

Risk mitigation Framework

Dr. Bilel Jamoussi

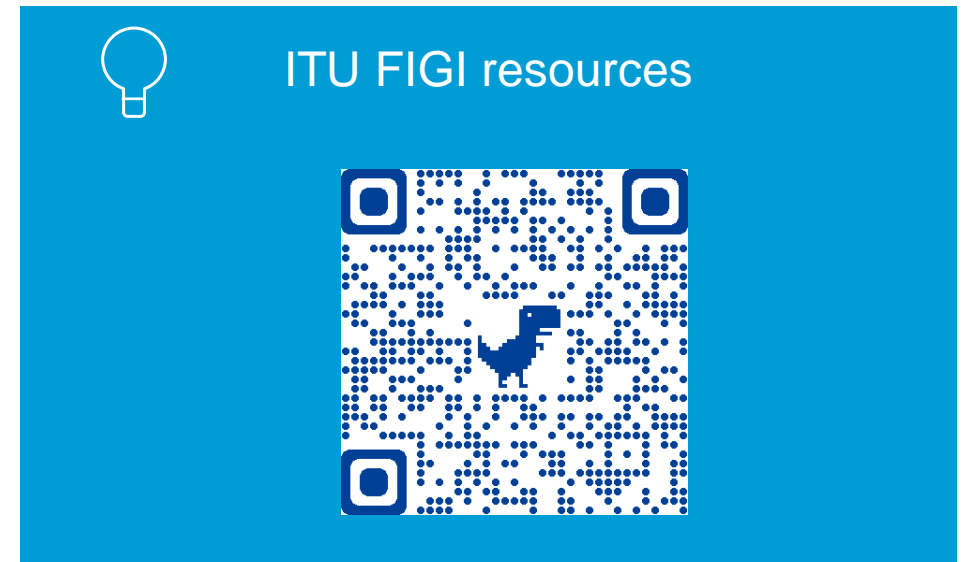
Chief of Study Groups Department, TSB, ITU

22 October 2021



Outline

1. Intro: DFS security at ITU
2. The DFS ecosystem security challenges
3. Security risk management in DFS






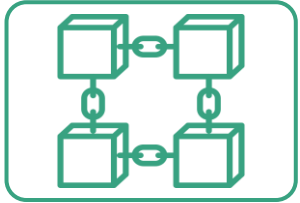
DFS security at ITU

FIGI Security Infrastructure & Trust Working Group



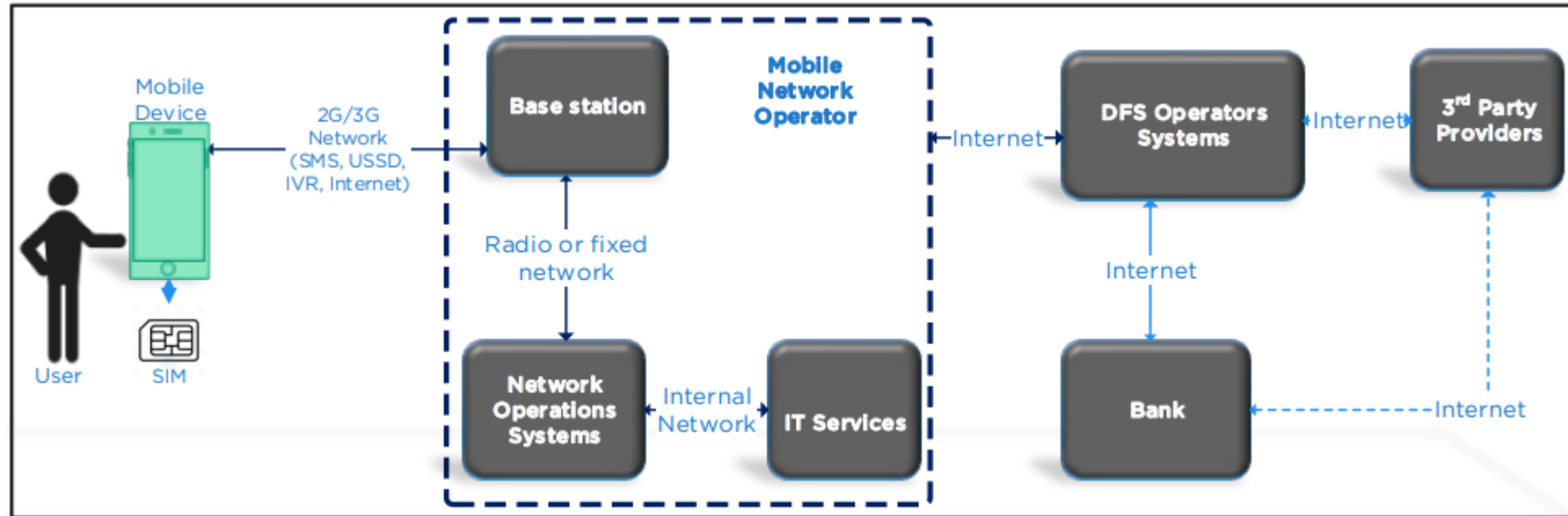
Security, Infrastructure & Trust Working Group workstreams

Working Group Reports

- **Security Workstream**
Address DFS application security, telecom infrastructure security issues, consumer authentication and cybersecurity risk management.
- **Trust Workstream**
Address unlicensed digital investment schemes, digital skills for users, and innovations and risks that AI and big data pose when used in financial inclusion.
- **Quality of Service Workstream**
Developed methodologies for measurement of key performance indicators (KPIs) for Quality of Service and Quality of Experience for DFS
- **Distributed Ledger Technologies Workstream**
Use of distributed ledger technology to secure digital financial services transactions.

The DFS ecosystem security challenges

Security risks in the DFS ecosystem



User

target user 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

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

DFS ecosystem security challenges

DFS ecosystem vulnerable to a variety of threats due to:

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

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.

117 Security controls identified in the DFS Security Assurance Framework report.

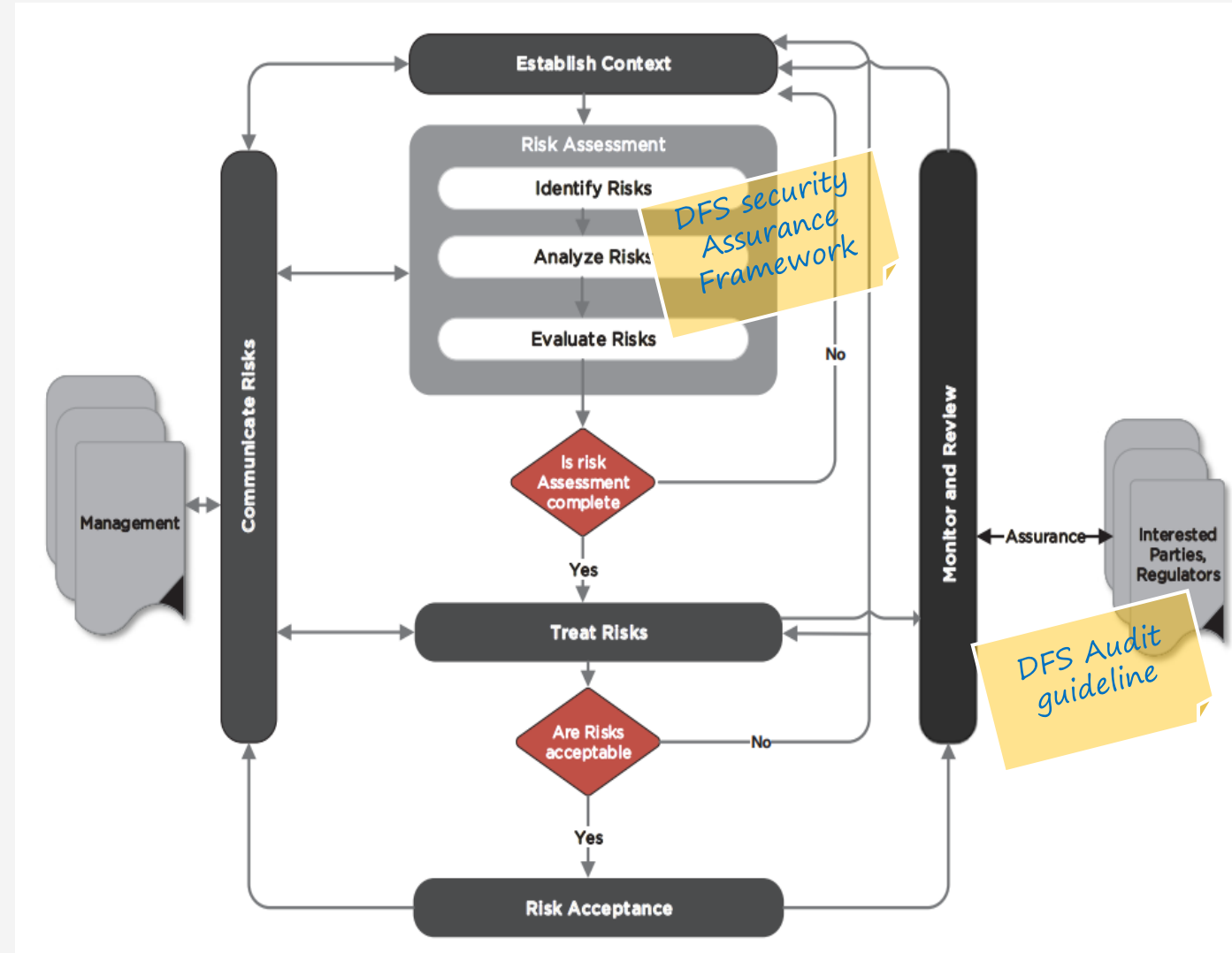


Digital Financial Services security assurance framework

Process for Security Risk Management

Security Risk Management

- 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



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
- Assessment of threats and vulnerabilities to underlying infrastructure, DFS applications, services, network operators, third-party providers
- Identification of vulnerabilities enabling the threats
- Security control measures and the ITU-T Rec X.805 security dimension they represent (117 controls identified)
- Mobile Payment App Security Best Practices



Digital Financial Services security assurance framework



Roadmap for DFS Security

- The Security Assurance Framework recommends a structured methodology for security risk management
- Clarify roles and responsibilities for each stakeholder in the ecosystem
- Will evolve over time

How can the DFS security Assurance and Audit Guidelines be used?

- Identify security threats and vulnerabilities within the ecosystem
- Define security controls to provide end-to-end security and mitigate the risks
- Strengthen management practices with respect to security risk management.
- The **audit guideline** is for DFS regulators to assess whether DFS controls in place and can also be used by DFS providers for internal audit purposes.

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security audit guideline

REPORT OF SECURITY WORKSTREAM



ITU DFS Security Lab

For a common approach for regulators, developers and DFS providers to test DFS mobile apps in a complex mobile ecosystem in order to provide/verify the level of assurance on security against systemic vulnerabilities.

Lab objectives



Collaboration with DFS regulators on DFS security.



Perform DFS **security audits** of DFS Apps



Organise **security clinics**



Assist DFS regulators to evaluate the **cyber preparedness** for DFS ecosystem



Knowledge sharing on threats to security of DFS apps with regulators



Encourage adoption of **international standards on DFS security**

Resources



Security testing for **USSD** and **STK based DFS**



Security audit of **Android** DFS apps using **OWASP** Mobile Top 10 Risks.



Developer resources for strong authentication using **FIDO**

Get in touch



dfssecuritylab@itu.int



<https://figi.itu.int/figi-resources/dfs-security-lab/>



Thank You

