Securing Mobile Payment Applications

ITU Digital Financial Services (DFS) Webinar

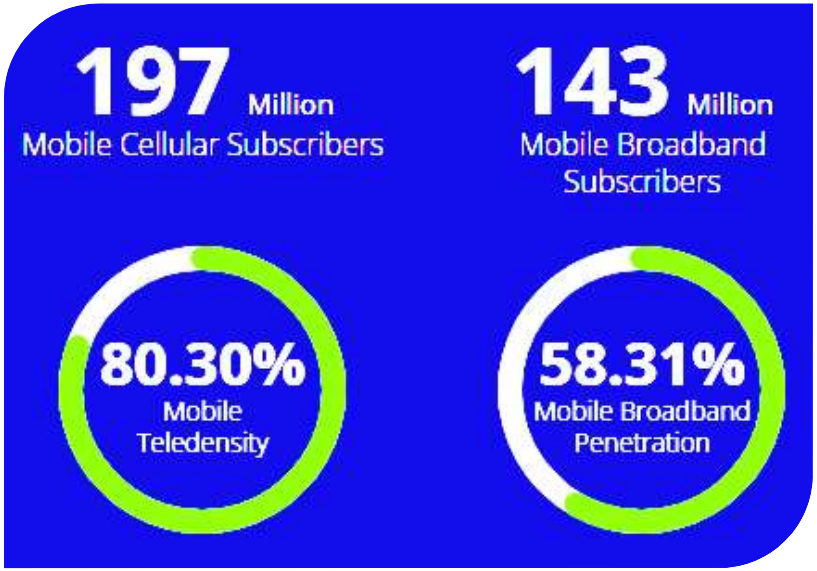
Rehan Masood
State Bank of Pakistan

The content presented in this slide deck is solely the opinion and perspective of the presenter.
It does not necessarily reflect the views or position of the SBP.
SBP is not responsible for the content, opinions, or statements expressed by the presenter during this webinar.

Prelude

Background & Introduction of Pakistan's Digital Payments Landscape

Mobile app users of digital financial services are on the rise



64.3 mn
Branchless Banking App Users

13.3 mn
Internet Banking Portal Users

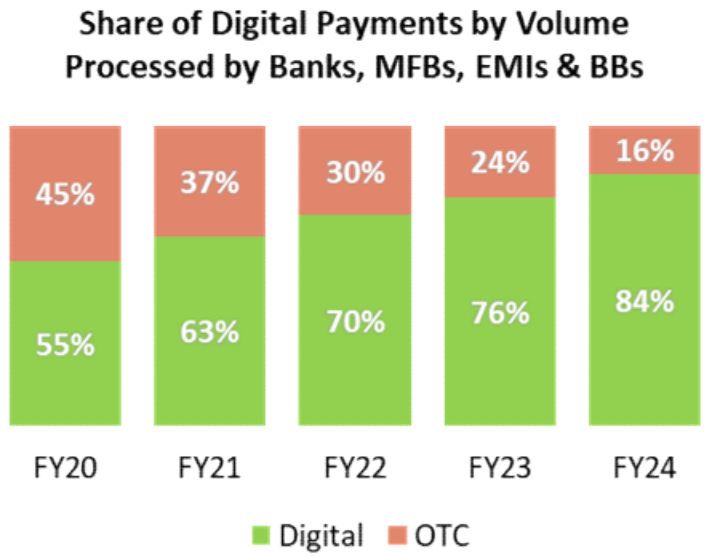
21 mn
Mobile Banking App Users

4.7 mn
e-Wallet Users
(EMI's wallet)

Retail Payments during FY 2024

(by volume)

(processed by Banks, MFBs, EMIs and BBs)



POS: Point-of-Sale Machines | **IB**: Internet banking | **MB**: Mobile Banking Apps | **BB**: Branchless Banking | **OTC**: Over-the-Counter

Trends: Digital Payments

Transactions via		Volume (in million)			Value (in PKR billion)		
Branchless Banking App Wallets		FY24	2,697 mn	↑58%	FY24	PKR 8.8 tn	↑119%
		FY23	1,705 mn		FY23	PKR 4.0 tn	
Mobile Banking Apps		FY24	1,123 mn	↑70%	FY24	PKR 46.3 tn	↑95%
		FY23	661 mn		FY23	PKR 23.8 tn	
Internet Banking Portals		FY24	223 mn	↑30%	FY24	PKR 23.5 tn	↑44%
		FY23	172 mn		FY23	PKR 16.3 tn	
E-Wallets (EMI's issued)		FY24	85 mn	↑156%	FY24	PKR 0.2 tn	↑215%
		FY23	33 mn		FY23	PKR 0.1 tn	

Raast! Pakistan's instant payment system

A payment **platform** which is:

Instant

Interbank payment processing within milliseconds, customer payment within 17 seconds

Reliable

Infrastructure as well as support available 24/7/365

Interoperable

30+ participants connected on the infrastructure

Advanced

Based on ISO20022 messaging standard. State-of-the-art API gateway to support innovation using APIs

Secure

From network connectivity till applications, higher standards of security ensured

Low cost

No membership fee, certification fee or transactional charges on Raast participants

Raast Use-Cases & Performance

Bulk Payments

P2P Payments

P2M Payments

~ 40 Participants

~44 Million Raast IDs

~ 1.612 billion Transactions

~ 5 Million Daily Transactions

SBP's app security framework

Major mobile app vulnerabilities & threats

- Insecure Authentication/Authorization
- Insufficient Input/Output Validation
- Insecure Communication
- Inadequate Privacy Controls
- Unintended Data Leakage
- Security Misconfiguration
- Insecure Data Storage
- Insufficient Cryptography

- Social Engineering
- Phishing/Vishing
- UAN spoofing
- SIM swapping

General Requirements – App Development Policy

Business objectives, responsibilities, accountabilities

Security of apps, convenience and performance.

Annually and/or when a significant change is made in the environment.

Mobile App Policy

Policy Review Process

Overall DFS Policy

General Requirements – Testing & Assessments

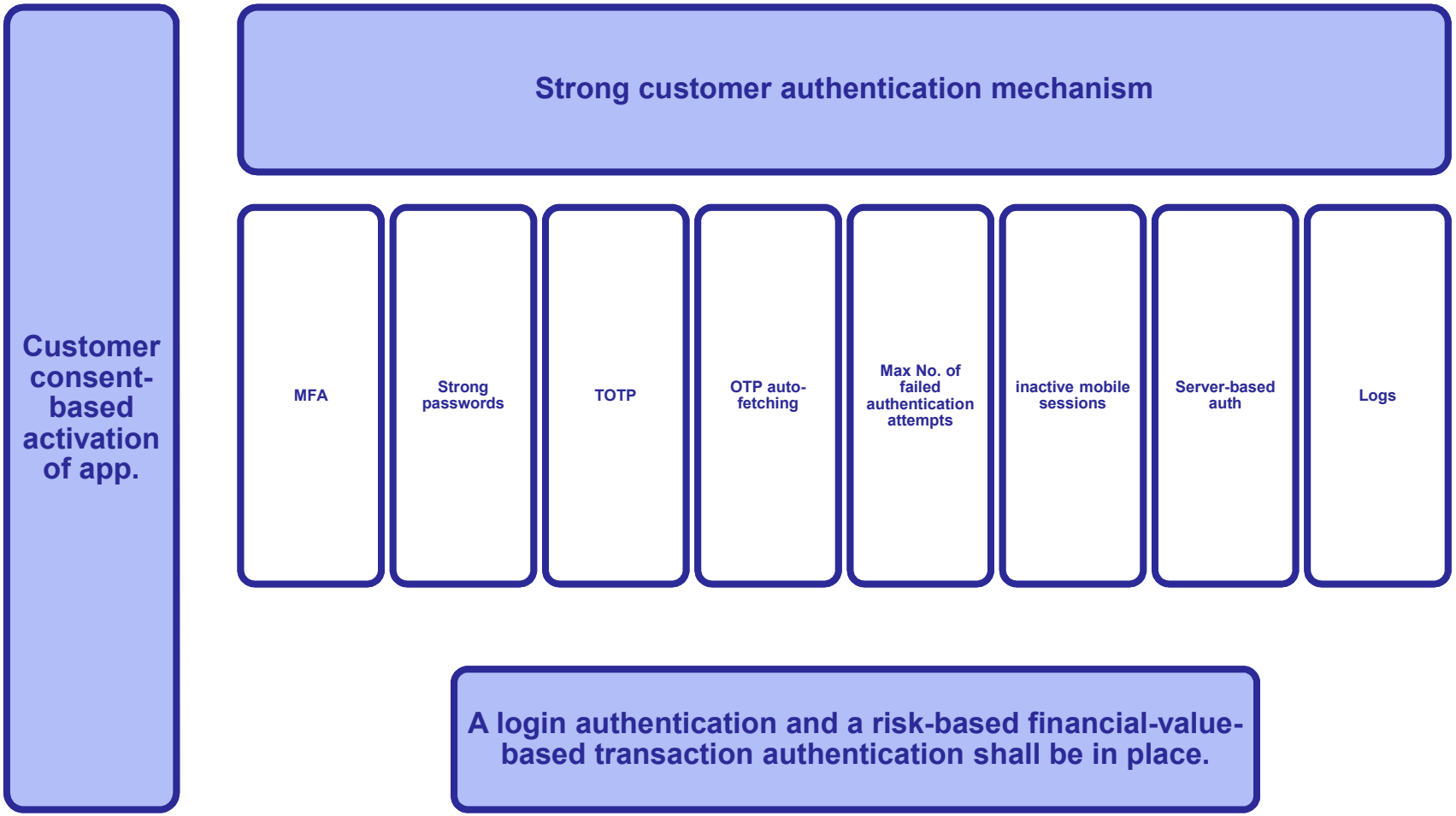
- vulnerability assessment
- penetration testing
- performance assessment
- System and User Acceptance Testing (UAT)
- Escrow arrangement

Mobile App Security Requirements

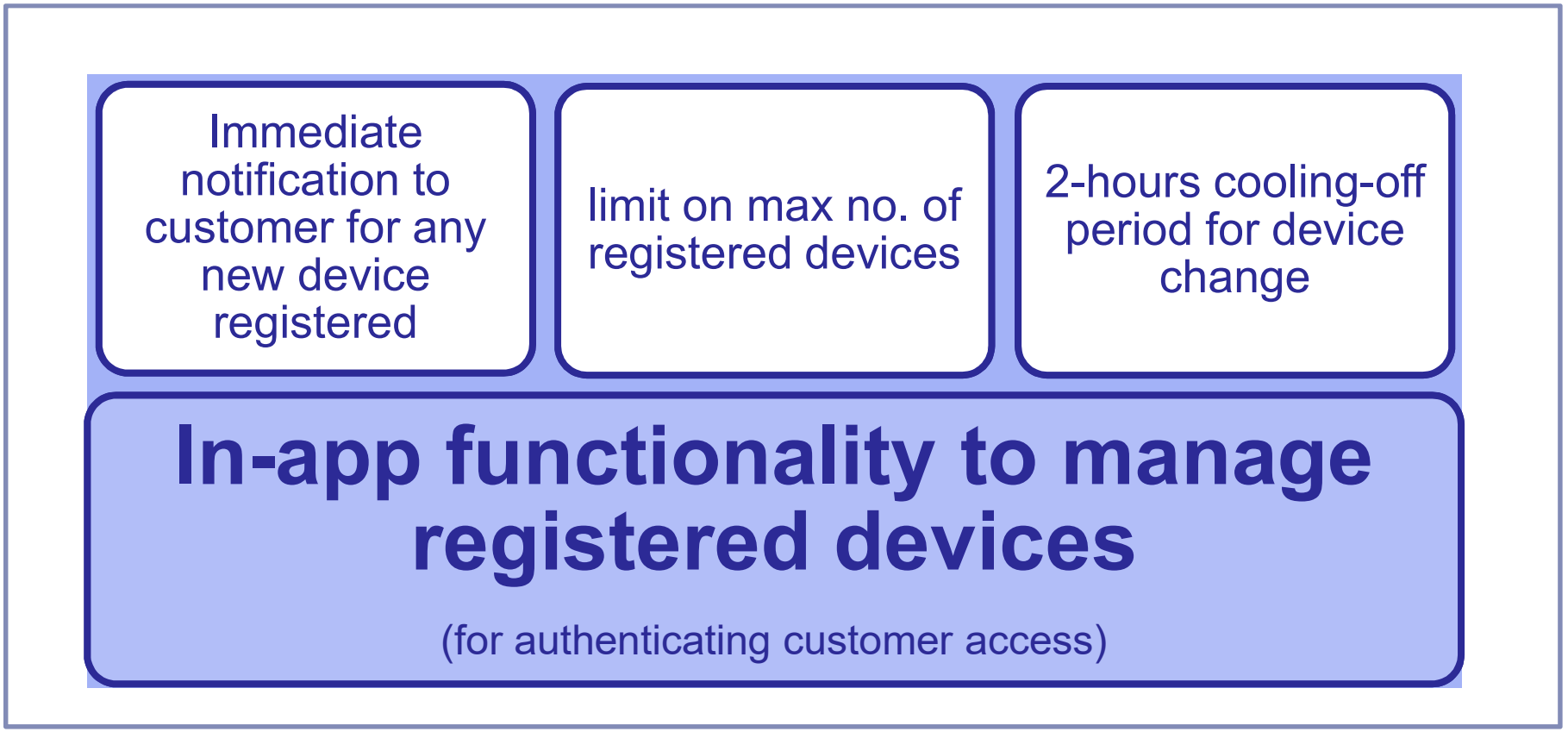
A. Mobile Application Architecture
B. Device Binding/Registration
C. User Authentication and Authorization
D. Protection of Sensitive Payment Data and Personal Data
E. Network and Interfacing Security
F. Session Management
G. Tampering Detection
H. App Permissions

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



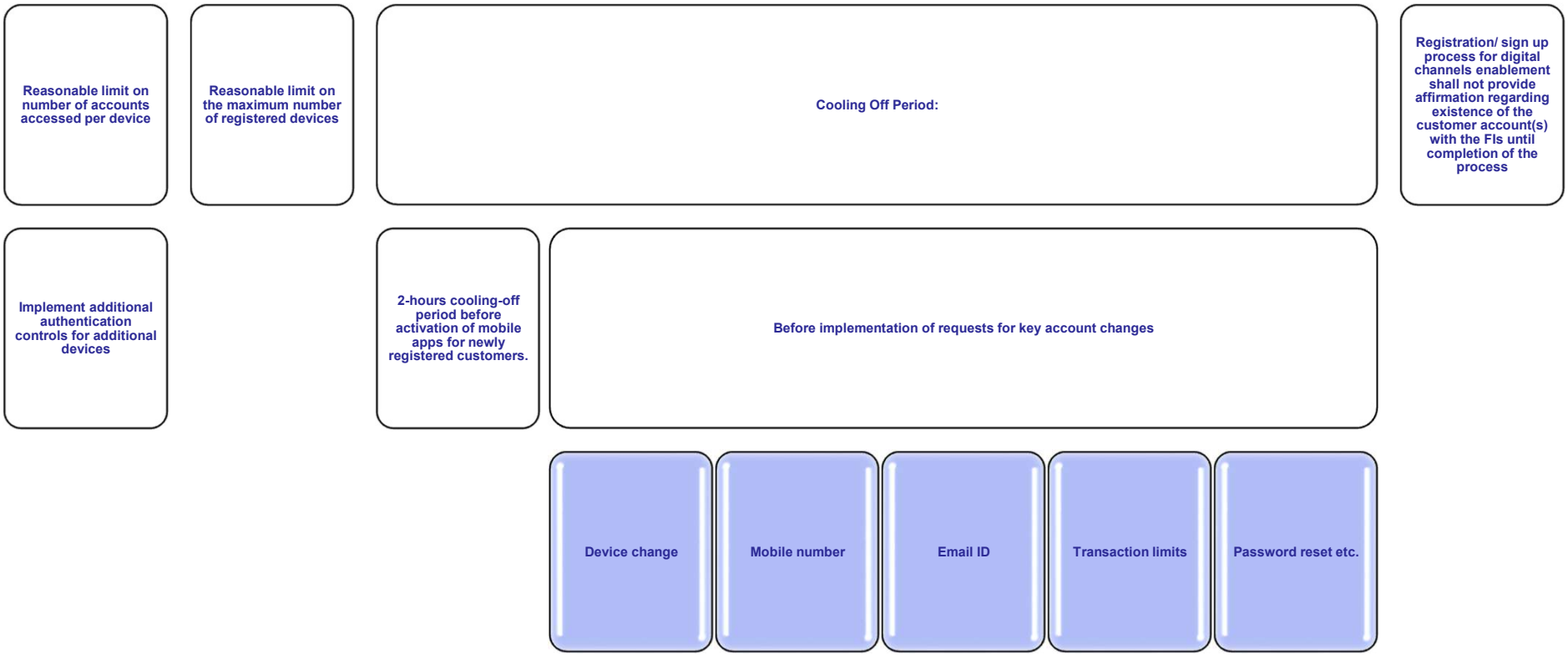
Device binding



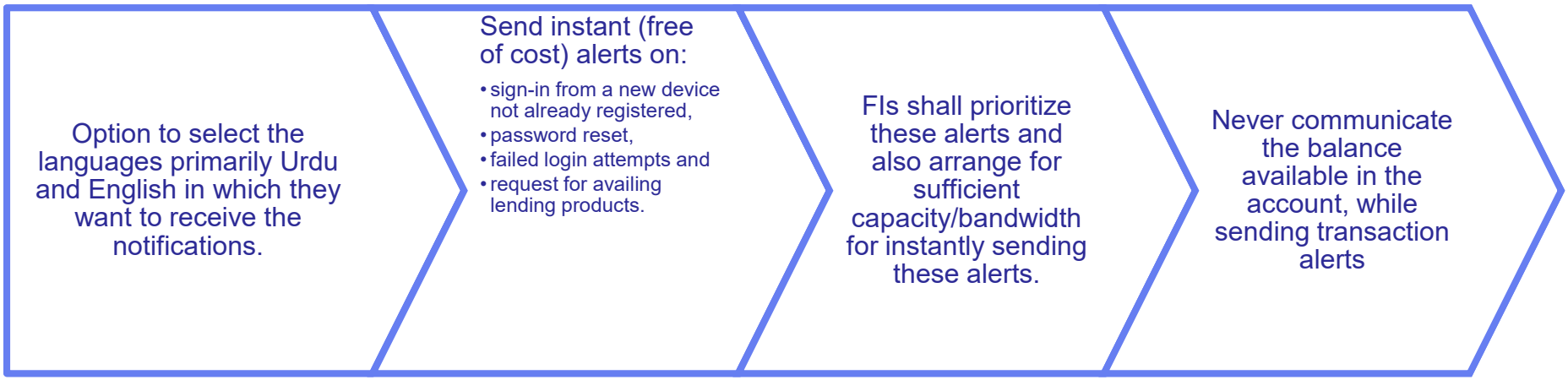
Credential reset (such as change in user ID/password of mobile banking/internet banking channel of customers)

- Only through customers' registered device
- One Time Password (OTP) auto-fetch
- Sender binding control restricting manual entry of OTP

Additional controls to safeguard users from mobile app frauds



User education and awareness



Our current work on preventing digital frauds at different stages of a transaction lifecyle

Pre-transaction

- Biometric authentication
- Device binding
- Transaction limits
- Cooling off period for key account changes

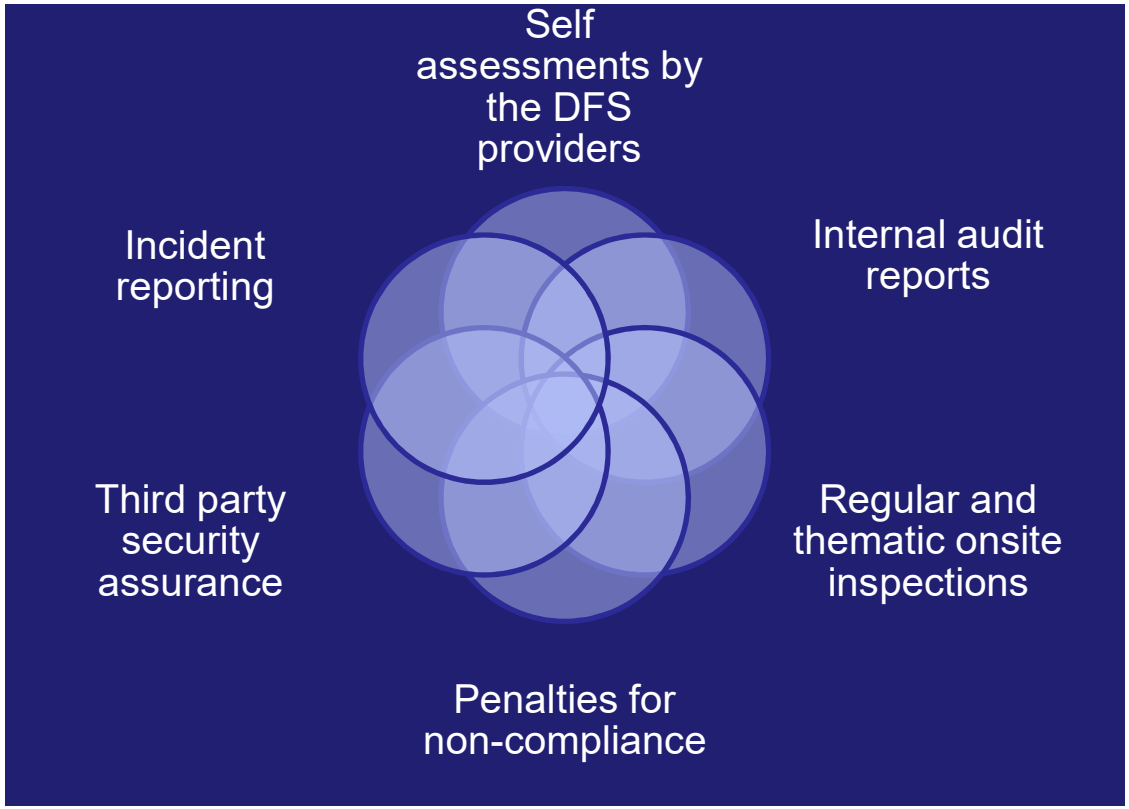
During transaction

- Rules-based fraud controls
- Negative customer list
- Development of a Machine learning based fraud prediction model

Post-transaction

- Fraudulent transactions dispute handling system
- Liability Framework
- Freeze on wallet withdrawals for 2-hours
- Sharing of information of fraudulent customers

How the regulators can ensure compliance?



Thanks!


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