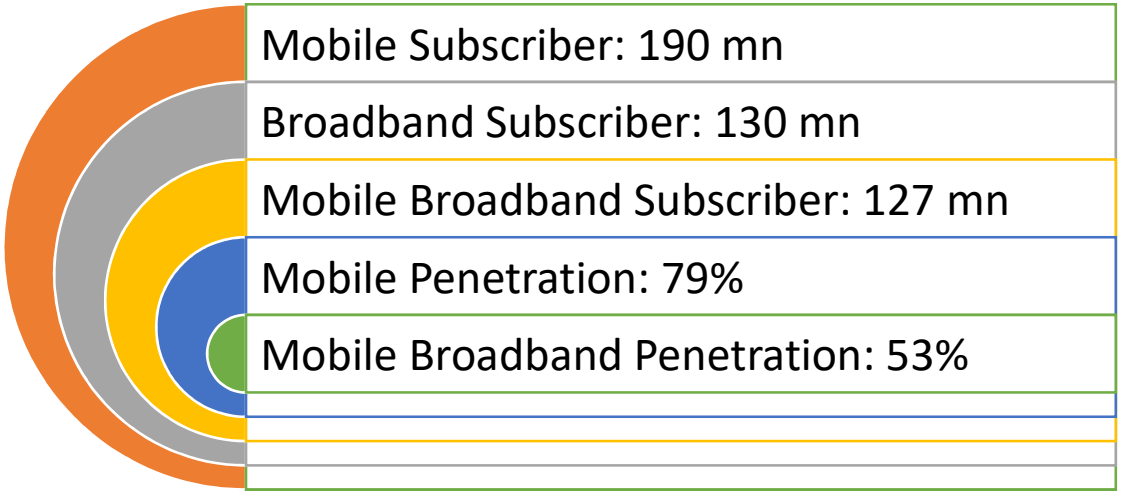
Security of Digital Financial Services in Pakistan

Rehan Masood
Joint Director, Payment Systems & Oversight Department
Digital Financial Services Group
State Bank of Pakistan

Country Demographics

Surface Area:	796,095 Sq. km
Financial Inclusion:	~50%
GDP:	~USD 375 billion
Per Capita Income:	~USD 1,550
Remittance % of GDP	~8%

Mobile and Internet Usage in Pakistan



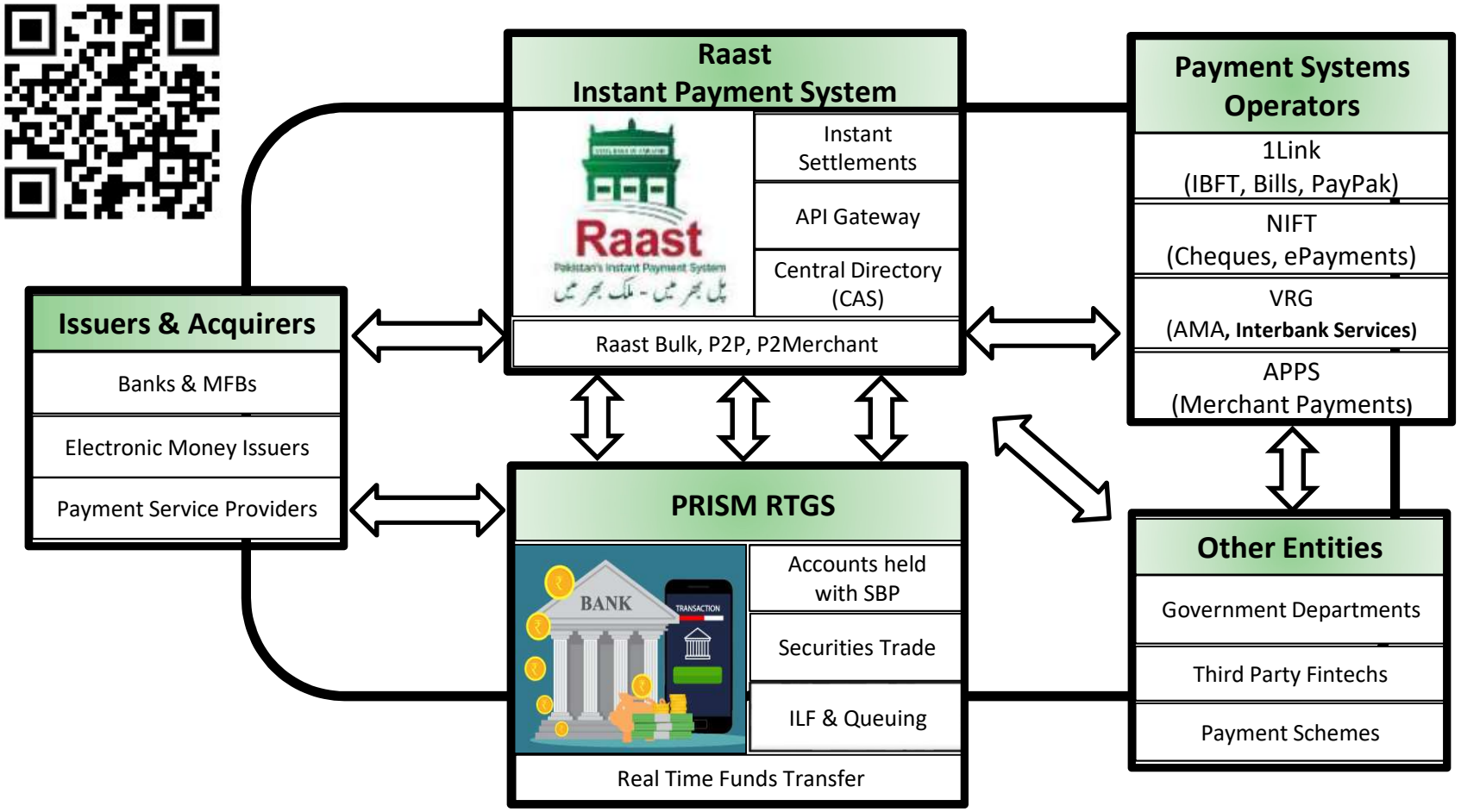
Population : 241 M
Male : 49%
Female : 51 %
Ratio: 104.6

Population: Below the age of 15 yrs: **29%**
Between the age of 15-30 yrs: **35%**
Above the age of 30 yrs: **36%**
NADRA ID: 110 Million
Issued to 46% of the population

Overseas Pakistanis
More than 9 Million
More than 50% Blue Collar Workers

Population data as per the 2023 digital census

Vision of National DFS Infrastructure



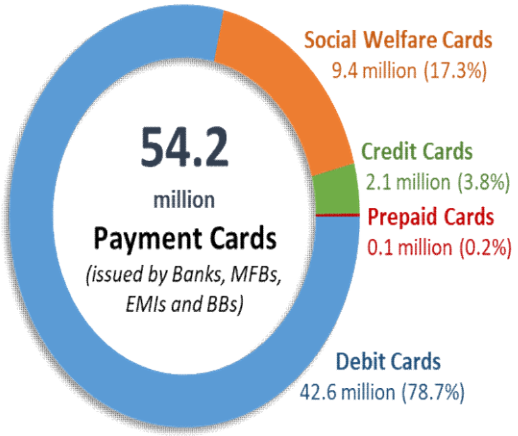
Key Statistics on DFS as of Sep 30, 2023

Mobile Banking Users
Jun-23: **16.1 mn**
Sep-23: **17.0 mn**
↑6.0%

BB App Users
Jun-23: **57.8 mn**
Sep-23: **61.3 mn**
↑6.1%

Internet Banking Users
Jun-23: **9.6 mn**
Sep-23: **10.3 mn**
↑6.8%

EMI Wallet Users
Jun-23: **2.0 mn**
Sep-23: **2.4 mn**
↑18.1%



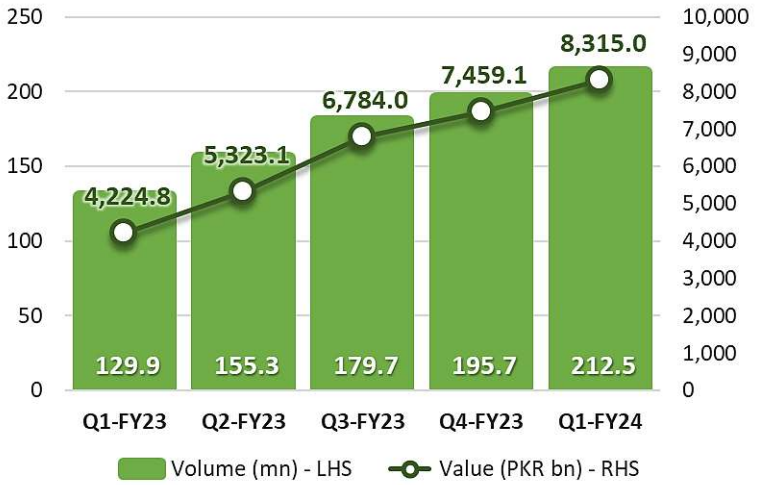
18,117 ATMs
facilitated **214.6 mn** transactions amounting **PKR 3,294 bn**

118,444 POS Machines
facilitated **59.8 mn** card present purchases amounting **PKR 323 bn**

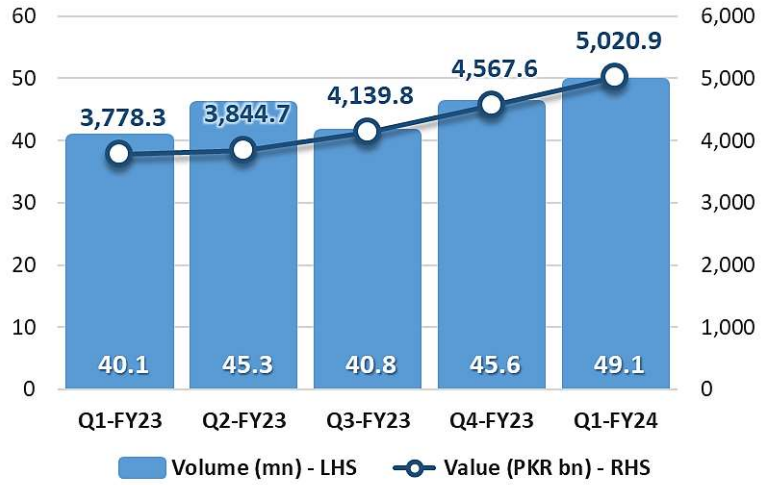
7,310 E-Merchants
registered with Banks/ MFBs processed **9.6 mn** transactions worth **PKR 40 bn**

Growth in Internet & Mobile Banking

Mobile Banking



Internet Banking



DFS Stakeholders

- Users
- Mobile Network Operators (MNOs)
- DFS Providers
- Retail Agents
- Banking Regulators
- Telecom Regulators
- Identity Verification Services
- Third Party Service Providers

Major DFS Risks

- Social engineering
  - UAN spoofing
  - Impersonation scams
  - Phishing (emails, websites, WhatsApp)
- SIM swapping
- Fake biometrics
  - Silicon-based fake thumbprints
- Card frauds
  - E-commerce (CNP)

SBP developed Mobile App Security Framework for DFS providers

- Draws on principles from several standards:

  OWASP top-10 ISO/IEC 27000 PCI/DSS NIST 800-53

- Core of the framework is based on ITU-T Rec. X.805:

  Access control, authentication, nonrepudiation, data confidentiality, communication security, data integrity, availability, privacy

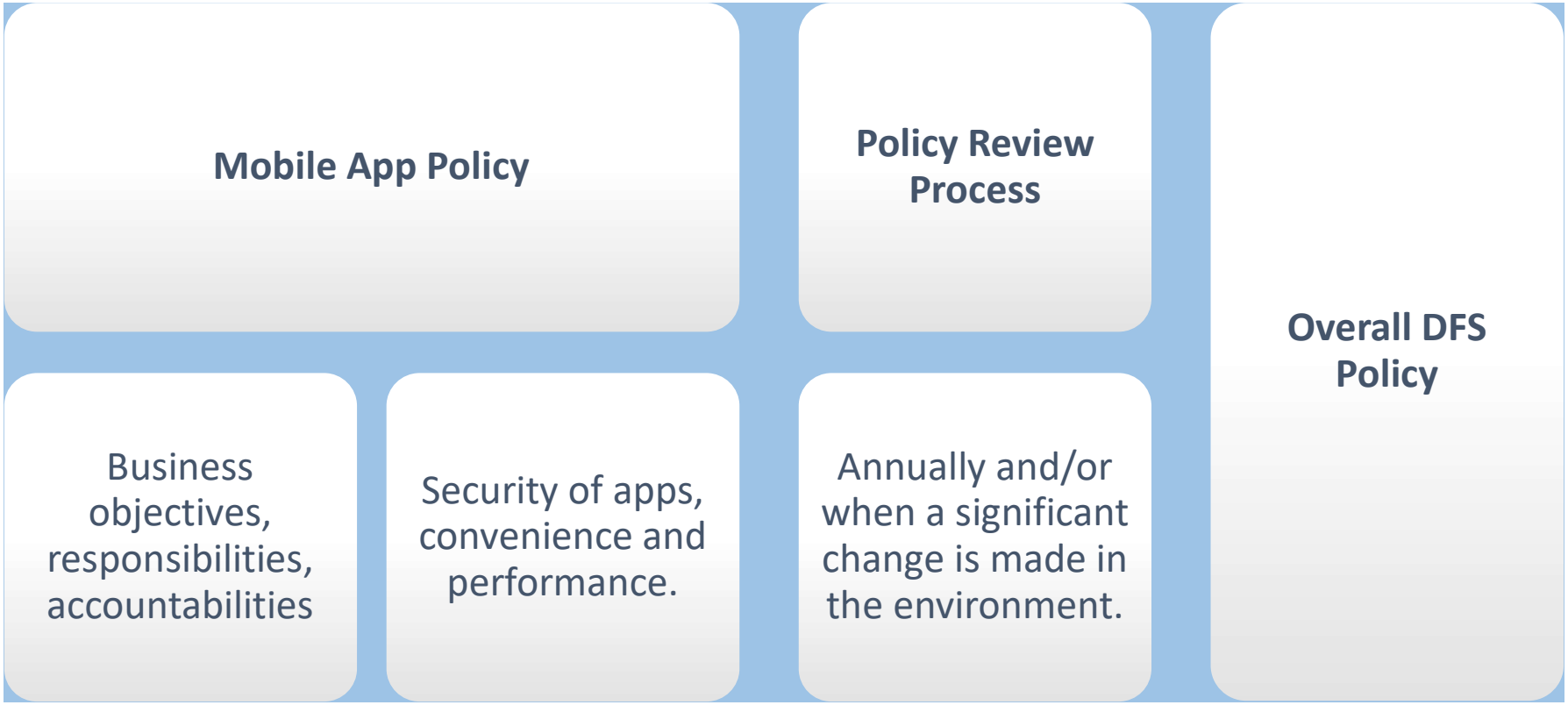
App Security Framework provides baseline security controls for DFS providers

- App owners shall use this framework for:
  - Architecture
  - Design
  - Development and
  - Deployment

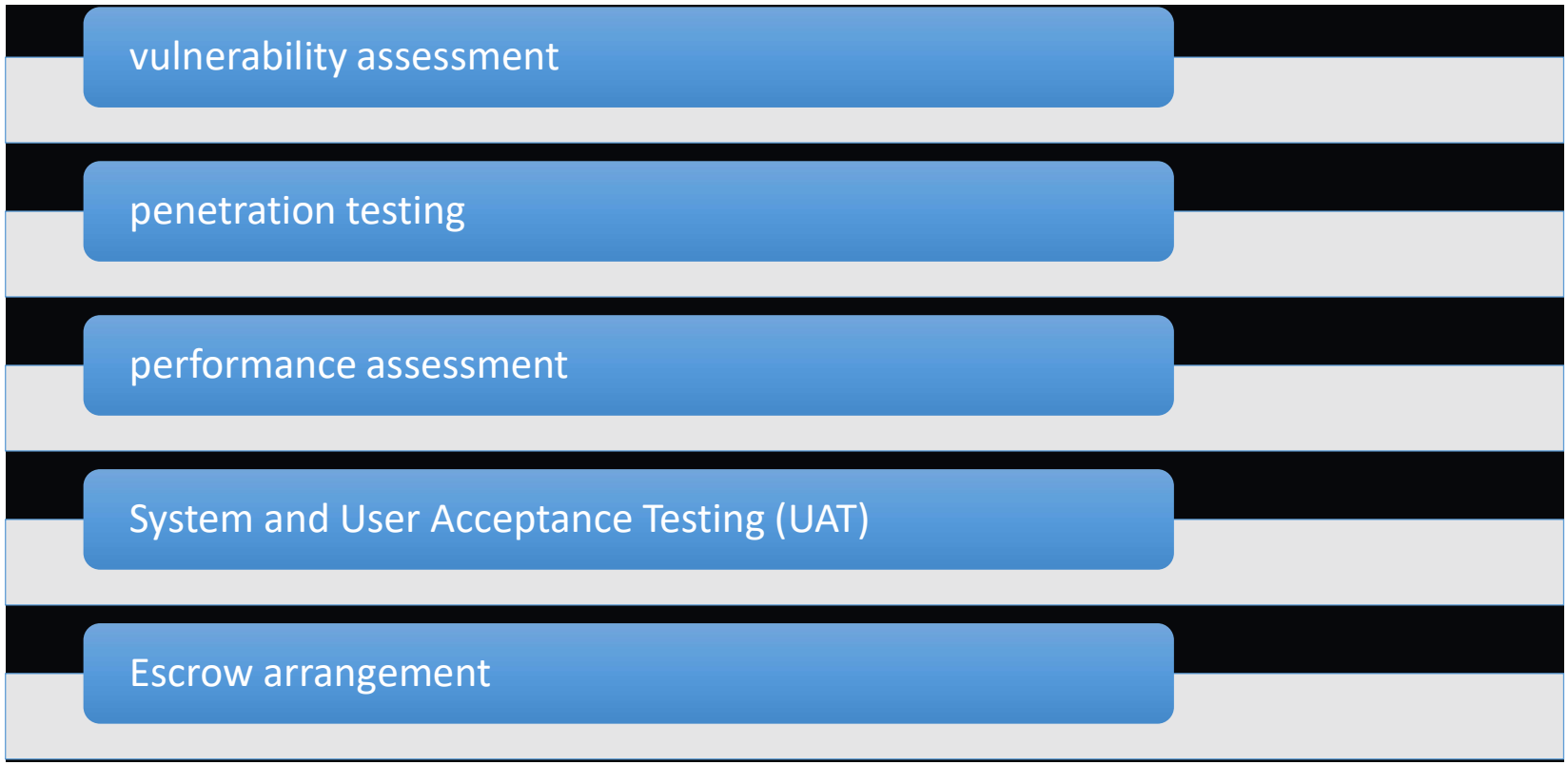
- App owners shall ensure that the requirements in this framework are used by architects, developers, testers, security professionals, and consumers to define and understand the qualities of a secure mobile app.

- The requirements of these Guidelines cover the entire mobile app ecosystem involved in capturing, storing, processing and transmitting financial/non-financial information, which includes but is not limited to mobile apps, web services, server-side databases, storage and network communications etc.

General Requirements – App Development Policy



General Requirements – Testing & Assessments



Mobile App Security Requirements

A. Mobile Application Architecture
B. Device Binding/Registration
C. User Authentication and Authorization
D. Protection of Sensitive Payment Data and Personal Data
E. Network and Interfacing Security
F. Session Management
G. Tampering Detection
H. App Permissions

I. Secure Coding
J. Input and Output Handling
K. Error and Exception Handling
L. Monitoring, Logs and Data Leakage
M. App Vulnerability Assessment, Patching and Updating
N. Application Programming Interface (APIs)
O. Customer Awareness

User Authentication and Authorization

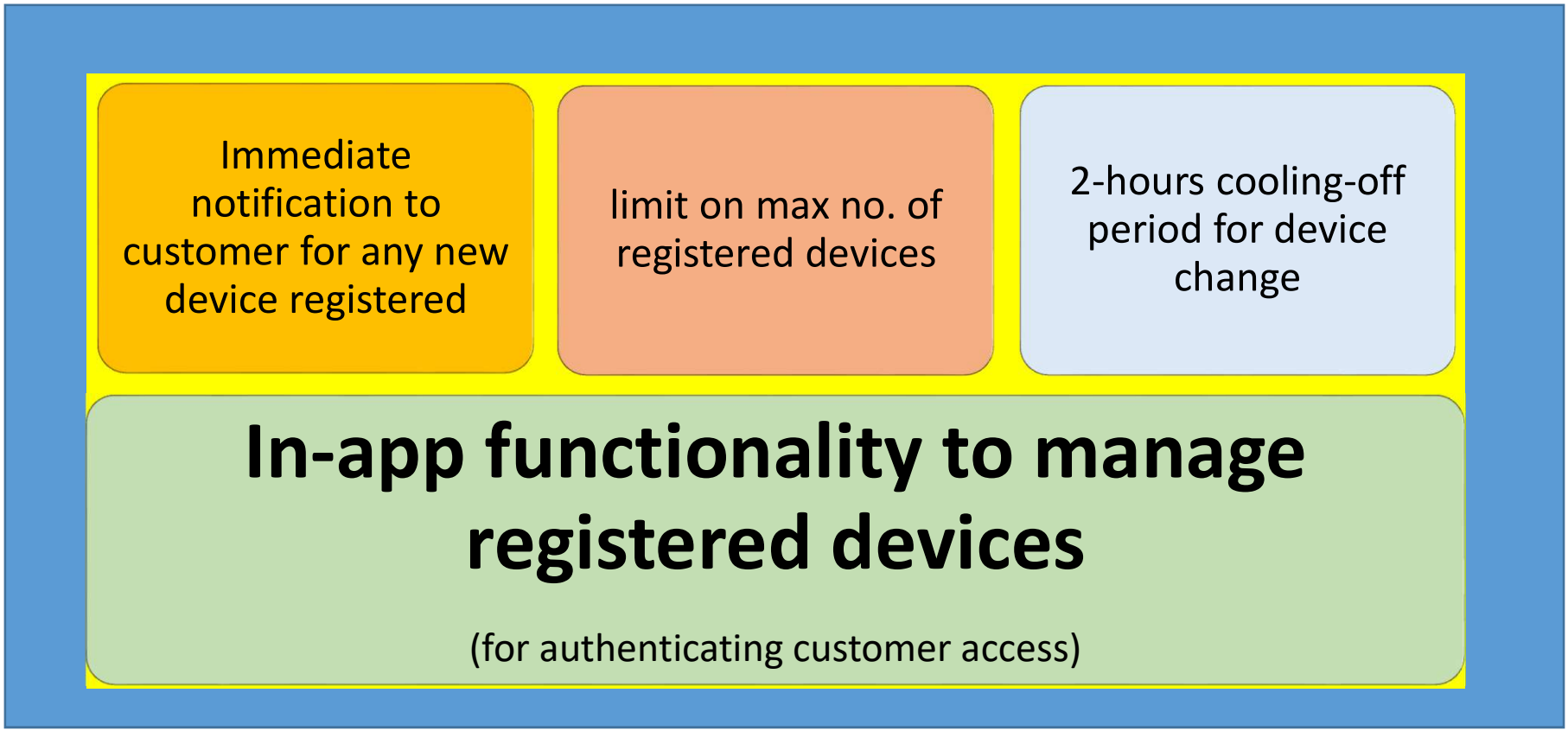
Customer consent-based activation of app.

Strong customer authentication mechanism

- MFA
- Strong passwords
- TOTP
- OTP auto-fetching
- Max No. of failed authentication attempts
- inactive mobile sessions
- Server-based auth
- Logs

A login authentication and a risk-based financial-value-based transaction authentication shall be in place.

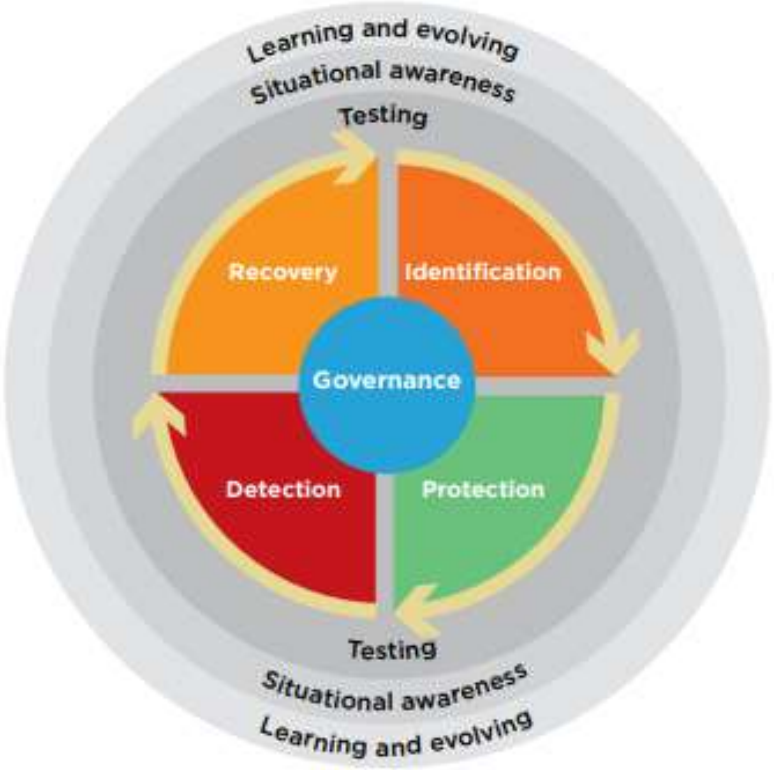
Device binding



Fintech Security and Digital Financial Inclusion in Pakistan

Day 1: Session 4

SBP's Cybersecurity supervisory framework is based on international standard & best practices. Our regulatory regime is not one-size fit all.

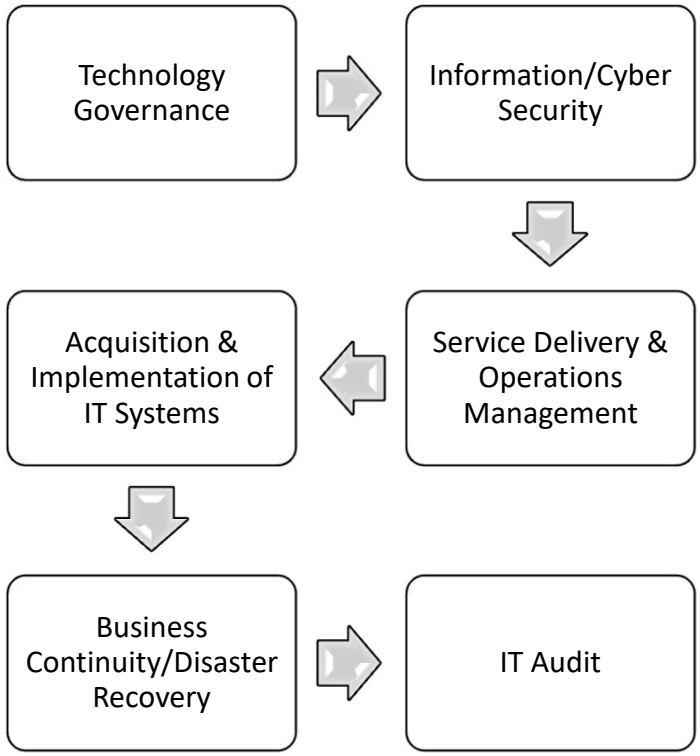


Source: CPMI-IOSCO Guidance, 2016

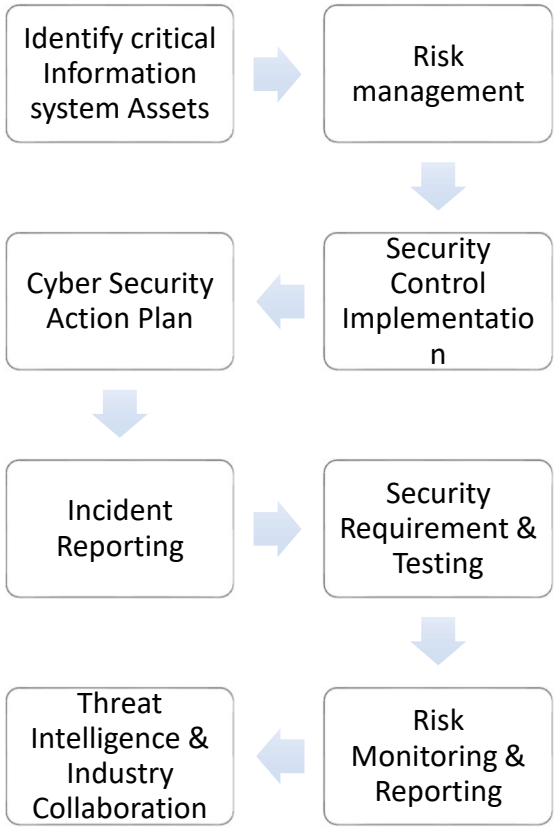
Technology Agnostic → Platform-neutral → Outcome based

SBP's Enterprise Technology Governance Framework

Technology Governance Framework



Cybersecurity Framework



Evolution of Security in DFS

Basic card security

tamper resistant signature panel

Card embossing

PIN (Personal Identification Number)

microprint security features

1950-1970

Real-time electronic authorization

Europay, MasterCard, Visa (EMV) Specifications for card security issued in 1994

PCI Security Standards issued in 2006

2-Factor Authentications

1985-2000s

Biometrics

Tokenization Services

Chip & PIN Standards

Geolocation

3DS

3rd party authentication Services

Present

As regulator, SBP has issued various instructions to regulate the safe and efficient use of digital financial services in Pakistan

Enterprise Technology Governance Framework

Governs the use of technology in Banks as an enterprise

PSD's Card Security Framework

Internet Banking Security Regulations

App Security Framework

Instructions on Security of Customer Facing Channels/Interfaces

Protection of Sensitive Data

- PCI-DSS
- Sensitive information not to be stored on mobile devices
- Use of industry standard cryptography
- Encryption of sensitive data in-transit and at rest
- Sensitive data shall not be transmitted through vulnerable channels

Monitoring, Logs and Data Leakage

Tools to monitor user behavior & anomaly detection

Mobile app logs shall not contain any sensitive data

Log server shall be segregated from application servers

Protect logs from unauthorized modification or destruction

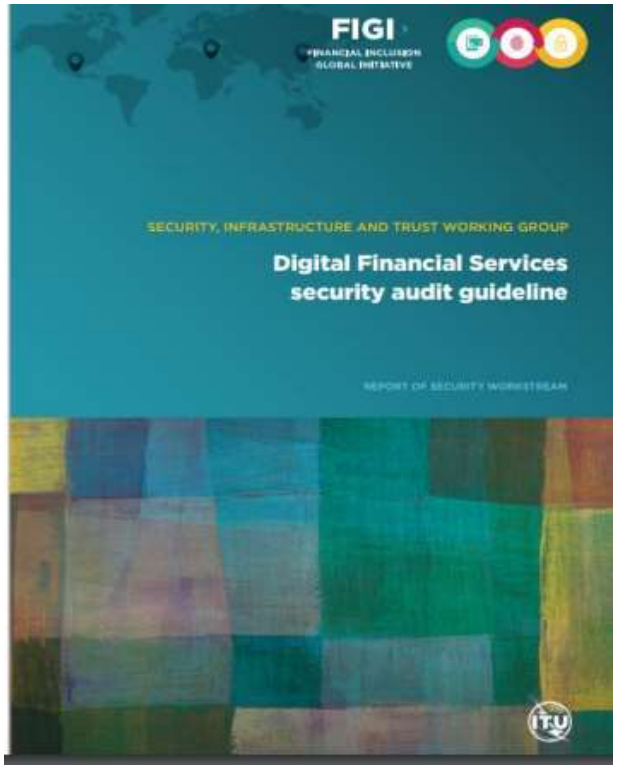
Audit logs shall be maintained at the server level

DLP Solution

Retain logs

How the regulators can ensure compliance?

- Self assessments by the DFS providers
- Internal audit reports
- Regular and thematic onsite inspections
- Penalties for non-compliance
- Third party security assurance
- Incident reporting



Thanks!


SBP
STRATEGIC PLAN
2023 - 2028
SBP
VISION
2028
State Bank of Pakistan