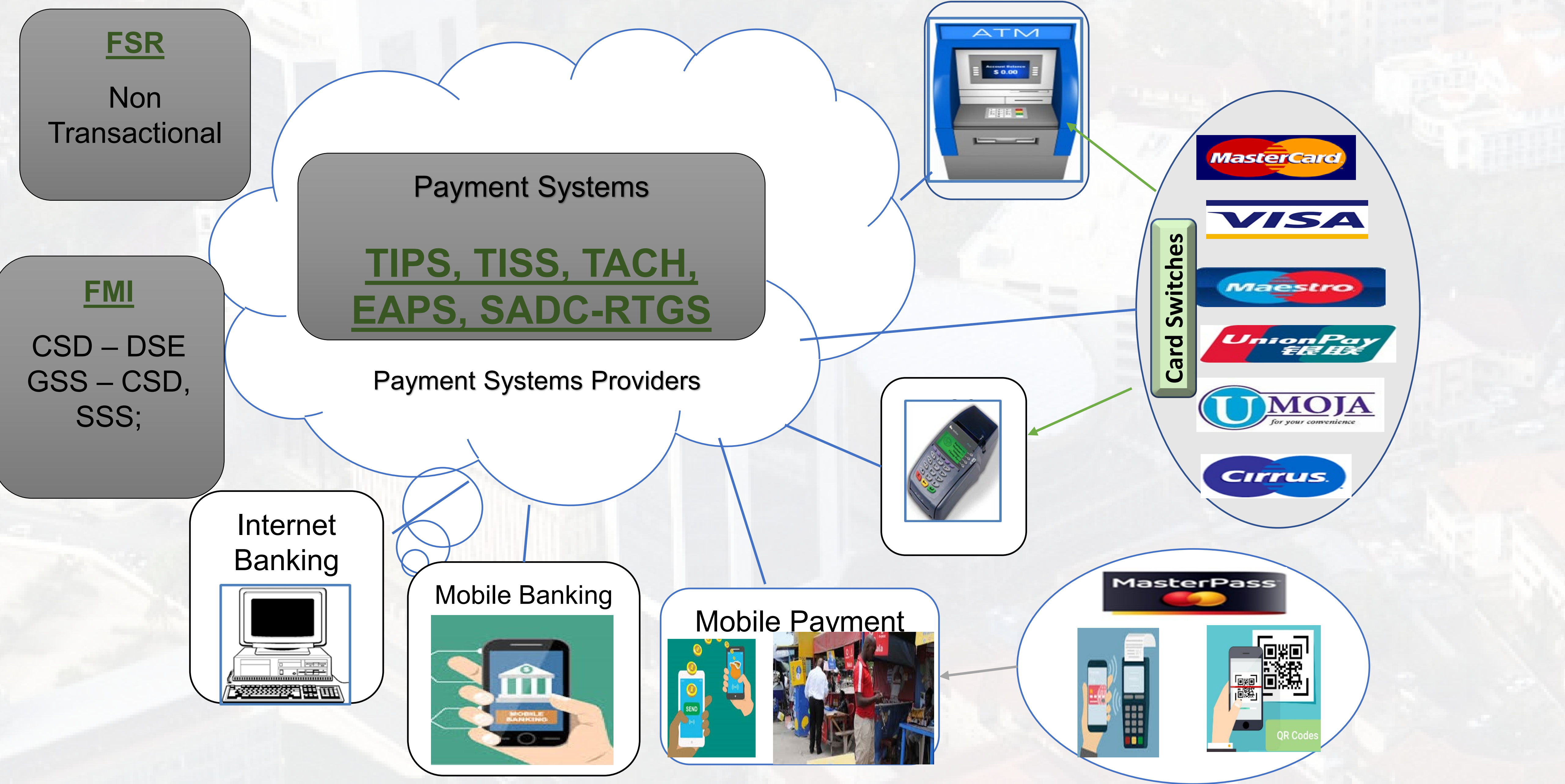
Asst. Manager
Large Value Payment Systems

Asst. Manager
Retail Value Payment Systems

Responsible for preparation of policy, Regulatory Framework, Licensing and Oversight of Payment Systems

Responsible for implementing, maintaining, and operational of Settlement and Clearing systems and retail payment systems, e.g. RTGS, TIPS, Cheque system, EFT, mobile payments, remittances and card systems

National Payment Systems Categories



FSR

Non Transactional

FMI

CSD – DSE
GSS – CSD,
SSS;

Payment Systems

TIPS, TISS, TACH, EAPS, SADC-RTGS

Payment Systems Providers

Card Switches

Internet Banking

Mobile Banking

Mobile Payment

Laws on Cyber Security

National Policy:

1. National ICT Policy 2003
2. National ICT Policy 2016

Acts:

1. The Cybercrime Act, 2015
2. Other supporting acts
   - i. The Electronic Transactions Act, 2015
   - ii. The National Payment Systems Act, 2015

BOT ICT Policies and Guidelines:

1. IT security Policy
2. Physical security Policy
3. IT security framework
4. BCP/BCM policy
5. Recovery procedure manuals
6. Enterprise architecture

Regulations:

1. The Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2018; amended in 2023
   - i. Internet Service Providers Minimum Security Guidelines
   - ii. Domain Name System Security Extension (DNSSEC) Deployment Guideline

National Initiative

1. Establishment of:
    1. Computer Emergency Response Team (CERT);
    2. Cybercrime Unit under the Tanzania Police Force; and
    3. Central Equipment Identification Register (CEIR)
        - ✓ safety issues of electronic communication devices

Bank of Tanzania Initiative

1. Establishment of:
    - ✓ Financial Computer Emergency Response Team (FinCERT); a specialized unit that will monitor, detect and respond to cyber incidents affecting the financial sector

ICT Security Governance

SECURITY MANAGEMENT FRAMEWORK	❖Provides: ✓Governance Structure for Physical and Information security management; ✓Roles and Responsibility of the Board and its Committees, Bank’s Committees, Heads of Directorates/Departments and employees
Directorate of Management Information Systems	✓Information System Services and Cyber Security department
Risk Management Department	✓Systems Risk department

Cyber Resilience

Detection:

❖Tools for monitoring and logging at network and database levels

Recovery:

❖Backup and recovery (cold and hot), and quarterly testing

Reporting :

❖Any suspicious activity is reported to Director management information system for intervention and escalation to the Information security management structure.

Test:

1. Penetration test
2. Vulnerability scan

Preventions

❖For FMI and other critical systems, the Bank look at six entry points for cyber-attack.

i. Business process (maker and checker), two factor authentication.

ii. Software - allows access and installation of approved software.

iii. Hardware - control all IT devices accessing Bank network.

iv. Interfaces with other exertional and intern systems – conformance to CIA

v. Network – segregated FMI network and controlled access

vi. People (staff) – each staff must undergo subscribed mandatory training on cyber security particularly on Social Engineering, Phishing, Ransomware, and strong password.

Training & Challenges

Training

- All staff are provided with training on Cyber security

  e.g Phishing, Social Engineering, Password, Ransomware

Challenges

- Human and financial recourses

- Compliance to FMI cyber security resilience guidelines

“ ~ Asante Sana-
Me da wo ase ~ ”