Managing Risks in Digital Finance - *DFS Security Assurance Framework*

Vijay Mauree, Programme Cordinator, ITU

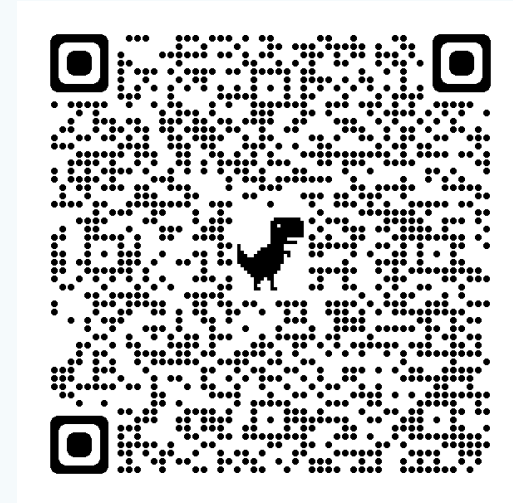Vijay.mauree@itu.int

25 April 2024

Outline

1. DFS Security Assurance Framework

2. DFS business models

3. DFS Ecosystem elements

4. Security risk management process

5. Threats, vulnerabilities & security controls

6. Mobile Payment App Security Best Practices
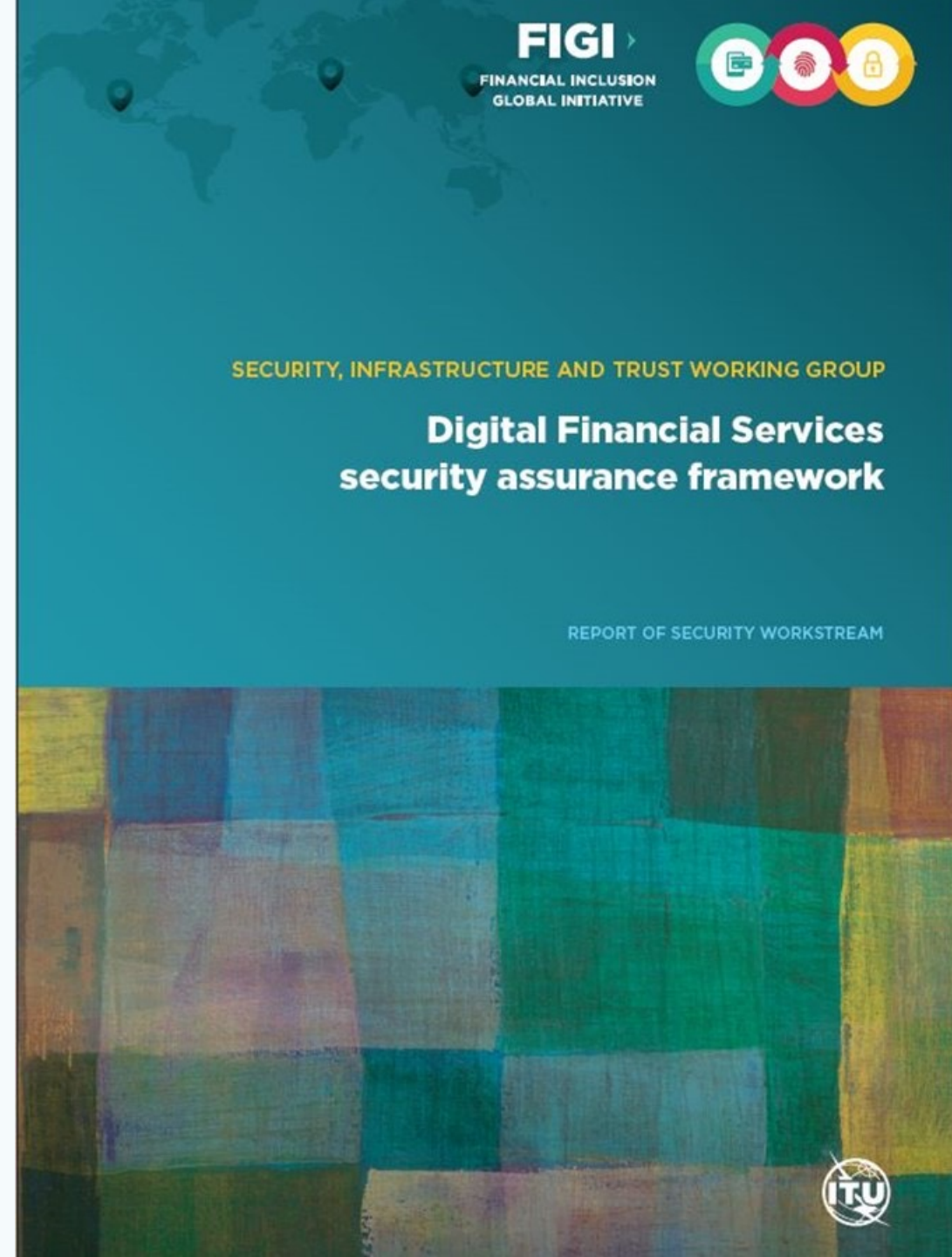
7. Summary

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

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 (117 controls identified)

- **Mobile application security best practices** for DFS applications

- The Security assurance framework for digital financial services is an ITU-T SG 17 TAP approved recommendation

FIGI ›
FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

**Digital Financial Services
security assurance framework**

REPORT OF SECURITY WORKSTREAM

ITU

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	Mobile Network Operator	Bank
DFS Customer, Merchant, Business, NGO	Communications Network & services Provider	E-Money Issuer Deposit Holder Agent Network Manager Payment Service Provider
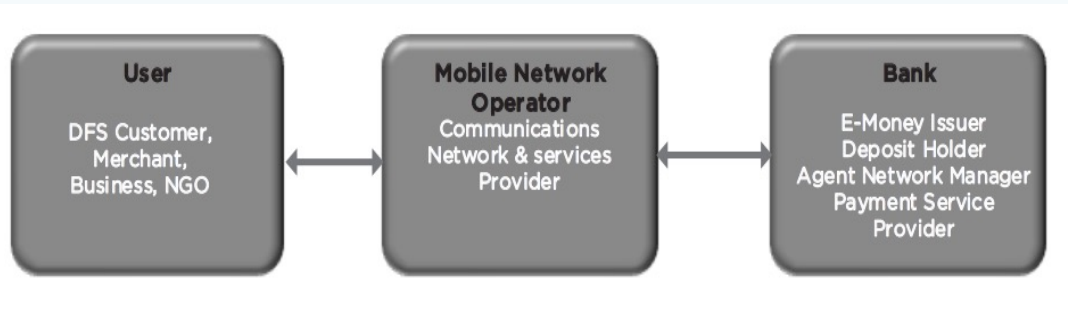
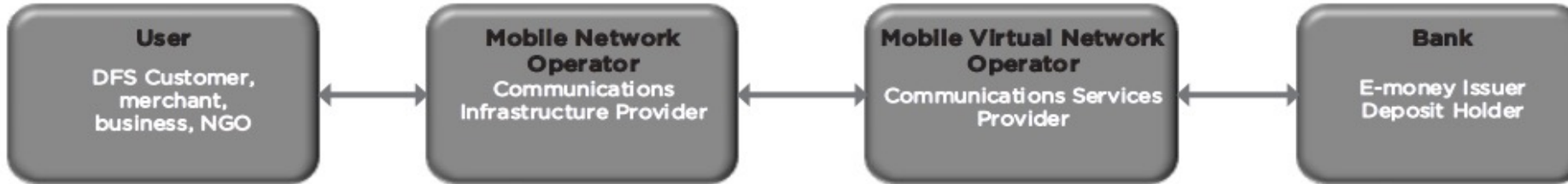bank performs key financial roles and leverages a mobile network operator for communication with users

MNO Led

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

User	Mobile Network Operator	Partner Bank
DFS Customer, merchant, business, NGO	Communications network & services provider, Payment Service Provider, DFS agent manager & e-money Issuer	Escrow/Custody account

MVNO led

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

Hybrid

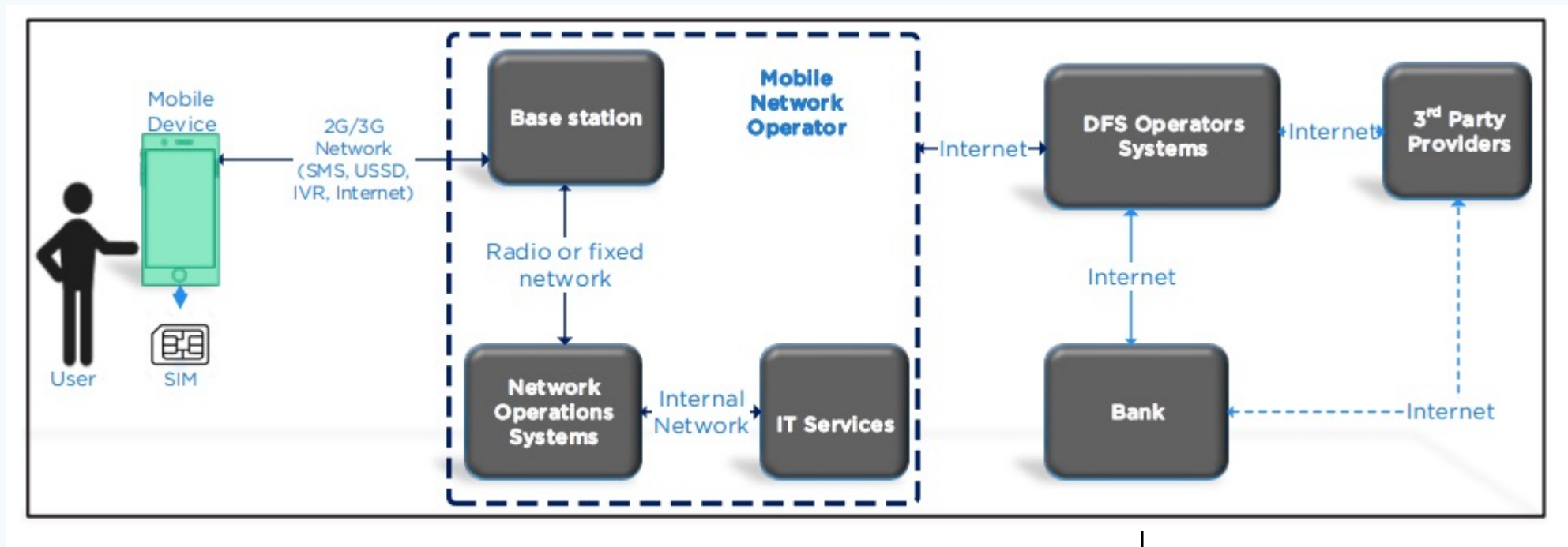Critical roles are shared between bank and MNO, third parties provide additional services (e.g., PSP, agent network)
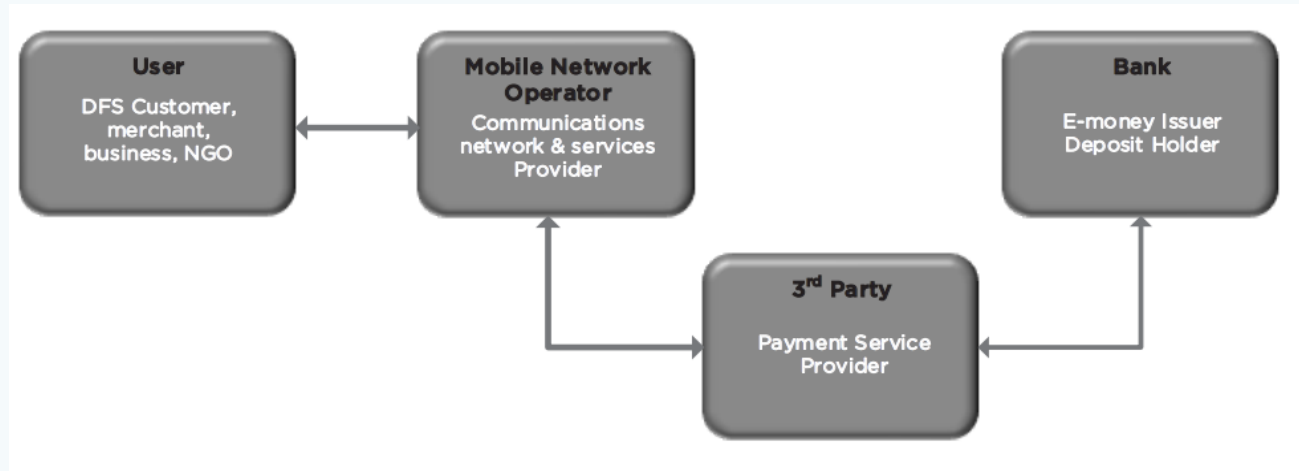
DFS ecosystem elements

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

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
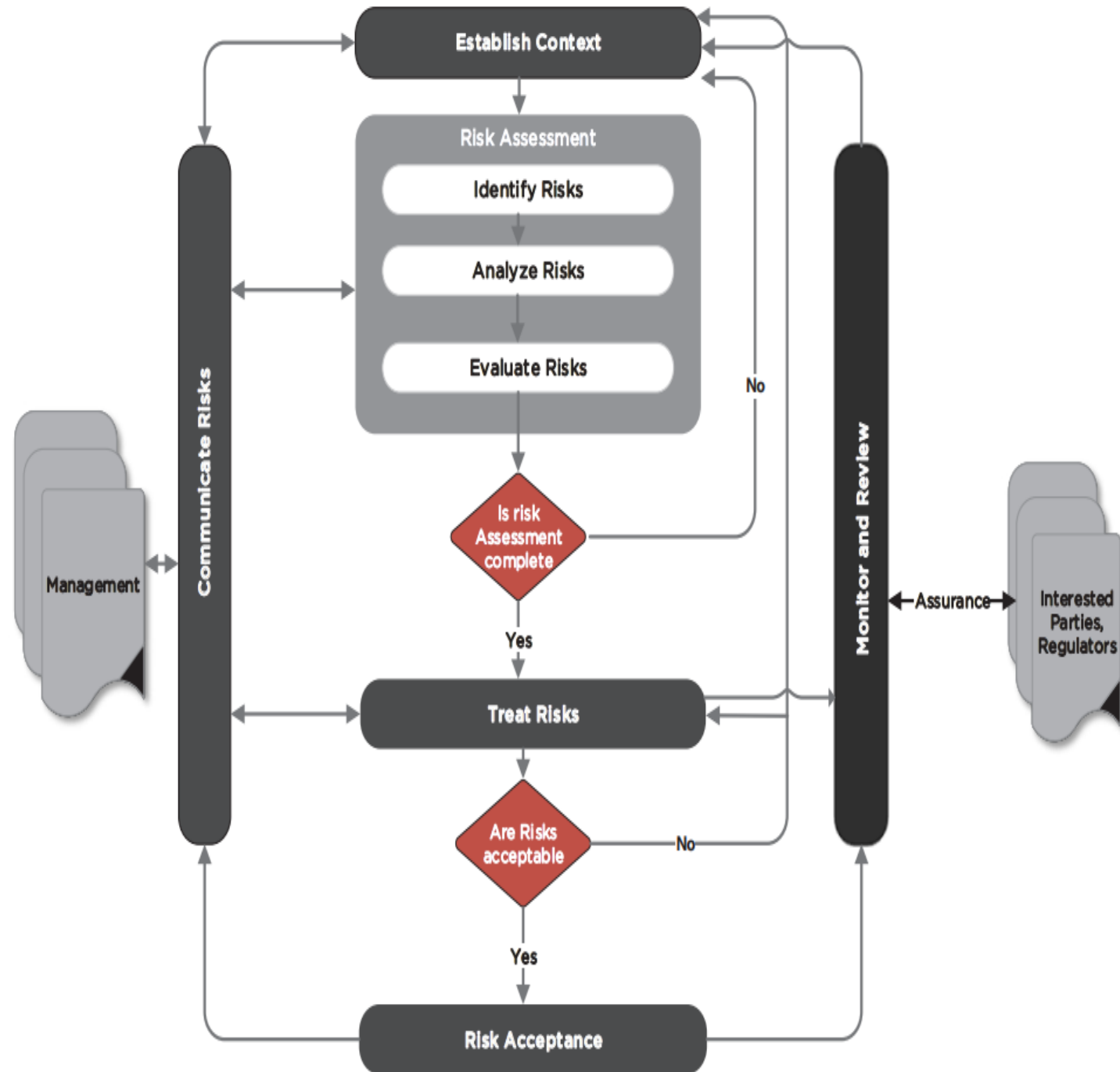
Threats, Vulnerabilities and Security Controls

DFS ecosystem threats

User	Mobile Device and SIM card	Mobile Network Operator	DFS Provider	3rd Party
❑ Social engineering (8.8)	❑ Code exploitation attack (8.4)	❑ Unauthorized access to DFS data (8.12)	❑ Attacks against credentials (8.2)	❑ Code exploitation attack (8.4)
❑ Unauthorized access to mobile device (8.16)	❑ Malware (8.13)	❑ Compromise of DFS infrastructure (8.9)	❑ Attacks against systems and platforms (8.3)	❑ Denial Of Service (8.6)
❑ Unintended Disclosure of personal information (8.17)	❑ Unauthorized access to mobile device/SIM (8.16)	❑ Insider attacks (8.7)	❑ Code exploitation attack (8.4)	❑ Insider attacks (8.7)
	❑ Rogue devices (8.15)	❑ Denial of service (8.6)	❑ Compromise of DFS infrastructure (8.9)	❑ Malware (8.13)
	❑ Unauthorized access to DFS Data (8.12)	❑ Man-in-the Middle attacks (8.8)	❑ Compromise of DFS Services (8.11)	❑ Unauthorized access to DFS data (8.12)
	❑ Denial of Service attack (8.6)	❑ Unauthorized disclosure of personal information (8.17)	❑ Data misuse (8.5)	
		❑ Malware (8.13)	❑ Insider attacks (8.7)	
		❑ Account and session hijack (8.1)	❑ Denial-of-service attacks (8.6)	
		❑ Code exploitation attack (8.4)	❑ Zero day attacks (8.14)	
		❑ Data misuse (8.5)	❑ Unintended disclosure of personal information (8.17)	

Example 1: Threat 8.1 Account and session hijacking

Affected Entity	Risk and Vulnerability	Controls
DFS Provider	The risk of **data exposure and modification** occurs because of the following vulnerability: - Inadequate controls on user sessions (SD: access control)	**C1:** Set timeouts and auto logouts 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 reasonably 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:** 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:	
	- Failure to perform geographical location validation (SD: Communication security)	**C3:** Limit access to DFS services based on user locations (for example disable access to DFS USSD codes while roaming, STK and SMS for merchants and agents) where possible restrict access by region for DFS agents, where possible check that agent and number performing a deposit or withdrawals are within the same serving area.
	- Inadequate user verification of preferred user communication channels for DFS services (SD: Communication security)	**C4:** Restrict DFS services by communication channels (during registration customers should optionally choose service access channel, USSD only, STK only, app only, or a combination) attempted DFS access through channels other than opted should be blocked and red-flagged.
	The risk of **unauthorised access to user data and credentials** occurs due to the following vulnerabilities:	
	- Replay session based on tokens intercepted (SD: communication security)	**C5:** The DFS system should not trust any client-side authentication or authorization tokens; validation of access tokens must be performed at the server-side.
	- Weak encryption algorithms for password storage (SD: data confidentiality)	**C6:** Store DFS passwords using strong salted cryptographic hashing algorithms.

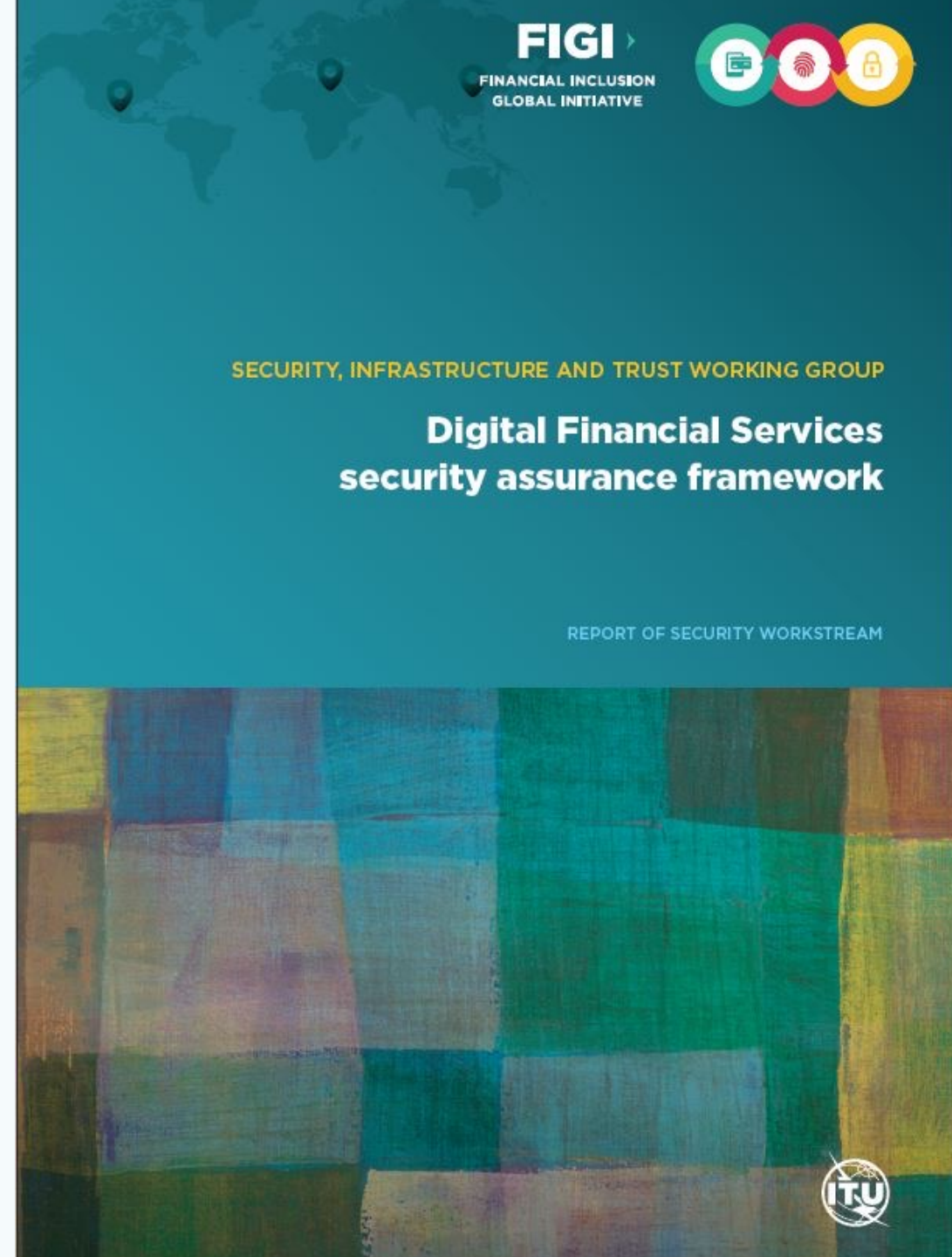Source: DFS security assurance framework

Mobile Payment App Security Best Practices (Section 9)

- Draws upon:
    - GSMA study on mobile money best practices,
    - ENISA smartphone security development guidelines,
    - State Bank of Pakistan mobile payment applications security framework
- 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.
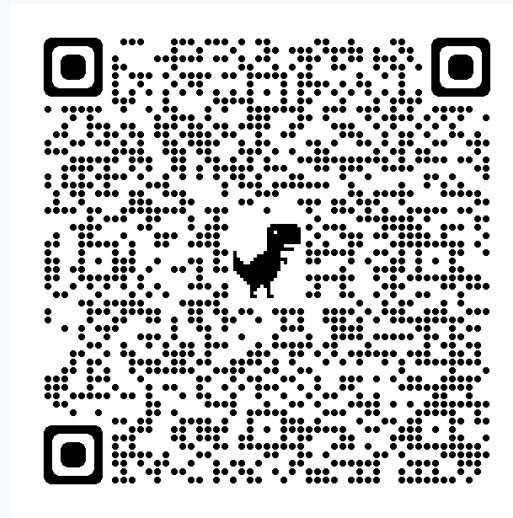   iv. secure data handling.
    v. secure application development.

Summary

- Identify the threats and vulnerabilities for different DFS stakeholder types.

- Adopt a risk management process

- Implement Information Security Management System (ISMS) based on ISO 27001

- Establish minimum security baselines for app security development → address systemic vulnerabilities

- Conduct periodic security audit of DFS providers and/or security audit of DFS applications

Aimed at DFS regulators and providers

FIGI ›
FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

**Digital Financial Services
security assurance framework**

REPORT OF SECURITY WORKSTREAM

Thank you!

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

Contact: dfssecuritylab@itu.int