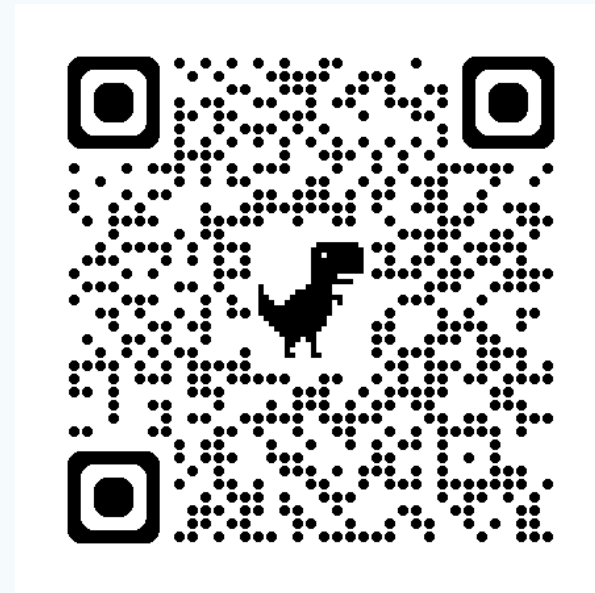


# ITU Digital Financial Services Security Lab

---

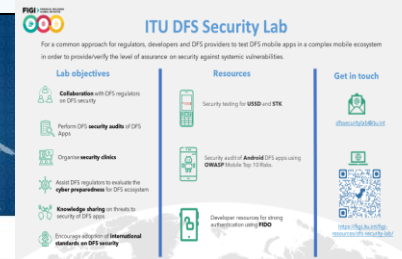
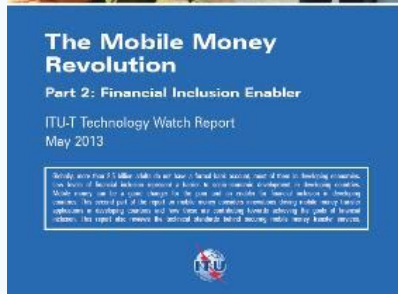
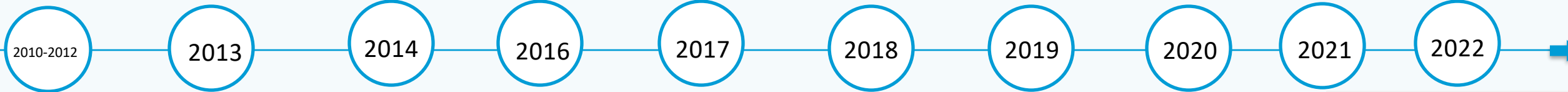
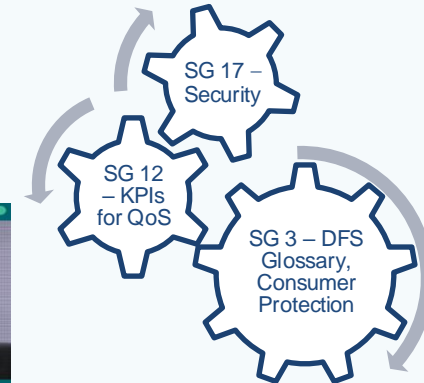
<http://www.itu.int/go/dfssl>



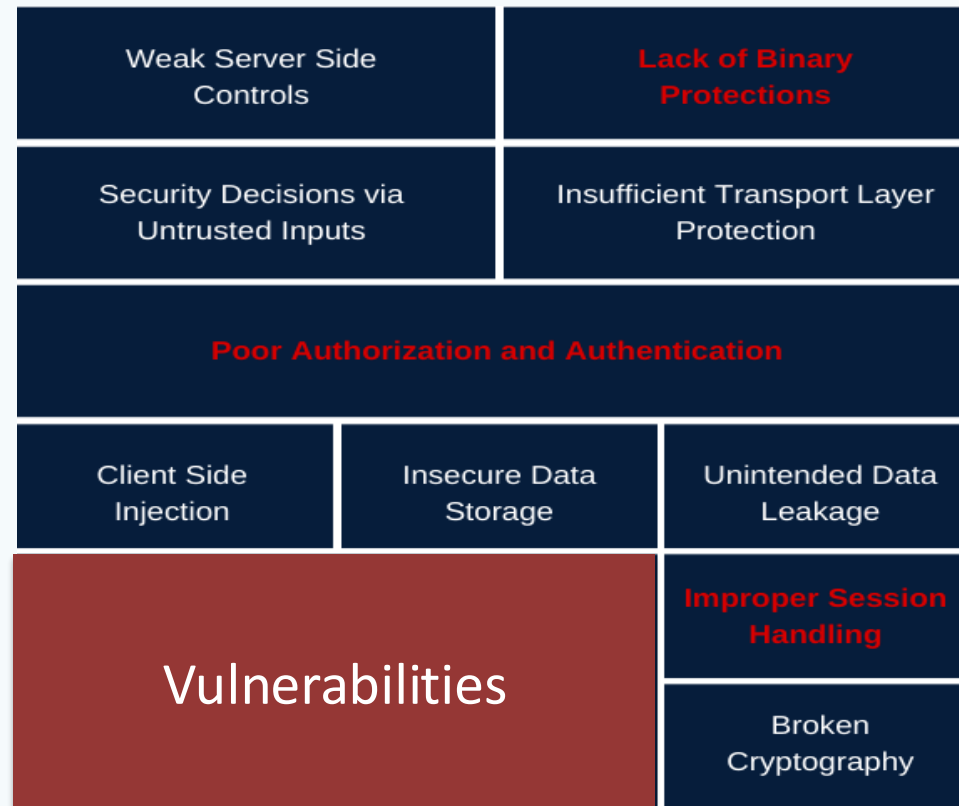
# Overview

1. ITU & Digital Finance
2. 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. Actions being implemented

# 1. ITU & Digital Finance



## 2. DFS application security challenges for regulators



### 3. DFS Security Lab

Set up and managed by TSB

#### 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.

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

### 3. DFS Security Lab

## DFS Security Lab

Cybersecurity capability of  
regulators

Security audit of mobile  
payment applications

Adoption of security best  
practices for digital finance

### 3. DFS Security Lab - Objectives



**Collaborate** with regulators to adopt DFS security recommendations from FIGI



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



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



Organise **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. Security recommendations for digital finance

Collaborate with DFS regulators and DFS providers to enhance the cybersecurity strategy for DFS and security assurance of the DFS ecosystem **by implementing the recommendations** in the following reports:

1. [DFS Security Assurance Framework](#)
2. [Security testing for USSD and STK based DFS applications](#)
3. [Security audit of various DFS applications](#)
4. [DFS security audit guideline](#)
5. [DFS Consumer Competency Framework](#)





## Adoption of DFS Security Recommendations

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

1. [Recommendations for regulators to mitigate SS7 vulnerabilities](#)
2. [Security recommendations to protect against DFS SIM risks and SIM swap fraud](#)
3. [Mobile Application Security Best practices](#) (From [ITU-T X.1150](#) - Section 9)
4. [Template for a Model MOU between a Telecommunications Regulator and Central Bank on Digital Financial Services Security](#)
5. [DFS consumer competency framework](#)

Link: [DFS Security recommendations for regulators and DFS providers developed under FIGI](#)

### 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**

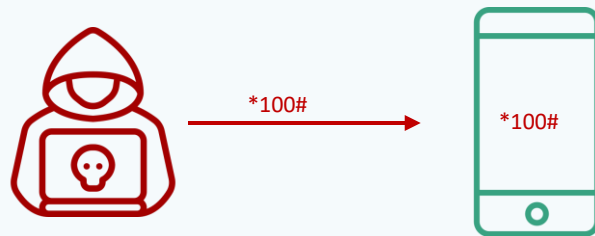
## 5. USSD & STK security audit tests



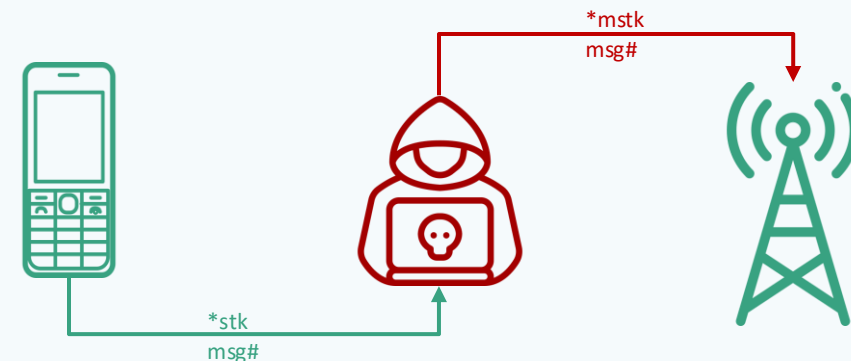
a. **SIM Swap** and **SIM cloning**



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

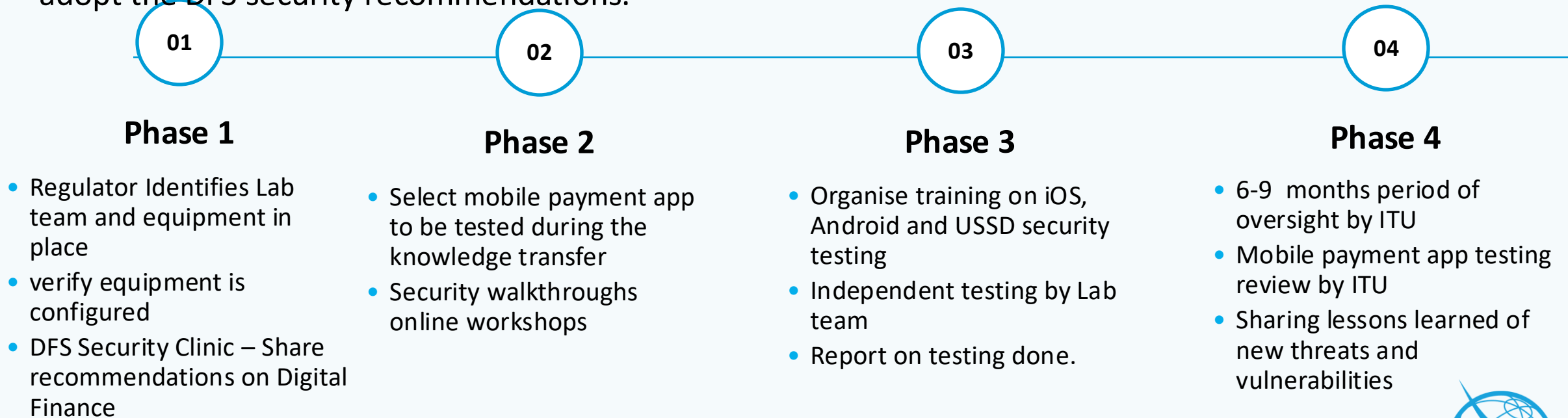
# Android and iOS app mobile payment app security audit tests

- 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. DFS Security Lab Knowledge Transfer phases

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

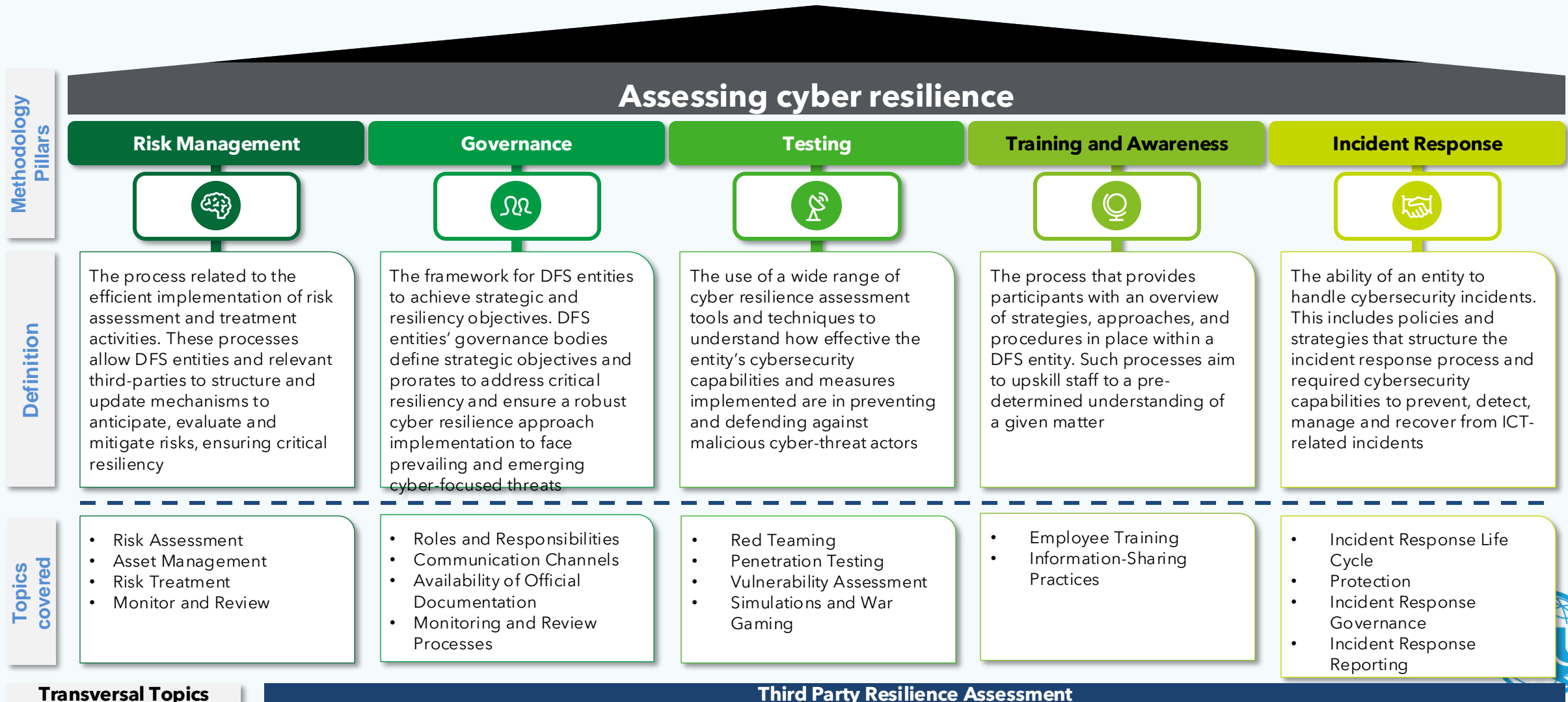
The objective is to empower the staff of the regulator to be able to conduct the security tests and adopt the DFS security recommendations.



## 7. ITU Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructure



# Cyber Resilience toolkit's methodology



# Technical assistance for Cyber Resilience Assessment toolkit

Technical assistance for regulators to facilitate cyber resilience self-assessments and enhance the resiliency of the Digital Financial Services (DFS) infrastructure.

01

## 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

02

## 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

03

## 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

04

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

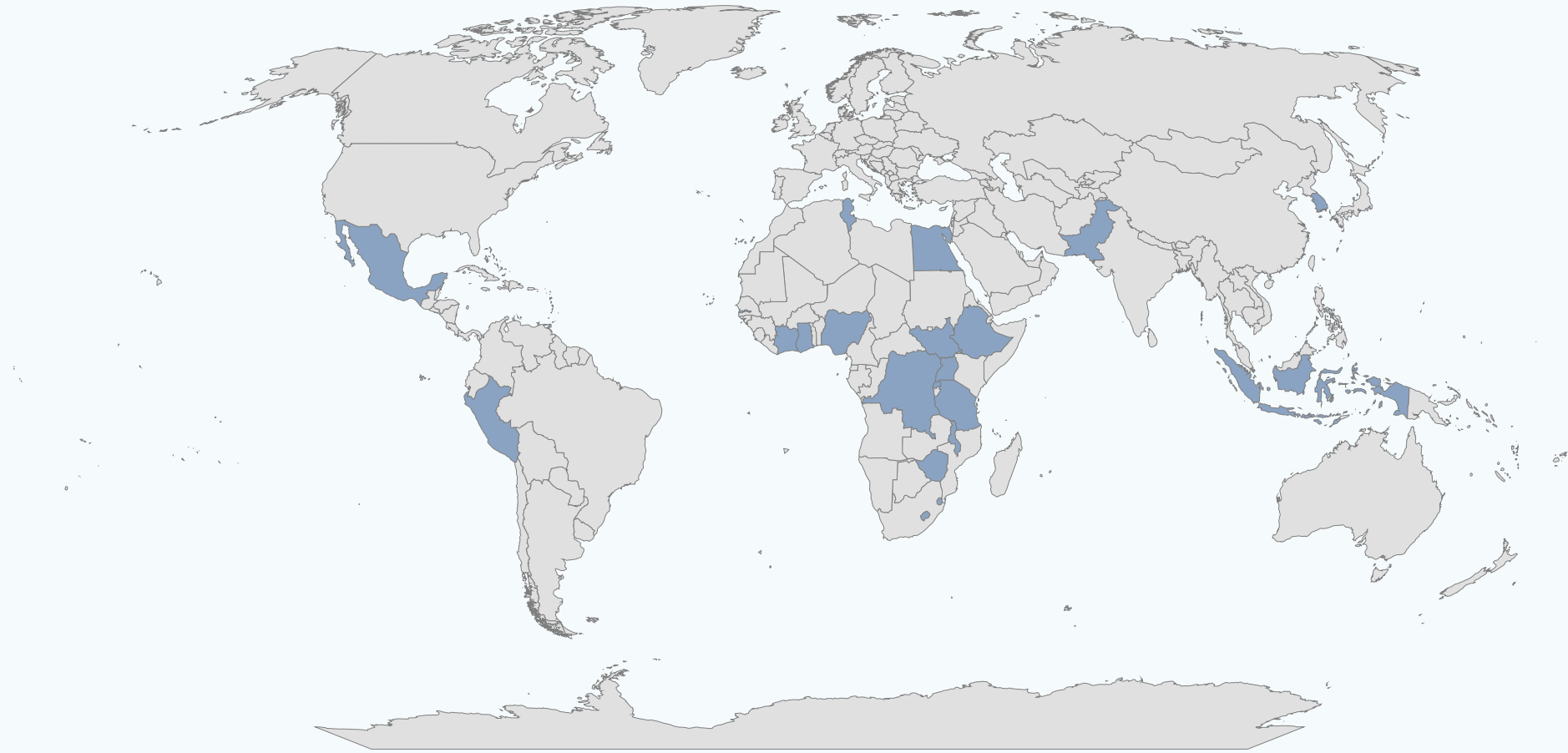
- Coordination meetings for roadmap implementation.
- Second cyber resilience assessment after 1 year.



## 7. Actions being implemented

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

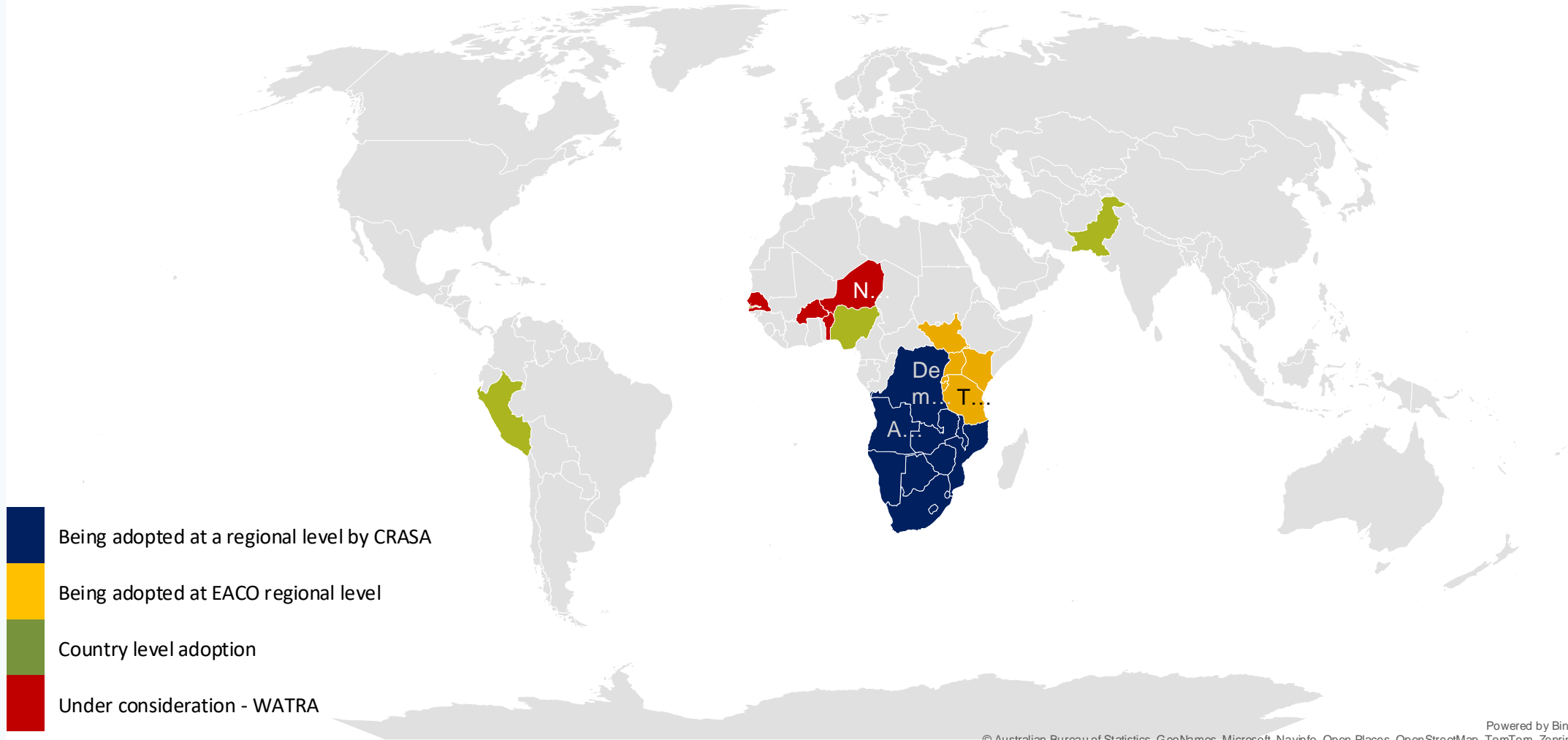
## DFS security clinics held in 2021-2024



Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Security Clinics were held in some 27 countries, 3 regional bodies

## Countries and Regions adopting the recommendations



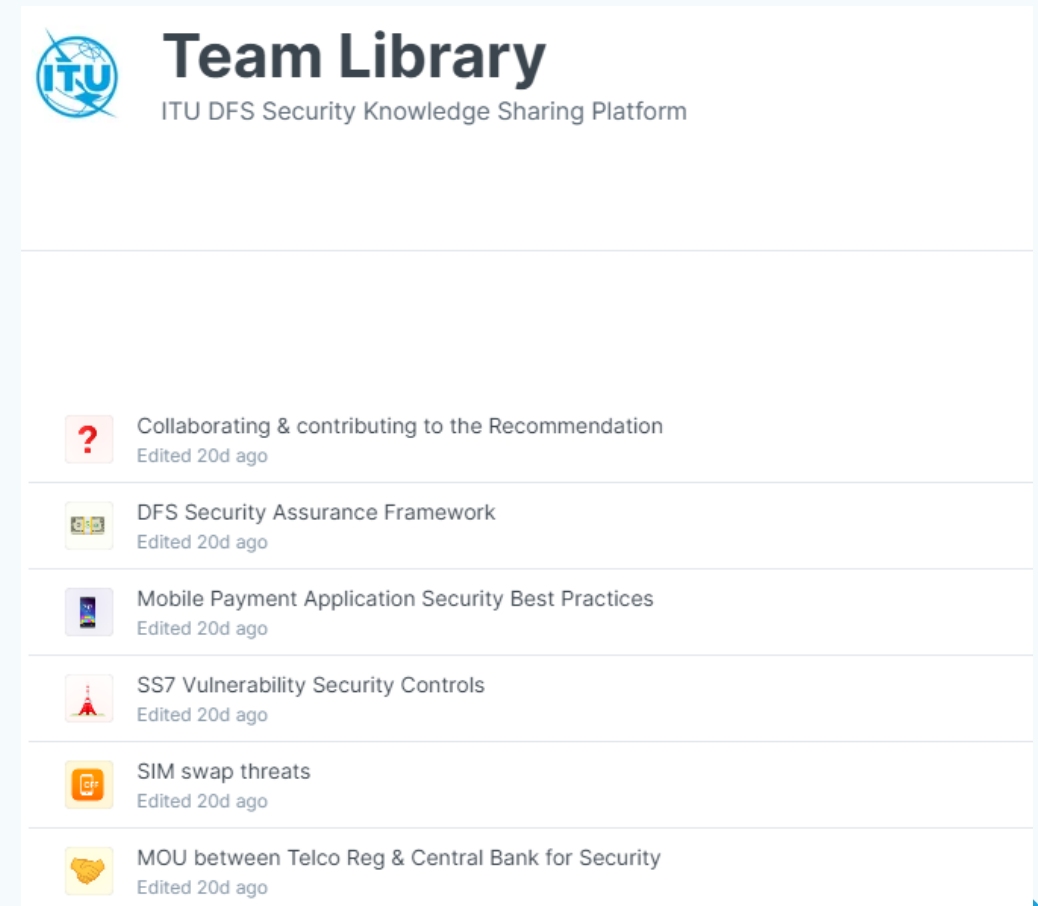
Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

# ITU Knowledge Sharing Platform for Digital Finance Security

## Objective

- Collaborate with ITU to 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.

<https://www.itu.int/en/ITU-T/dfs/Pages/share-platform.aspx>




# How to register to the ITU Knowledge Sharing Platform for Digital Finance Security


Scan qrcode to go to registration page




<https://www.itu.int/en/ITU-T/dfs/Pages/share-platform.aspx>

 **Team Library**  
ITU DFS Security Knowledge Sharing Platform


---

 Collaborating & contributing to the Recommendation  
Edited 20d ago


---

 DFS Security Assurance Framework  
Edited 20d ago


---

 Mobile Payment Application Security Best Practices  
Edited 20d ago


---

 SS7 Vulnerability Security Controls  
Edited 20d ago

---

 SIM swap threats  
Edited 20d ago

---

 MOU between Telco Reg & Central Bank for Security  
Edited 20d ago



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

Contact: [dfssecuritylab@itu.int](mailto:dfssecuritylab@itu.int)

**Thank you!**