ITU Digital Financial Services Security Lab

Negash Namrud, Project Officer, ITU

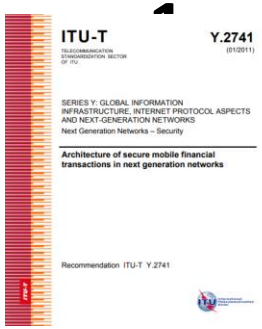
http://www.itu.int/go/dfssl

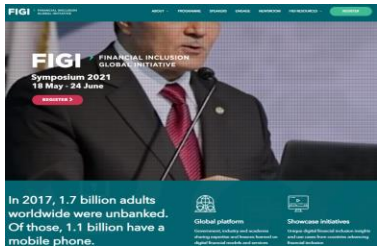
January 2025

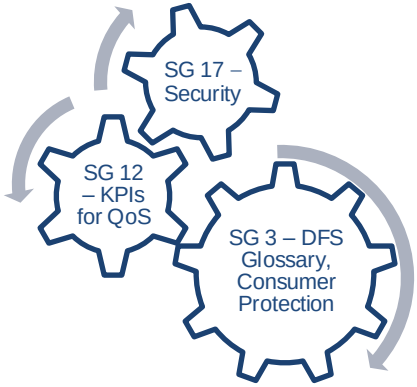
Overview

1. ITU & Digital Finance
2. DFS Security challenges
3. DFS Security Lab
4. Security recommendations for digital finance
5. USSD, Android and iOS mobile payment app security tests
6. DFS Security Lab Knowledge Transfer phases
7. Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructure
8. Actions being implemented

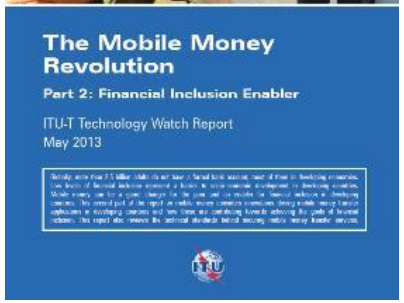
ITU & Digital Finance

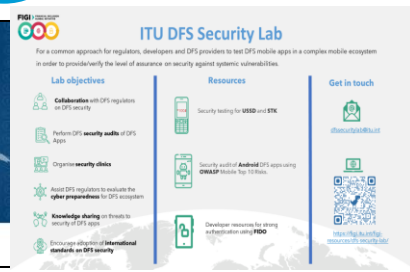






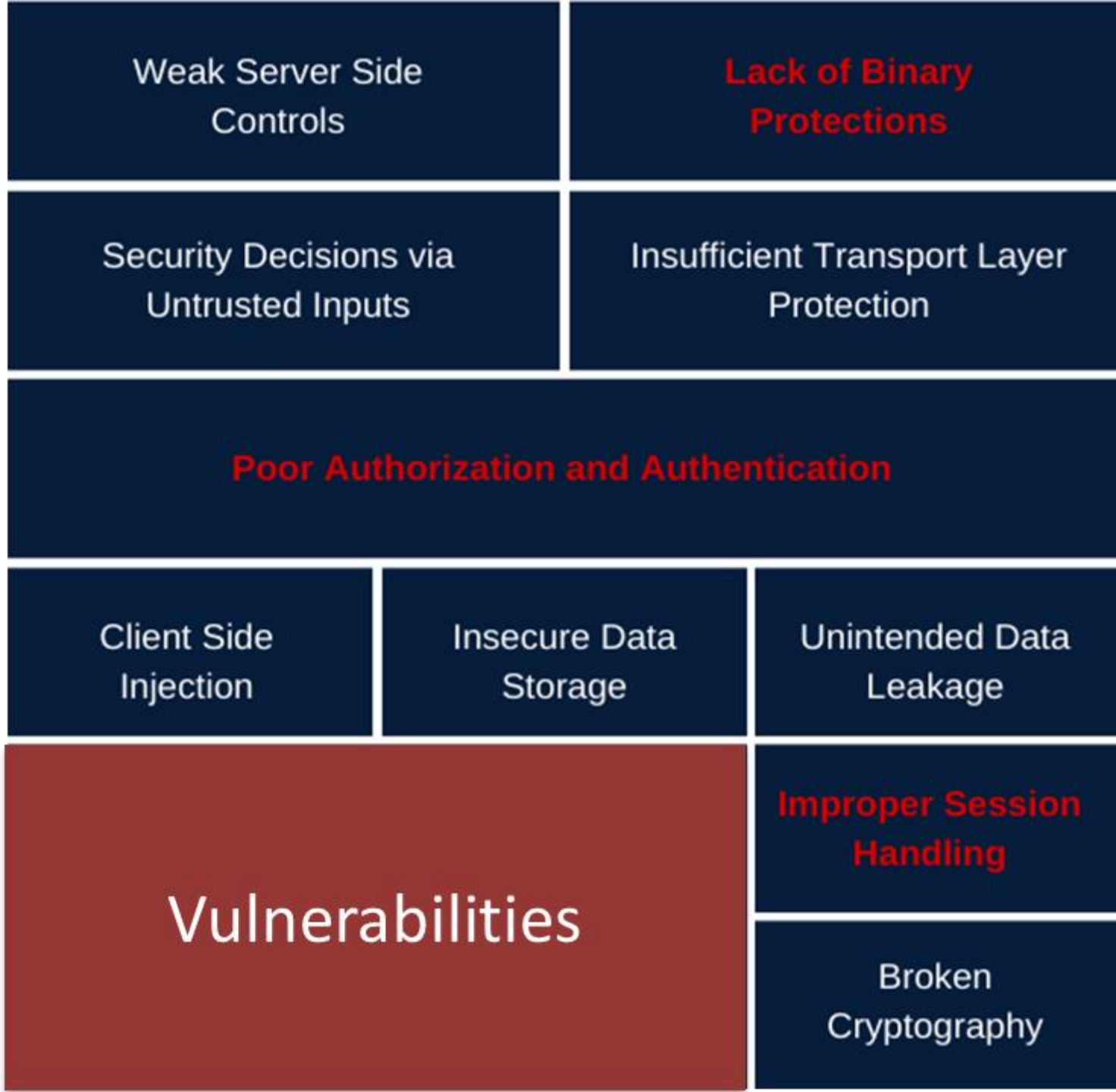
2010-2012 | 2013 | 2014 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022





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

2. DFS Security Challenges for Regulators



Objective

Provides a standard methodology to conduct security audit for mobile payment apps (USSD, Android and iOS), address systemic vulnerabilities and verify compliance against security best practices and standards.

3. DFS Security Lab

3. DFS Security Lab - Objectives

Collaborate with regulators to adopt DFS security recommendations

Perform **security audits** of mobile payment apps (USSD, Android and iOS)

Encourage adoption of **international standards on DFS security and participation in ITU-T SG17**

Organize **security clinics & Knowledge transfer** for Security Lab

Assist regulators to **evaluate** the **cyberresilience of DFS critical infrastructure**

Networking platform for regulators for knowledge sharing on threats and vulnerabilities

4. DFS Security Recommendations

The recommendations contain the following specific guidelines that may be adopted by regulators.

1. Recommendations to mitigate SS7 vulnerabilities
2. Security recommendations to protect against DFS SIM related risks
3. DFS Mobile application security Best practices (From ITU-T X.1150)
4. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
5. DFS consumer competency framework


ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

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

SERIES X: Data networks, open system communications and security

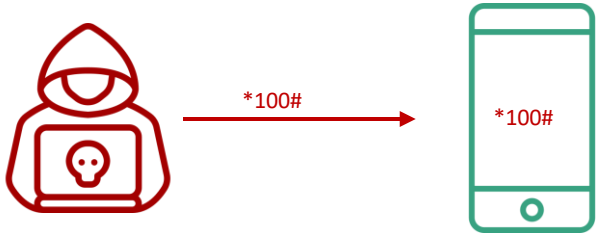
Secure applications and services (I) – Application Security (I)

Security assurance framework for digital financial services

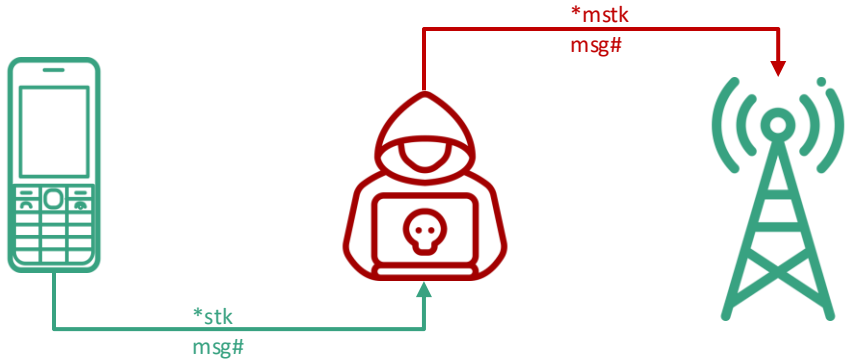
5. USSD & STK Security Audit Tests

a. **SIM Swap** and **SIM cloning**

b. susceptibility to **binary OTA attacks** (SIM jacker, WIB attacks)



c. **remote USSD** execution attacks



d. **man-in-the-middle attacks** on STK based DFS applications

Android and iOS App Mobile Payment App Security Audit Tests

- M1 Improper Credential Usage
- M2 Inadequate Supply Chain Security
- M3 Insecure Authentication/Authorization
- M4 Insufficient Input/Output Validation
- M5 Insecure Communication
- M6 Inadequate Privacy Controls
- M7 Insufficient Binary Protections
- M8 Security Misconfiguration
- M9 Insecure Data Storage
- M10 Insufficient Cryptography

6. ITU DFS Security Lab Knowledge Transfer Phases

The knowledge transfer programme for regulators to verify the security assurance of mobile payment applications based on Android, iOS, and USSD.

The objective is to empower the staff of the regulator to be able to conduct the security tests and adopt the DFS security recommendations.

Phase 1

- Regulator identifies Lab team
- Regulator ensures equipment in place
- DFS Security Clinic – Share recommendations on Digital Finance

Phase 2

- Select mobile payment app to be tested during the knowledge transfer
- Security walk throughs for testing manuals
- Verify equipment is configured

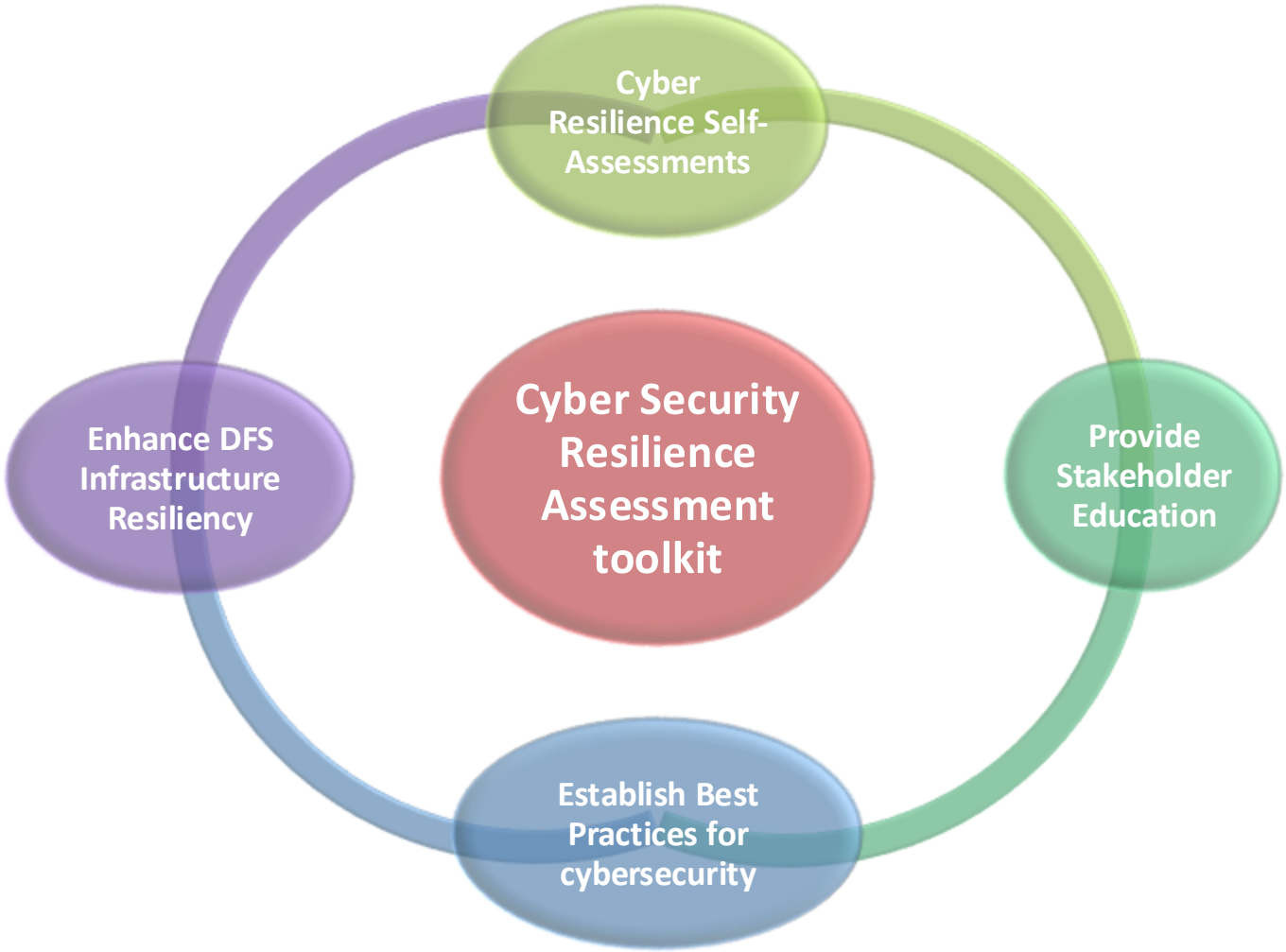
Phase 3

- Organize training on iOS, Android and USSD security testing
- Independent testing by Lab team
- Report on testing done.

Phase 4

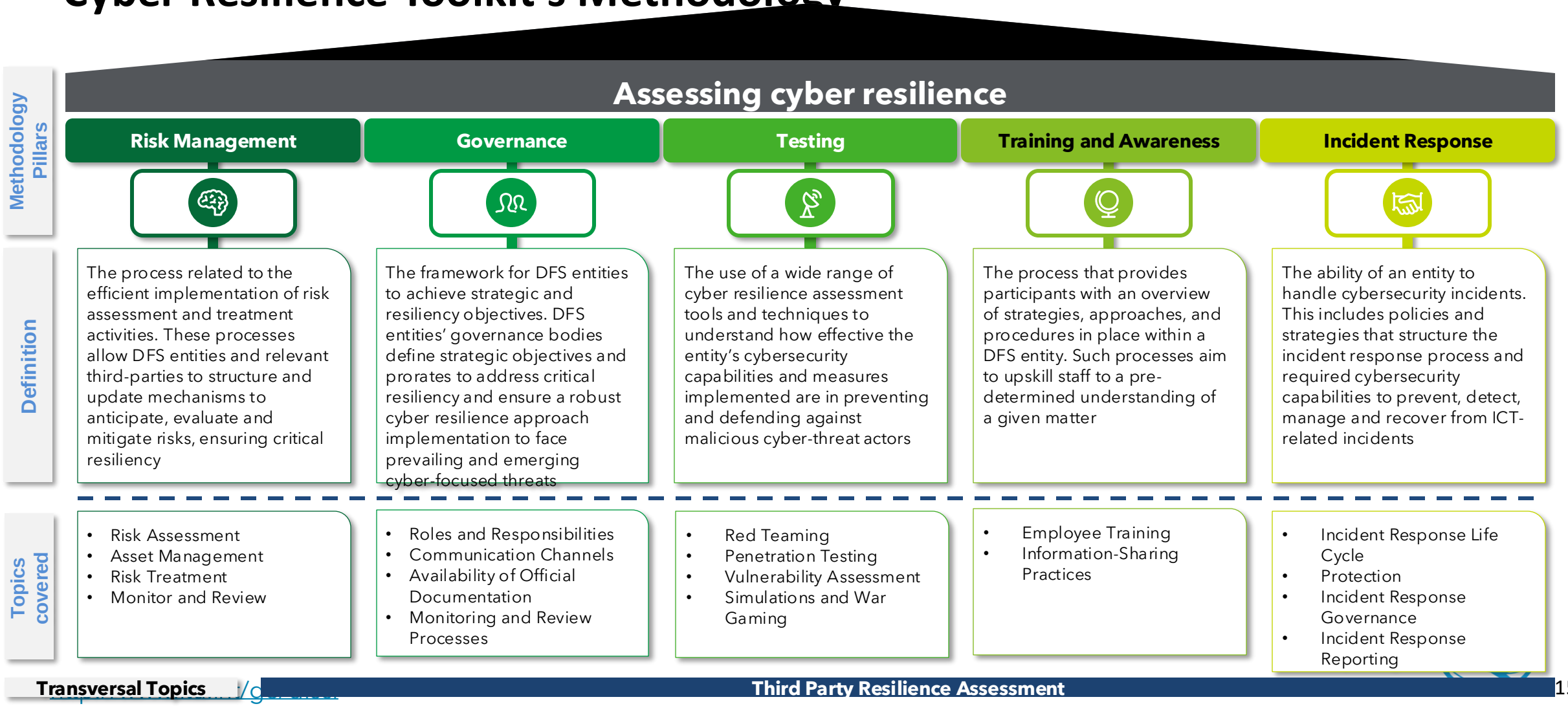
- 6-9 months period of oversight by ITU
- Mobile payment app testing review by ITU
- Sharing lessons learned of new threats and vulnerabilities

7. ITU Cyber Security Resilience Assessment Toolkit for DFS Critical Infrastructure



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

Cyber Resilience Toolkit's Methodology



Technical Assistance for Cyber Resilience Assessment Toolkit

Phase 1: Planning and Focal Point Identification (Month 1-2)

- First meeting
- Identify Focal Points
- Identify Critical Infrastructure for DFS
- Identify Key Personnel
- ITU Mission for the capacity building
- Briefing of the critical infrastructure service providers identified

Phase 2: Explaining the Cyber resilience assessment toolkit with a tabletop exercise. (Month 3-4)

- Phase 3 planning
- Capacity building on the cyber resilience assessment toolkit
- Knowledge transfer for the regulator on filling out and evaluating a real case questionnaire for the cyber resilience

Phase 3: Cyber resilience Assessment of Critical Infrastructure (Month 4-5)

- Coordination with the service providers to respond to the questionnaire for the cyber resilience assessment and assist wherever necessary.
- Analysis of the responses received.
- Report Preparation and review
- Communication of results
- Prioritize Enhancements
- Development of Road Map for monitoring cyber resilience of DFS

Phase 4: Roadmap for Cyberresilience and follow up (Duration: 12 months after phase 3)

- Coordination meetings for roadmap implementation.
- Second cyber resilience assessment after 1 year.

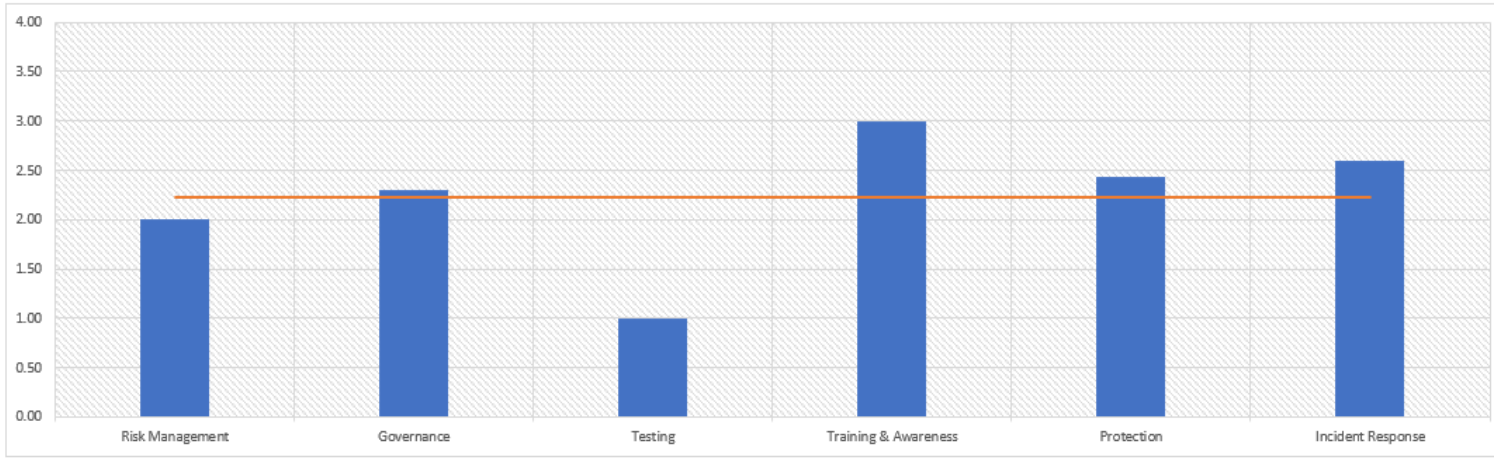
Cyber Security Resilience Assessment Toolkit

Results Summary

This section provides an overview of the results and lays the foundation for a mitigation roadmap to be identified, structured, and presented to the decision-maker. All results presented here aggregate the sub-pillars of each methodological question. For a more granu
results, the user is advised to review the results in the radar charts section.

Pillar	Resiliency Level
Risk Management	2.00
Governance	2.30
Testing	1.00
Training & Awareness	3.00
Protection	2.44
Incident Response	2.60

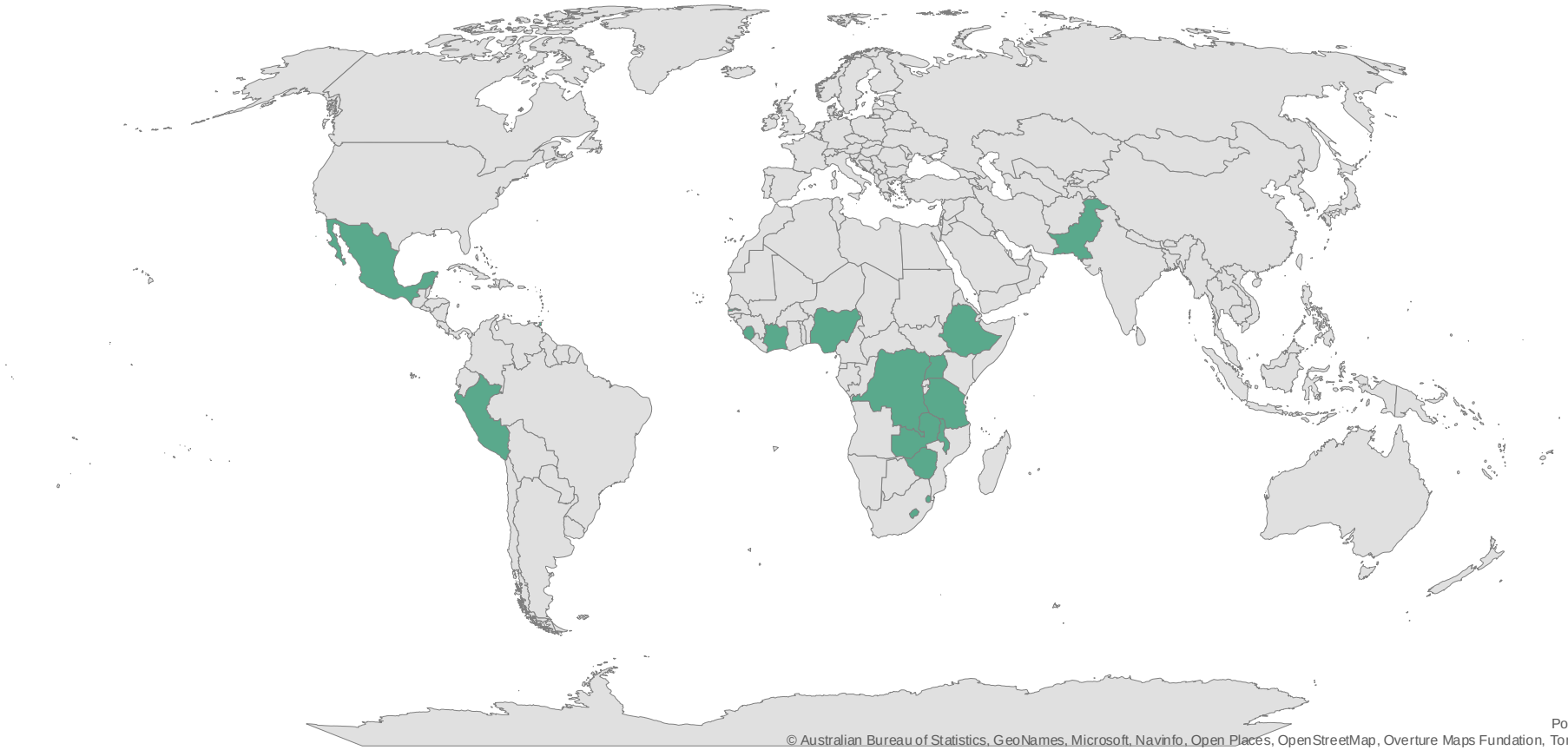
Overall score	2.22



7. Actions Being Implemented

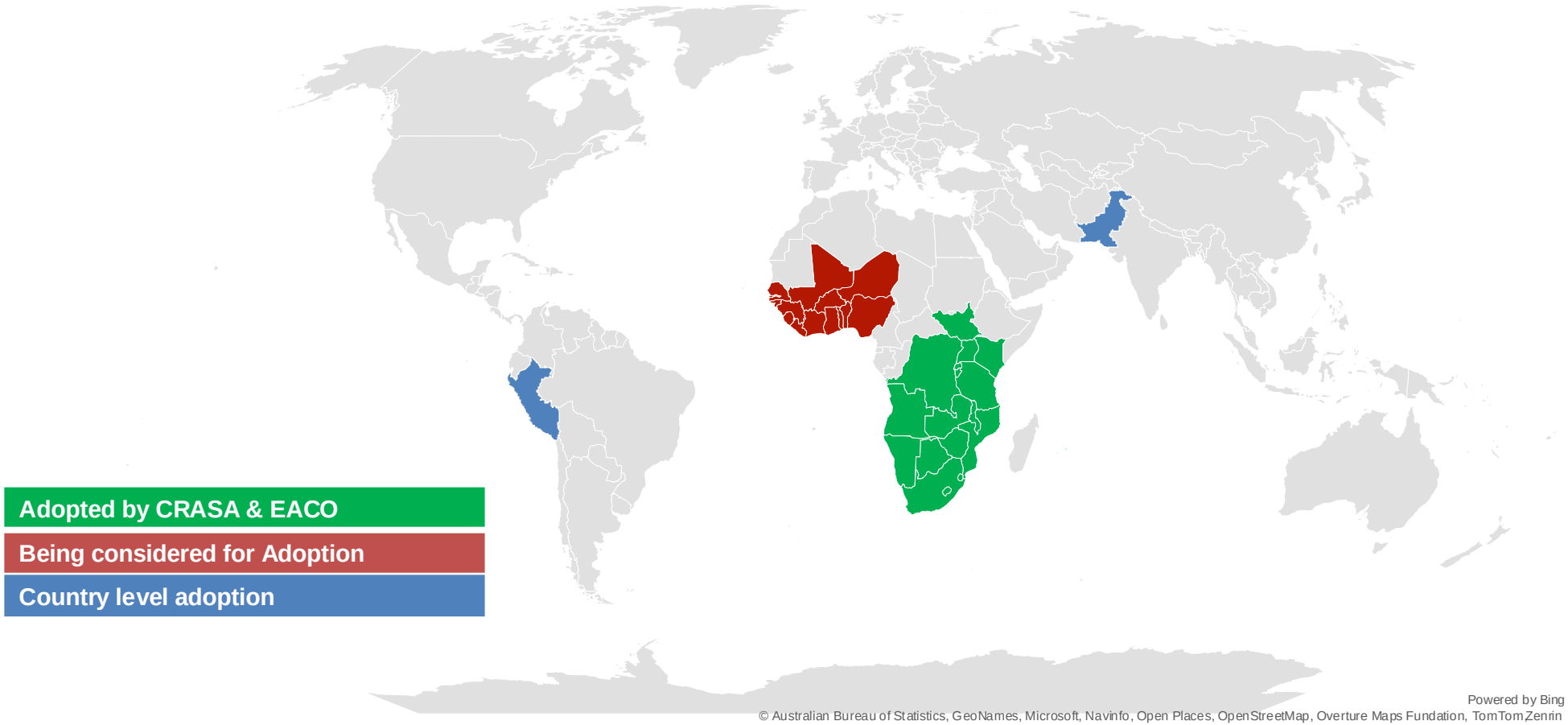
1. Organizing of DFS Security clinics with a focus on knowledge sharing on DFS security recommendations
2. Knowledge transfer for regulators (Tanzania, St. Lucia, Antigua and Barbuda, Uganda, Peru, Zimbabwe, South Sudan, Ghana, The Gambia and Ethiopia)
3. Supporting regulators on implementing DFS security recommendations
4. Conducting security audits of mobile payment applications (conducted tests for Zambia, Zimbabwe, DRC, The Gambia, Peru, Tanzania, Indonesia).
5. ITU Knowledge Sharing Platform for Digital Finance Security
6. ITU Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructure

DFS Security Clinics Held



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

Countries and Regions Adopting the Recommendations

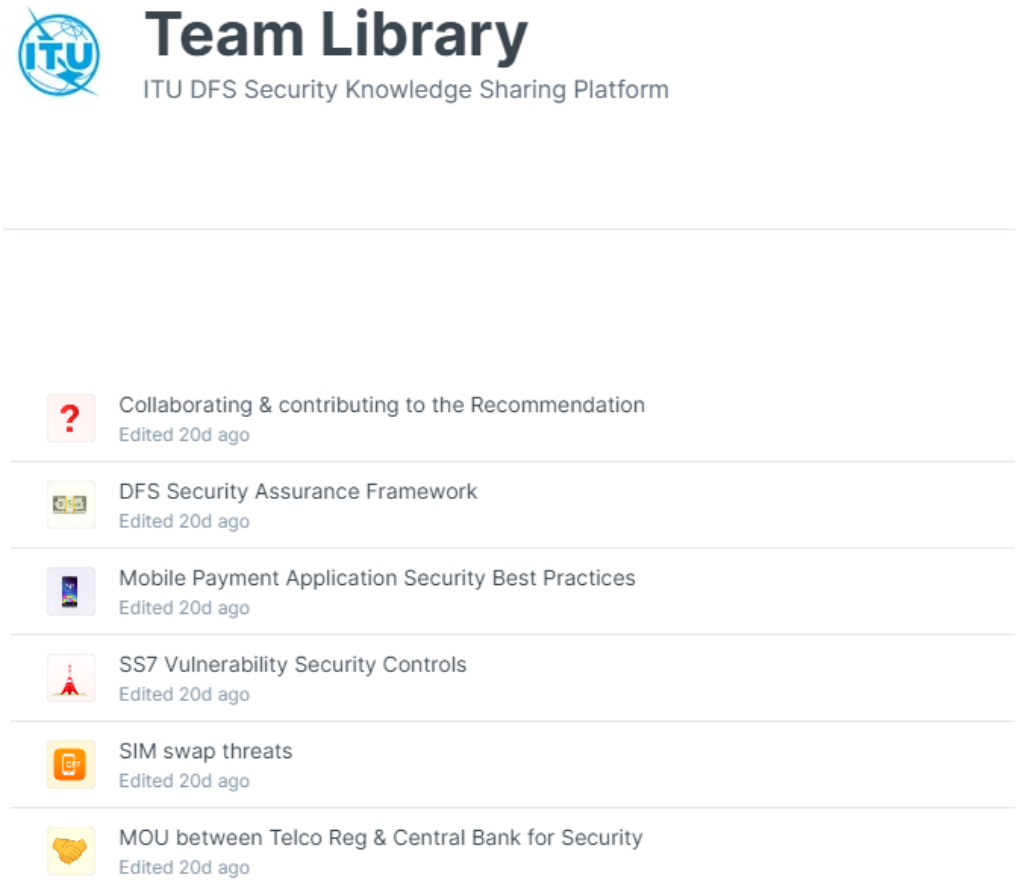


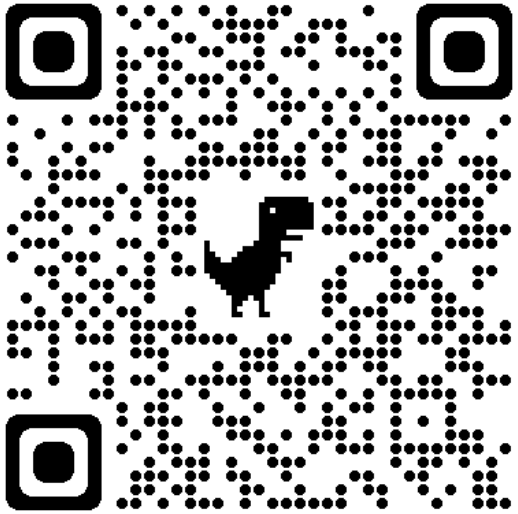
http://www.itu.int/go/dfssl

ITU Knowledge Sharing Platform for DFS

Objective

- Keep up to date the DFS security assurance framework & security recommendations.
- Share experiences, challenges, and lessons learned from the implementation of security measures across various jurisdictions.
- Communicate directly with their peers on issues relating to security of digital financial services.





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

Contact: dfssecuritylab@itu.int

Thank you!