DFS Security recommendations for regulators and providers

dfssecuritylab@itu.int

November 2024

DFS Security Recommendations

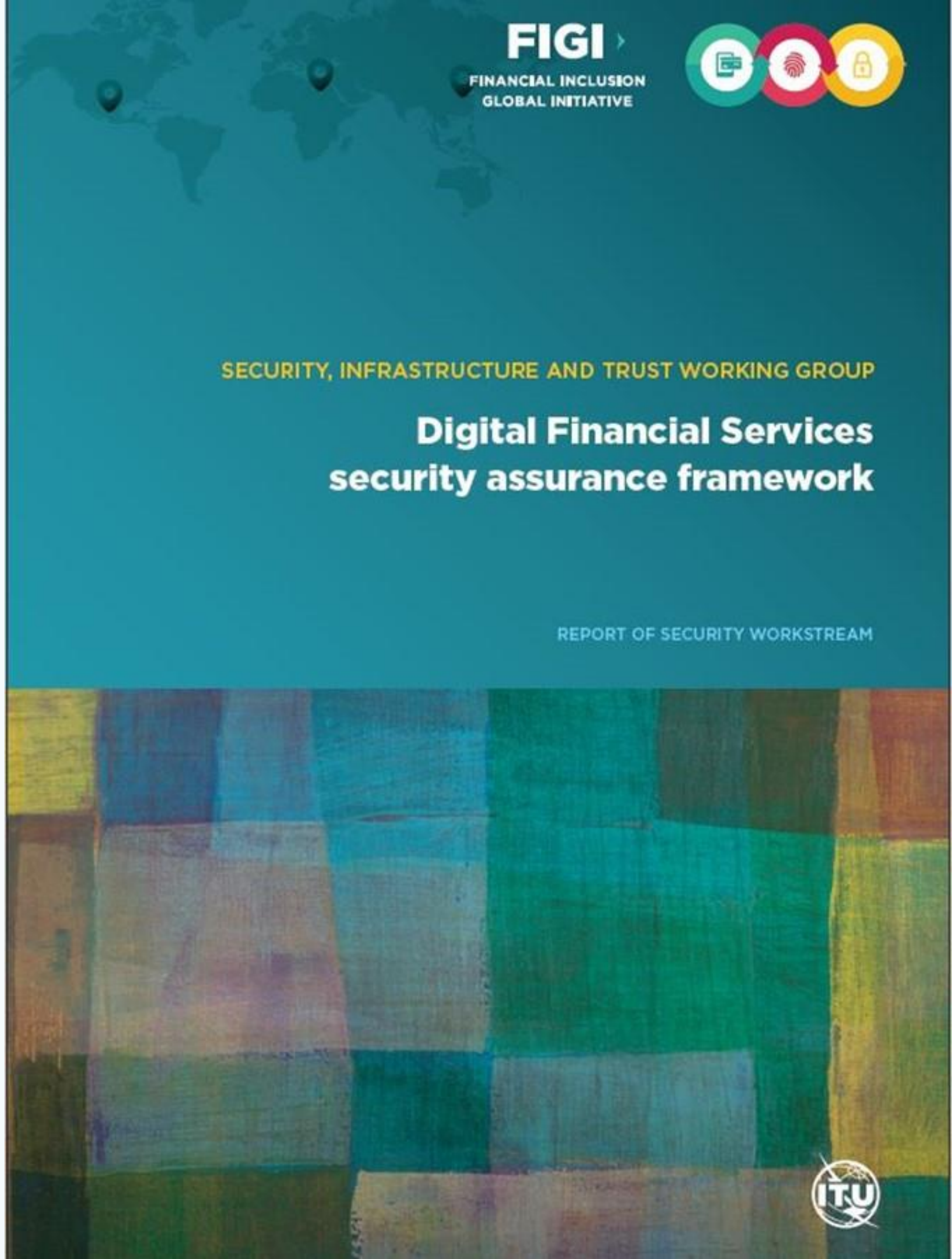
1. Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling
2. Recommendations to mitigate SS7 vulnerabilities
3. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
4. Mobile Application Security Best practices
5. DFS Consumer Competency Framework

DFS Security Assurance Framework

DFS ecosystem vulnerable to variety of threats:

- Interconnectedness of system entities
- Extended security boundaries due to reliance on numerous parties
- Mobile ecosystem itself is increasingly complex – devices, OSes

Difficult for stakeholders in DFS ecosystem to manage the interdependencies of the security threats within the DFS value chain and keep up with the new vulnerabilities and risks.



FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services
security assurance framework

REPORT OF SECURITY WORKSTREAM

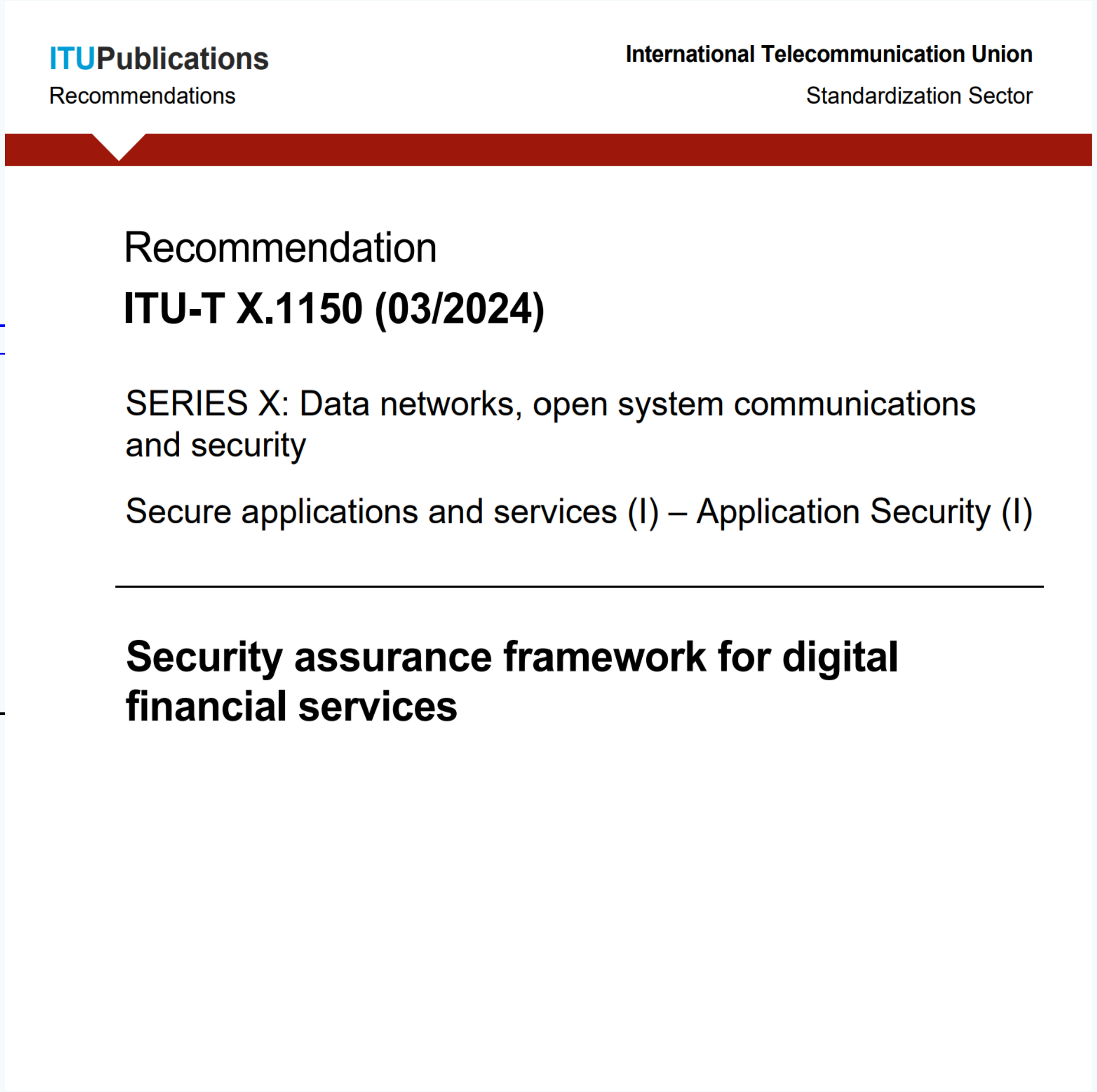
ITU

DFS Security Assurance Framework

Draws on principles from several standards: ISO/IEC 27000 security management systems standards, PCI/DSS v3.2, NIST 800-53, OWASP top-10 vulnerabilities, GSMA application security best practices. The DFS Security assurance framework is an ITU-T recommendation (ITU-T X.1150)

Contains the following components:

- **Security risk assessment** based on ISO/IEC 27005
- **Identifies common threats and vulnerabilities** to underlying infrastructure, DFS applications, services, network operators, third-party providers
- **Security control measures** and the x.805 security dimension they represent (119 controls identified)
- **Mobile application security best practices** for DFS applications.



ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation
ITU-T X.1150 (03/2024)

SERIES X: Data networks, open system communications and security

Secure applications and services (I) – Application Security (I)

Security assurance framework for digital financial services

How can the DFS security assurance and audit guidelines can be used?

- Identify security threats and vulnerabilities within the ecosystem
- Define security controls to mitigate the risks
- Strengthen security risk management.
- The ***audit guideline*** is for DFS regulators & providers to assess whether DFS controls in place

Introductory Concepts

ITU-T Rec. X.805

ITU-T Recommendation X.805 provides a foundation for the document, with eight *security dimensions* to address security:

1. *access control,*
2. *authentication,*
3. *non-repudiation,*
4. *data confidentiality,*
5. *communication security,*
6. *data integrity,*
7. *availability,*
8. *privacy*

Vulnerability

A weakness in a system that can be exploited by an adversary/hacker

Threat

the specific means by which a vulnerability is exploited

Risk

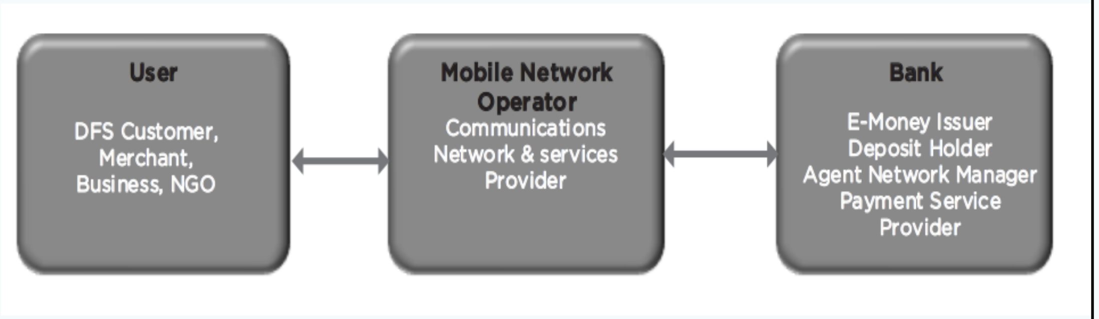
the consequences of a threat being successfully deployed

Control:

A *safeguard* or *countermeasure* prescribed to protect the **confidentiality**, **integrity**, and **availability** of information systems and assets to meet a set of defined security requirements.

DFS Business Models

Bank led



User

DFS Customer, Merchant, Business, NGO

Mobile Network Operator

Communications Network & services Provider

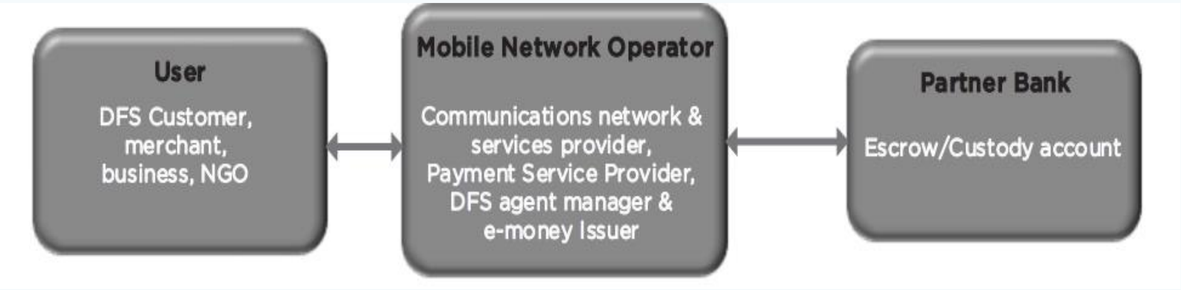
Bank

E-Money Issuer
Deposit Holder
Agent Network Manager
Payment Service Provider

bank performs key financial roles and leverages a mobile network operator for communication with users

MNO Led

MNO not only provides communication but also the bulk of financial roles, manages DFS agent network



User

DFS Customer, merchant, business, NGO

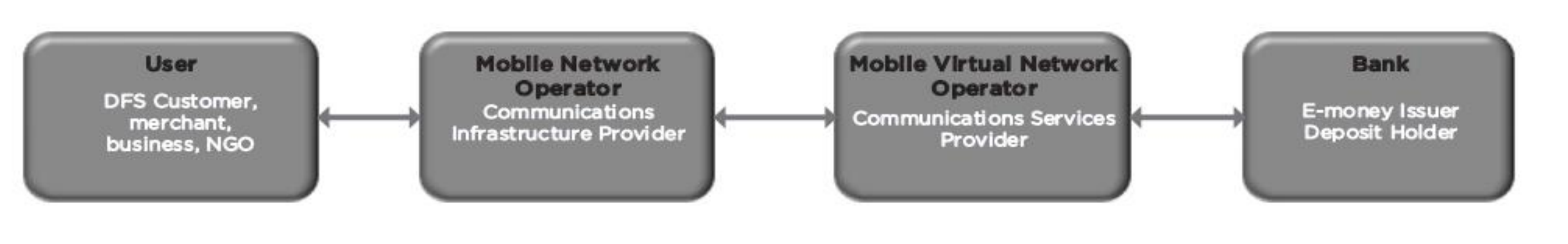
Mobile Network Operator

Communications network & services provider, Payment Service Provider, DFS agent manager & e-money Issuer

Partner Bank

Escrow/Custody account

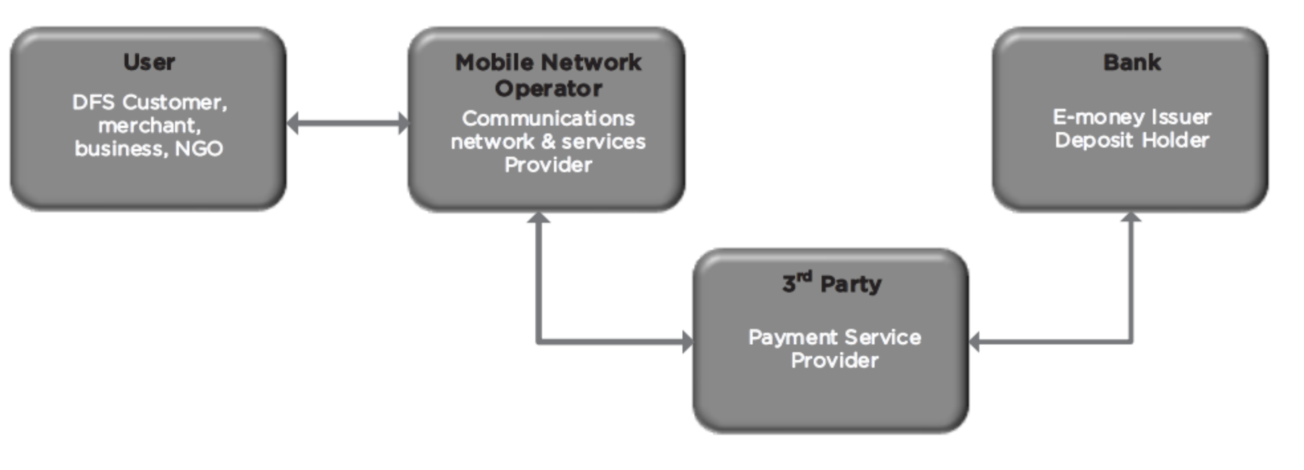
MVNO led


User
DFS Customer, merchant, business, NGO
Mobile Network Operator
Communications Infrastructure Provider
Mobile Virtual Network Operator
Communications Services Provider
Bank
E-money Issuer
Deposit Holder

MVNO provides telecommunication services using MNO infrastructure, DFS provided with a bank or independently

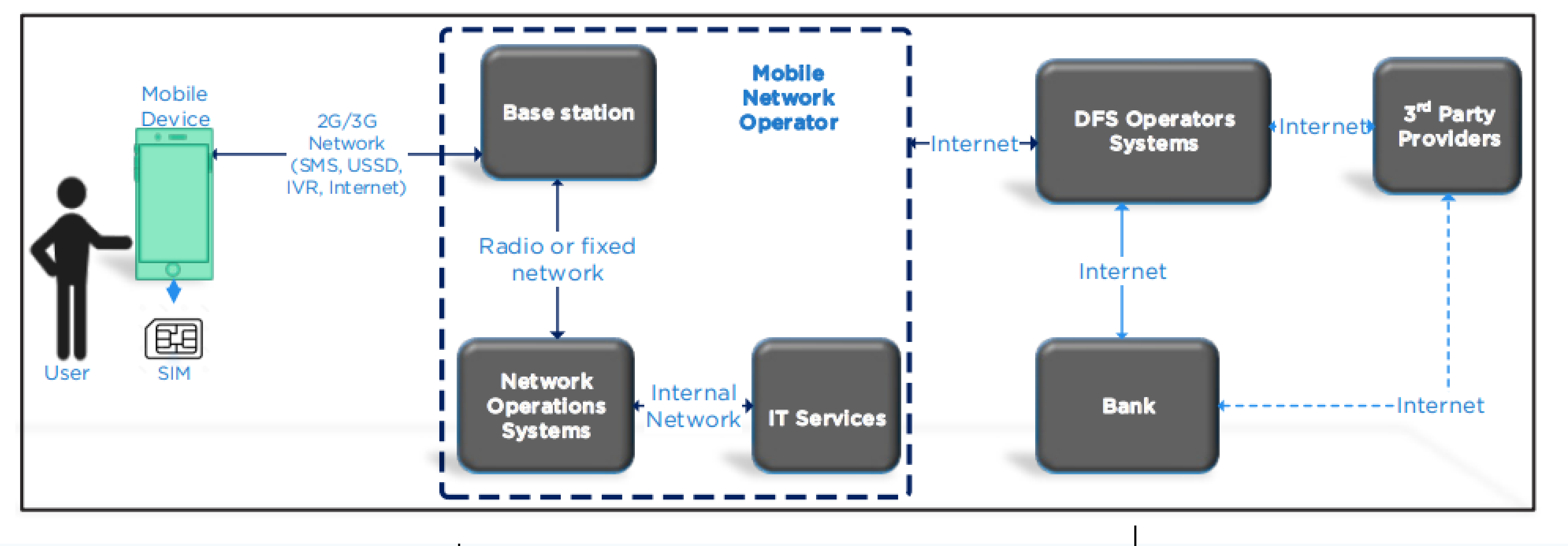
Hybrid

Critical roles are shared between bank and MNO, third parties provide additional services (e.g., PSP, agent network)



DFS ecosystem elements

Elements of a DFS Ecosystem



User

is target audience for DFS, uses mobile money application on a mobile device to access the DFS ecosystem

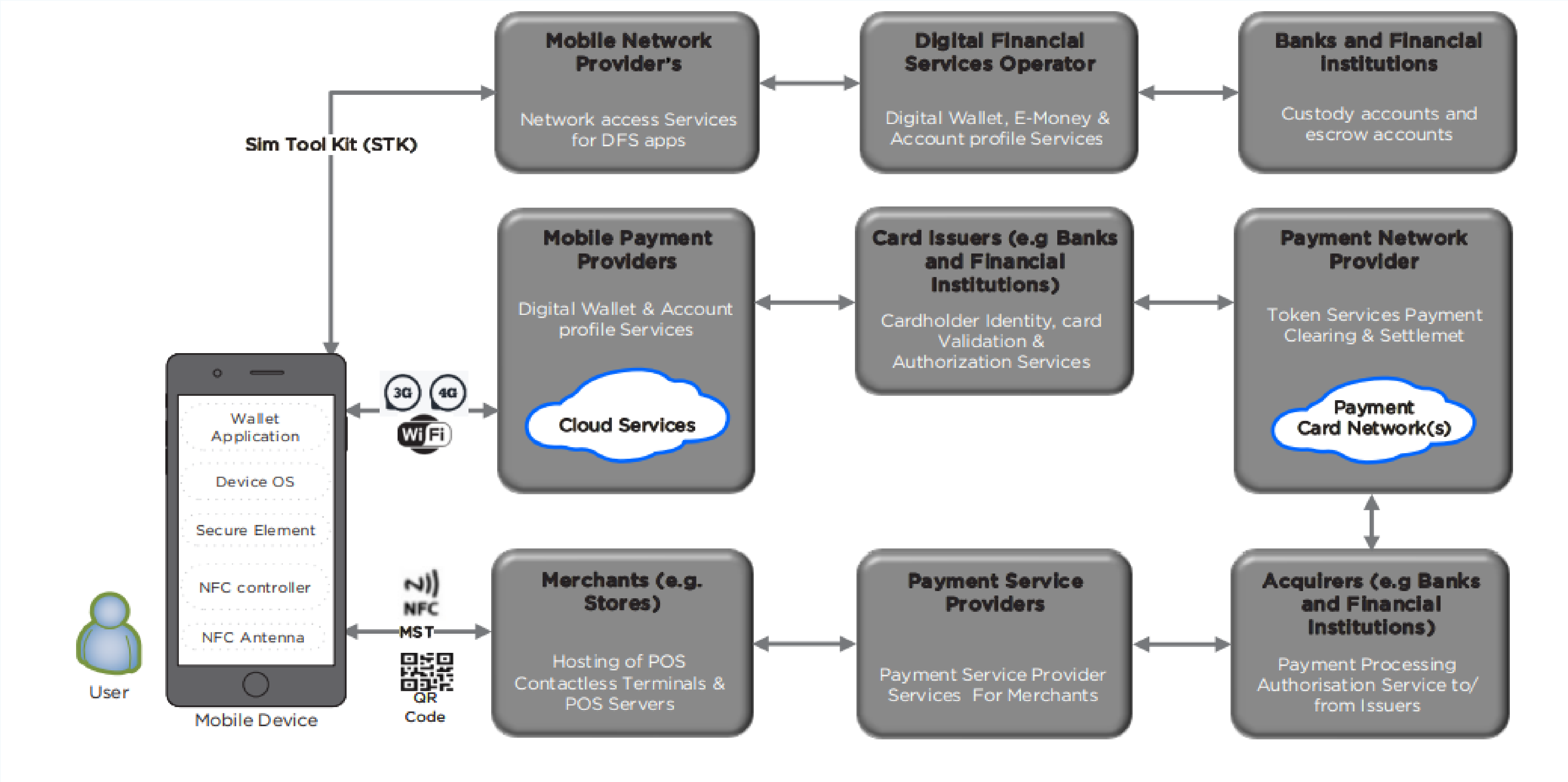
MNO

provides communication infrastructure from wireless link through the provider network

DFS Provider

handles application component, interfaces with payment systems and third-party providers.

Digital wallet DFS Ecosystem



Mobile Network Provider’s

Network access Services for DFS apps

Digital Financial Services Operator

Digital Wallet, E-Money & Account profile Services

Banks and Financial Institutions

Custody accounts and escrow accounts

Mobile Payment Providers

Digital Wallet & Account profile Services

Cloud Services

Card Issuers (e.g Banks and Financial Institutions)

Cardholder Identity, card Validation & Authorization Services

Payment Network Provider

Token Services Payment Clearing & Settlemet

Payment Card Network(s)

Merchants (e.g. Stores)

Hosting of POS Contactless Terminals & POS Servers

Payment Service Providers

Payment Service Provider Services For Merchants

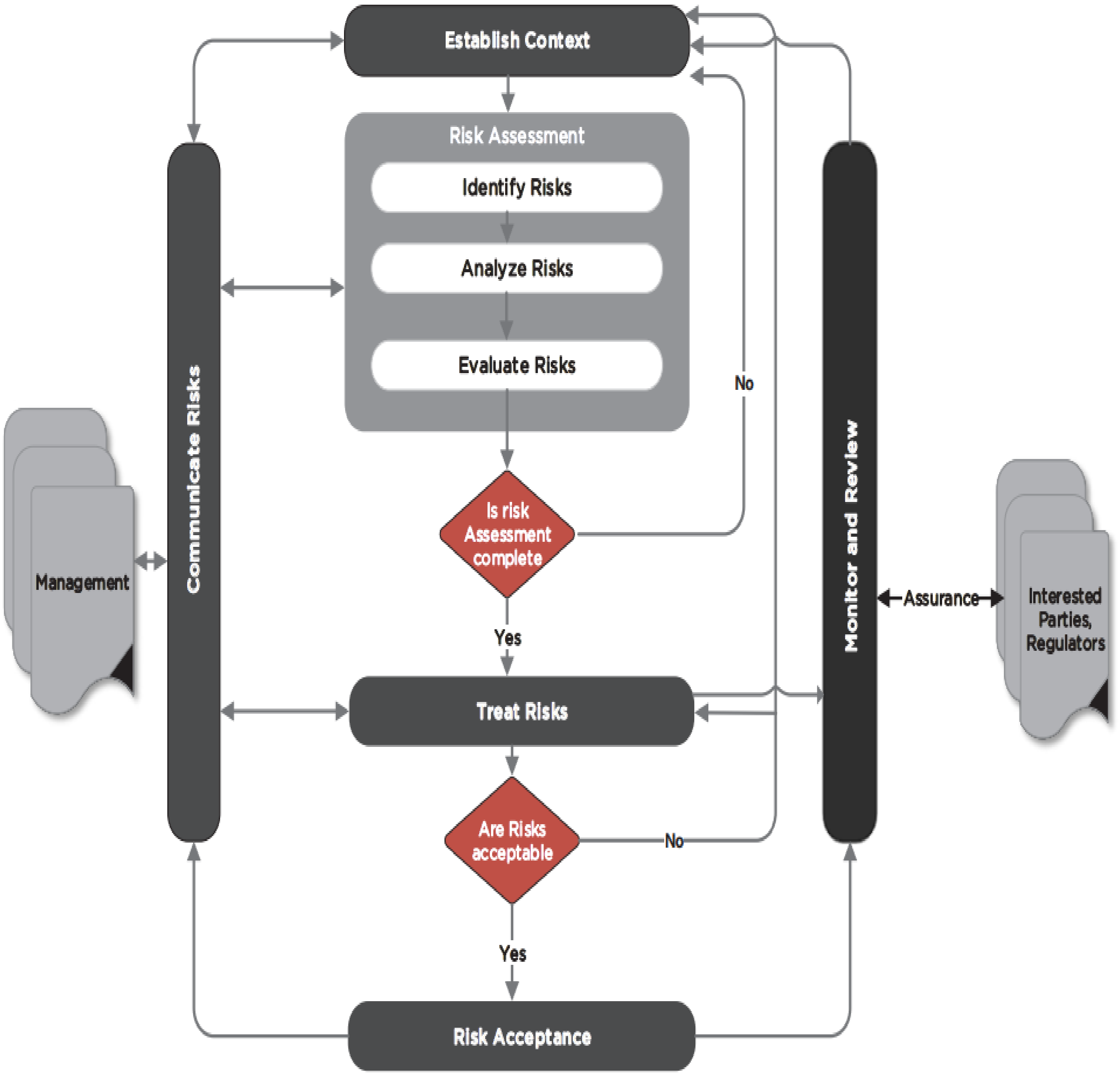
Acquirers (e.g Banks and Financial Institutions)

Payment Processing Authorisation Service to/ from Issuers

Security risk management process

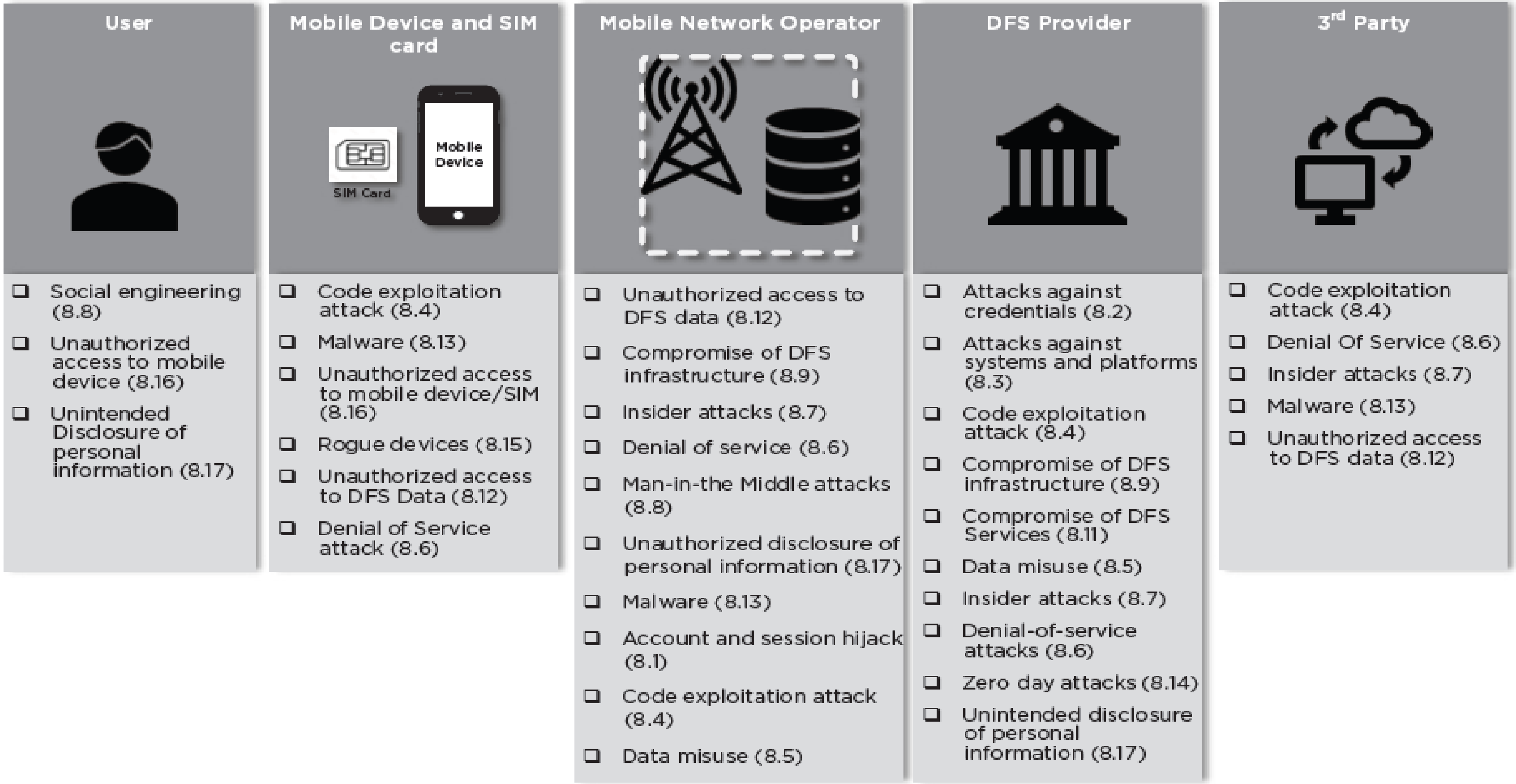
Risk Assessment methodology

- Based on Deming cycle of Plan, Do, Check, Act (PDCA) phases of the ISO 27001 – information security management
- Monitoring and review depend on the stakeholder (e.g., regulator reviewing controls, internal audits or new service)
- Context with inputs from Senior Management necessary for effective risk assessment/evaluation/analysis
- **Information Security Management System** based on ISO 27001 describing the risk treatment plans and security controls implemented for each threat and vulnerability is the main output of this phase



Threats, Vulnerabilities and Security Controls

DFS ecosystem threats



User

- □ Social engineering (8.8)
- □ Unauthorized access to mobile device (8.16)
- □ Unintended Disclosure of personal information (8.17)

Mobile Device and SIM card

- □ Code exploitation attack (8.4)
- □ Malware (8.13)
- □ Unauthorized access to mobile device/SIM (8.16)
- □ Rogue devices (8.15)
- □ Unauthorized access to DFS Data (8.12)
- □ Denial of Service attack (8.6)

Mobile Network Operator

- □ Unauthorized access to DFS data (8.12)
- □ Compromise of DFS infrastructure (8.9)
- □ Insider attacks (8.7)
- □ Denial of service (8.6)
- □ Man-in-the Middle attacks (8.8)
- □ Unauthorized disclosure of personal information (8.17)
- □ Malware (8.13)
- □ Account and session hijack (8.1)
- □ Code exploitation attack (8.4)
- □ Data misuse (8.5)

DFS Provider

- □ Attacks against credentials (8.2)
- □ Attacks against systems and platforms (8.3)
- □ Code exploitation attack (8.4)
- □ Compromise of DFS infrastructure (8.9)
- □ Compromise of DFS Services (8.11)
- □ Data misuse (8.5)
- □ Insider attacks (8.7)
- □ Denial-of-service attacks (8.6)
- □ Zero day attacks (8.14)
- □ Unintended disclosure of personal information (8.17)

3rd Party

- □ Code exploitation attack (8.4)
- □ Denial Of Service (8.6)
- □ Insider attacks (8.7)
- □ Malware (8.13)
- □ Unauthorized access to DFS data (8.12)

Example 1: Threat 8.1 Account and session hijacking

Source: DFS security assurance framework

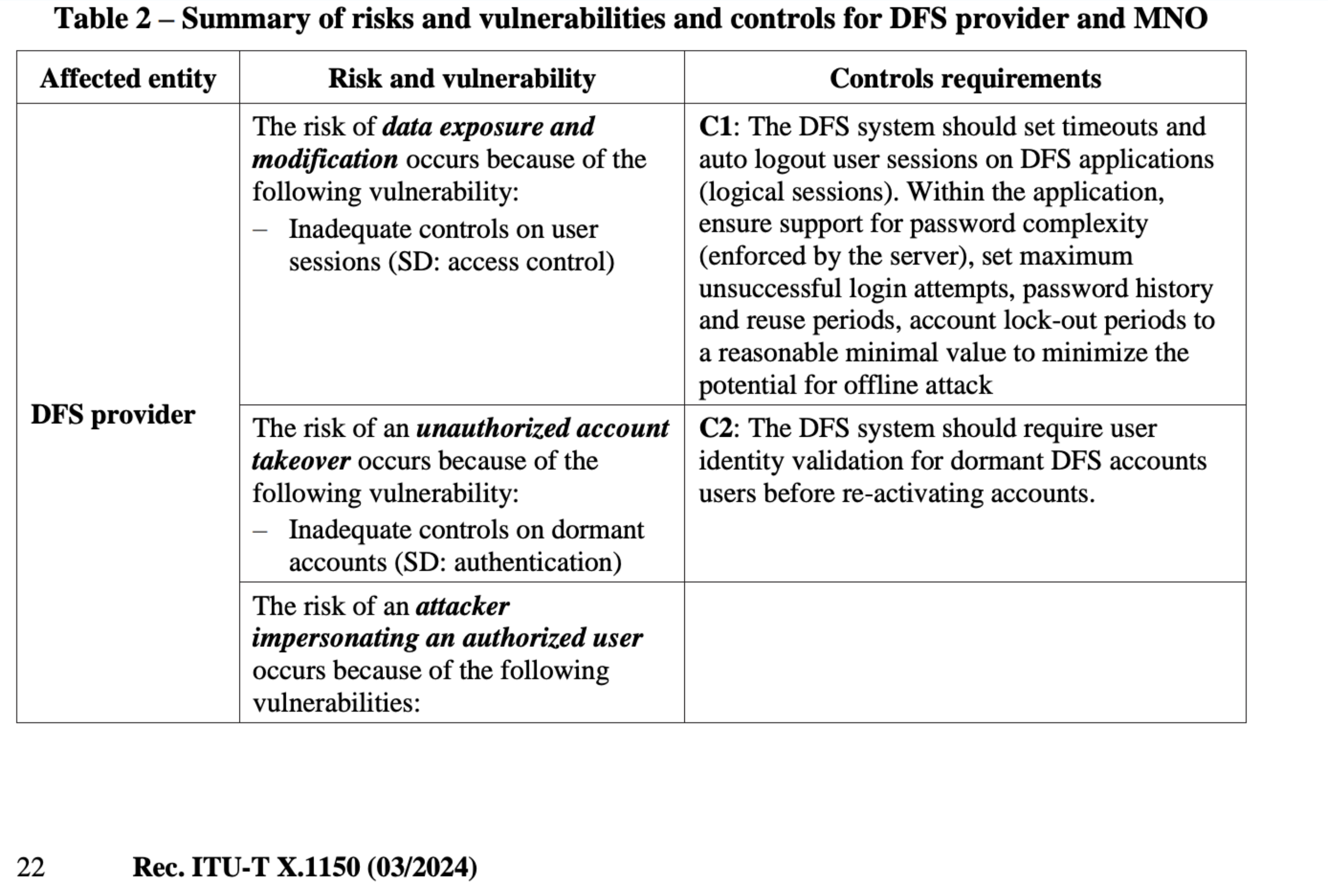


Table 2 – Summary of risks and vulnerabilities and controls for DFS provider and MNO

Affected entity	Risk and vulnerability	Controls requirements
DFS provider	The risk of ***data exposure and modification*** occurs because of the following vulnerability: – Inadequate controls on user sessions (SD: access control)	**C1**: The DFS system should set timeouts and auto logout user sessions on DFS applications (logical sessions). Within the application, ensure support for password complexity (enforced by the server), set maximum unsuccessful login attempts, password history and reuse periods, account lock-out periods to a reasonable minimal value to minimize the potential for offline attack
	The risk of an ***unauthorized account takeover*** occurs because of the following vulnerability: – Inadequate controls on dormant accounts (SD: authentication)	**C2**: The DFS system should require user identity validation for dormant DFS accounts users before re-activating accounts.
	The risk of an ***attacker impersonating an authorized user*** occurs because of the following vulnerabilities:	

Mobile Payment App Security framework

Mobile Payment App Security Best Practices (Section 9)

- Draws upon:
    - GSMA study on mobile money best practices,
    - ENISA smartphone security development guidelines,
- Template can be used as input to an app security policy by DFS providers to provide minimum security baselines for app developers and DFS providers as well as setting criteria for verifying compliance of apps
- Template considerations:

  i. device and application integrity.

  ii. communication security and certificate handling.

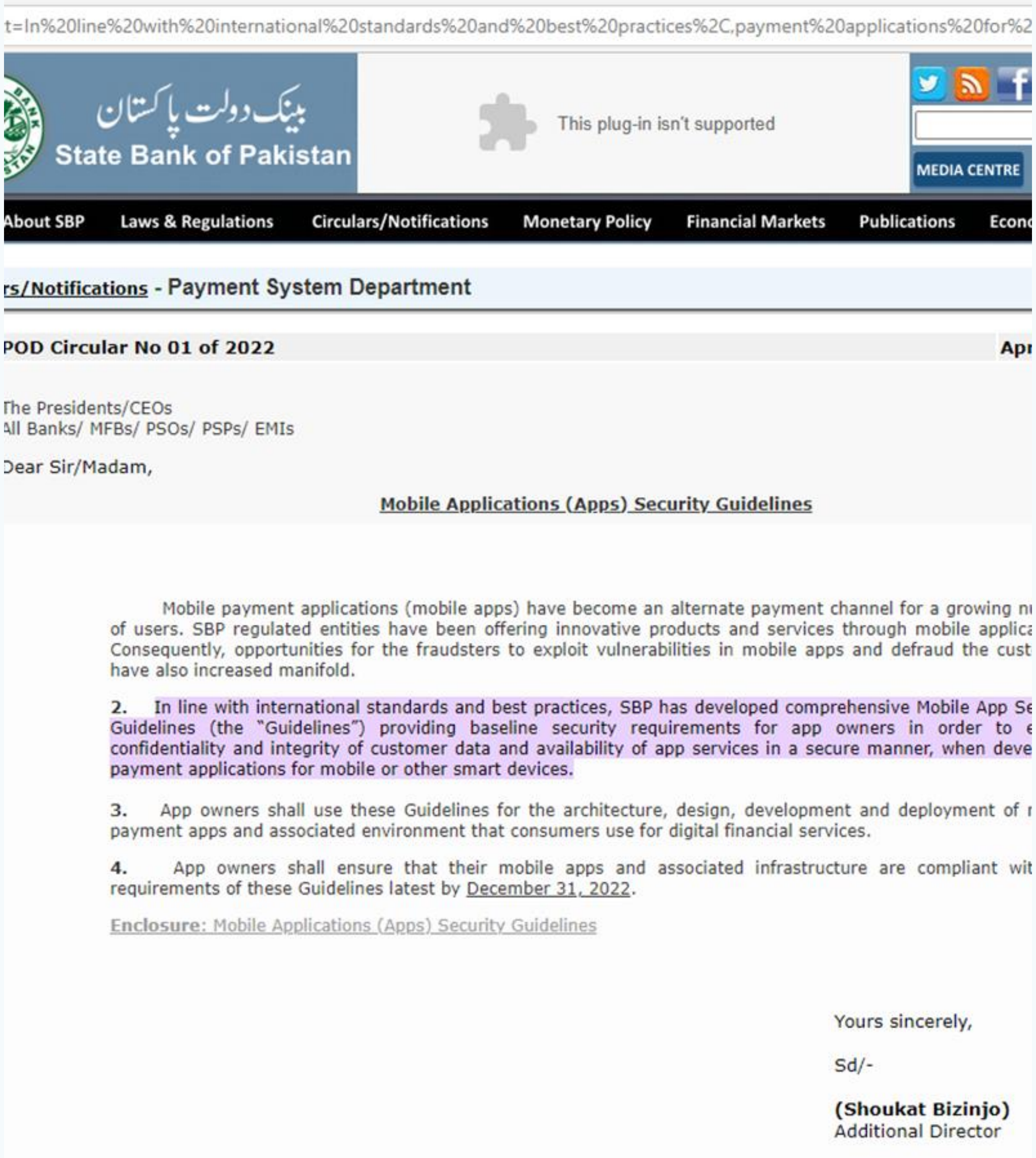
  iii. user authentication.

  iv. secure data handling.

  v. secure application development.

Application security best considerations:

- device and application integrity.
- communication security and certificate handling.
- user authentication.
- secure data handling.
- secure application development.



rs/Notifications - Payment System Department

POD Circular No 01 of 2022 Apr

The Presidents/CEOs
All Banks/ MFBs/ PSOs/ PSPs/ EMIs

Dear Sir/Madam,

Mobile Applications (Apps) Security Guidelines

Mobile payment applications (mobile apps) have become an alternate payment channel for a growing nu
of users. SBP regulated entities have been offering innovative products and services through mobile applica
Consequently, opportunities for the fraudsters to exploit vulnerabilities in mobile apps and defraud the cust
have also increased manifold.

2. In line with international standards and best practices, SBP has developed comprehensive Mobile App Se
Guidelines (the "Guidelines") providing baseline security requirements for app owners in order to e
confidentiality and integrity of customer data and availability of app services in a secure manner, when deve
payment applications for mobile or other smart devices.

3. App owners shall use these Guidelines for the architecture, design, development and deployment of r
payment apps and associated environment that consumers use for digital financial services.

4. App owners shall ensure that their mobile apps and associated infrastructure are compliant wit
requirements of these Guidelines latest by December 31, 2022.

Enclosure: Mobile Applications (Apps) Security Guidelines

Yours sincerely,

Sd/-

(Shoukat Bizinjo)
Additional Director

Mobile Application Security best practices

Device and Application Integrity

Use platform services for integrity checks;

remove extraneous code

maintain high-integrity state server-side.

Communication Security and Certificate Handling

Standardized cryptographic libraries; strong,

up-to-date TLS certificates; limit certificate lifetimes (825 days);

contingency for untrusted CA; secure TLS configuration;

certificate pinning; correct server certificate validation.

User Authentication

Disallow easily guessable credentials;

encourage multi-factor authentication;

prefer authenticator apps over SMS for OTPs;

secure storage of biometric information.

Secure Data Handling

Secure storage of confidential info;

trusted hardware for sensitive data;

avoid external storage;

clean caches/memory;

`fine-grained permissions for data sharing;

avoid hard-coding sensitive info;

validate client input for database storage.

Secure Application Development

Adhere to secure coding practices and standards;

provide secure application updates;

regular internal or external code reviews.

http://www.itu.int/go/dfssl

Contact: dfssecuritylab@itu.int

Thank you!