

Digital Financial Services Security Lab

Vijay Mauree
Programme Coordinator
Standardization Bureau, ITU

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 audit
6. Setting up the security lab & Knowledge transfer for regulators
7. Actions being implemented

ITU Digital Finance & Inclusion Journey

ITU-T
TELECOMMUNICATIONS STANDARDIZATION SECTOR OF ITU

Y.2741
(01/2011)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS
Next Generation Networks – Security

Architecture of secure mobile financial transactions in next generation networks

Recommendation ITU-T Y.2741

ITU FOCUS GROUP DIGITAL FINANCIAL SERVICES: MAIN RECOMMENDATIONS

ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

FIGI symposium
29 November - 1 December 2017
Bengaluru, India
#financialinclusion

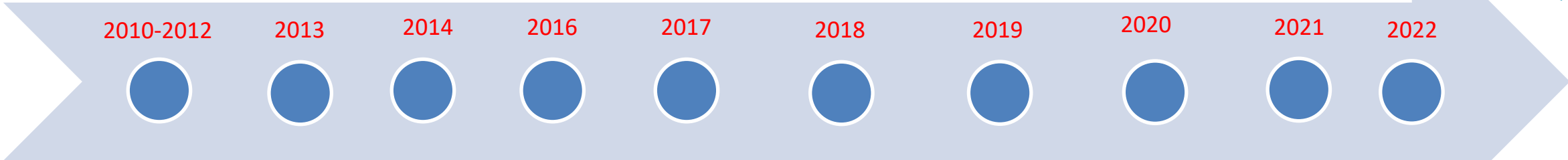
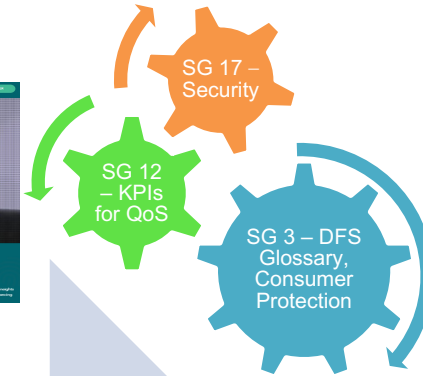
FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium
22-24 January 2019
Cairo, Egypt

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium 2021
18 May - 24 June

In 2017, 1.7 billion adults worldwide were unbanked. Of those, 1.1 billion have a mobile phone.



The Mobile Money Revolution
Part 2: Financial Inclusion Enabler
ITU-T Technology Watch Report
May 2013

Tech Watch Report Mobile Money

FOCUS GROUP
Digital Currency including Digital Fiat Currency
Standards for digital fiat currency for financial inclusion

Res. 89
wtsa.16
TUNISIA
WORLD TELECOMMUNICATIONS STANDARDIZATION ASSEMBLY
25 OCTOBER - 3 NOVEMBER
HAMMAMET, TUNISIA

Workshop on standardizing Digital Fiat Currency and its Applications
18 - 20 July 2018
New York City, USA

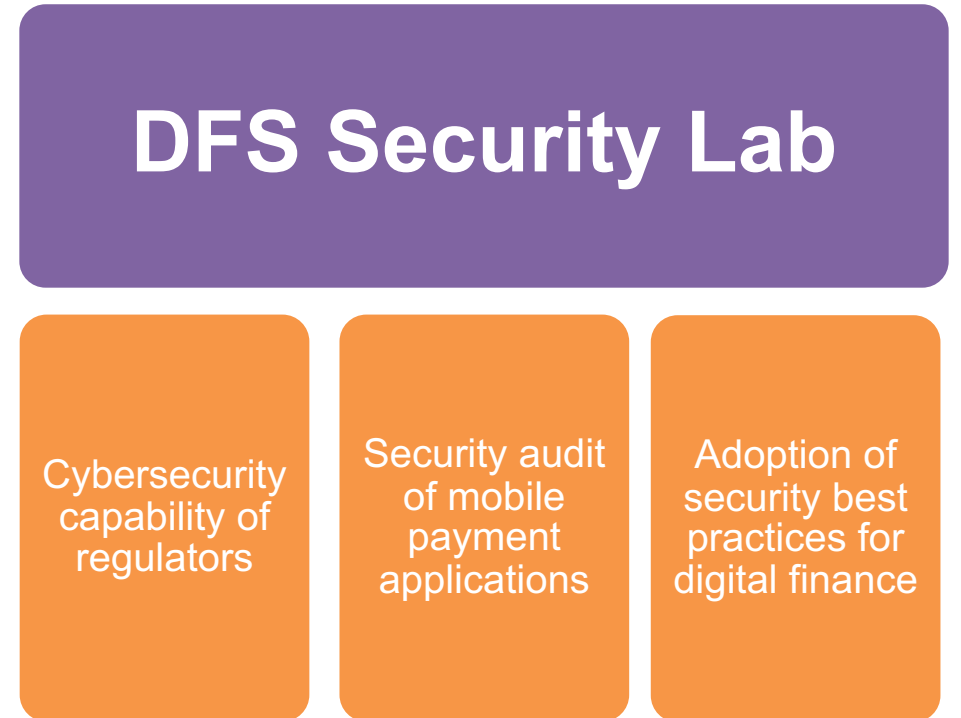
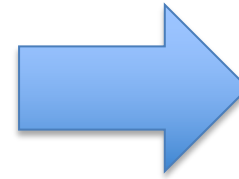
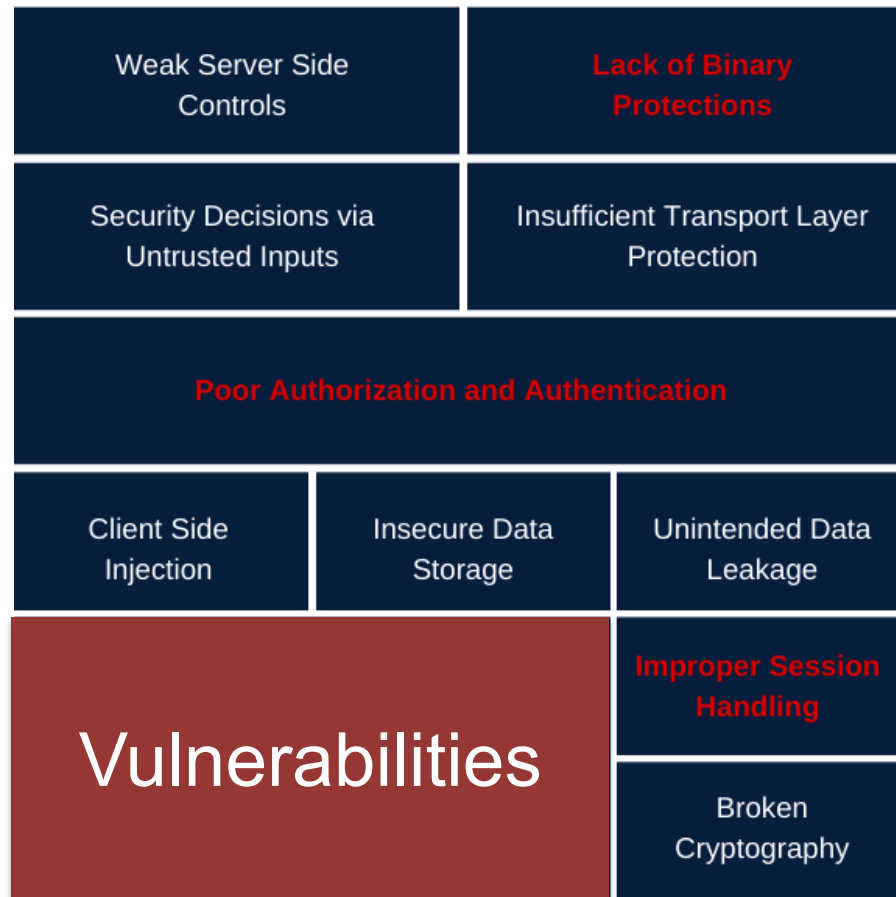
Workshop on standardizing Digital Fiat Currency and its Applications
18 - 20 July 2018
New York City, USA

Digital Currency Global Initiative

ITUEvents
Insights on Digital Financial Services during COVID-19 Webinar Series

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 progressively the level of assurance on security against systemic vulnerabilities.

DFS security challenges for regulators



DFS Security Lab

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

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

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)



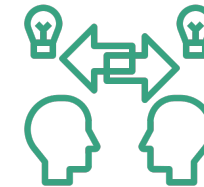
Encourage adoption of **international standards on DFS security** and participate in ITU-T SG17



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

Adoption of Security Recommendations

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:

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](#)



See <https://figi.itu.int/figi-resources/working-groups/>

Adoption of Security Recommendations

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

1. Recommendations to mitigate SS7 vulnerabilities
2. Model Memorandum of Understanding between a Telecommunications Regulator and a Central Bank Related to Security for Digital Financial Services
3. Recommendations for securing mobile payment apps
4. Recommendations for operators and regulators for SIM card risks such as SIM swap fraud and SIM card recycling

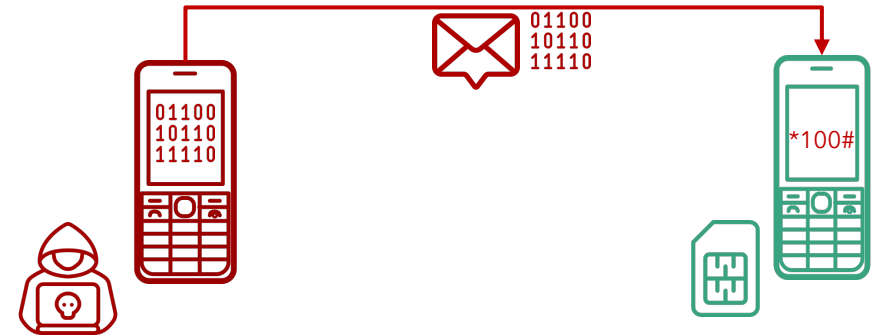


See <https://figi.itu.int/figi-resources/working-groups/>

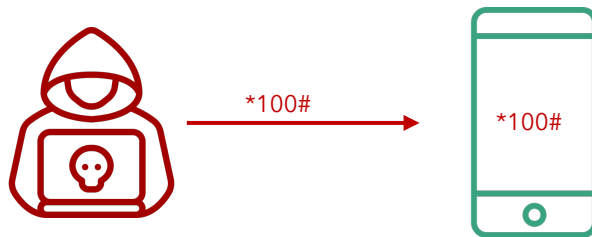
USSD & STK tests



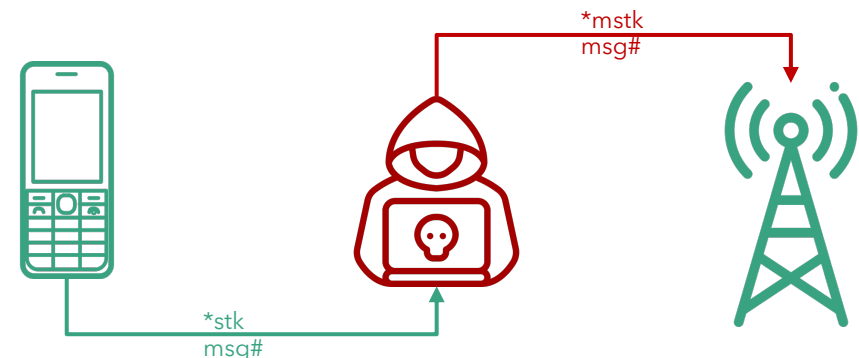
a. **SIM Swap** and **SIM cloning**



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 security tests

Risks	Security test
M1 Improper Platform Usage	Check misuse of platform features or failing to use platform security controls provided
M2 Insecure Data Storage	Check that malware and other apps do not have access to DFS sensitive information
M3 Insecure Communication	Check that communication channels are encrypted
M4 Insecure Authentication	Authentication cannot easily be bypassed
M5 Insufficient Cryptography	Check crypto algorithms used
M8 Code Tampering	Check whether it is possible to modify the code
M9 Reverse engineering	Decompile source code

DFS Security Lab Knowledge Transfer

Phase 1

- Lab team and Equipment in place
- verify equipment is configured
- DFS Security Clinic

Phase 2

- Select mobile payment app
- Security walkthroughs online workshops

Phase 3

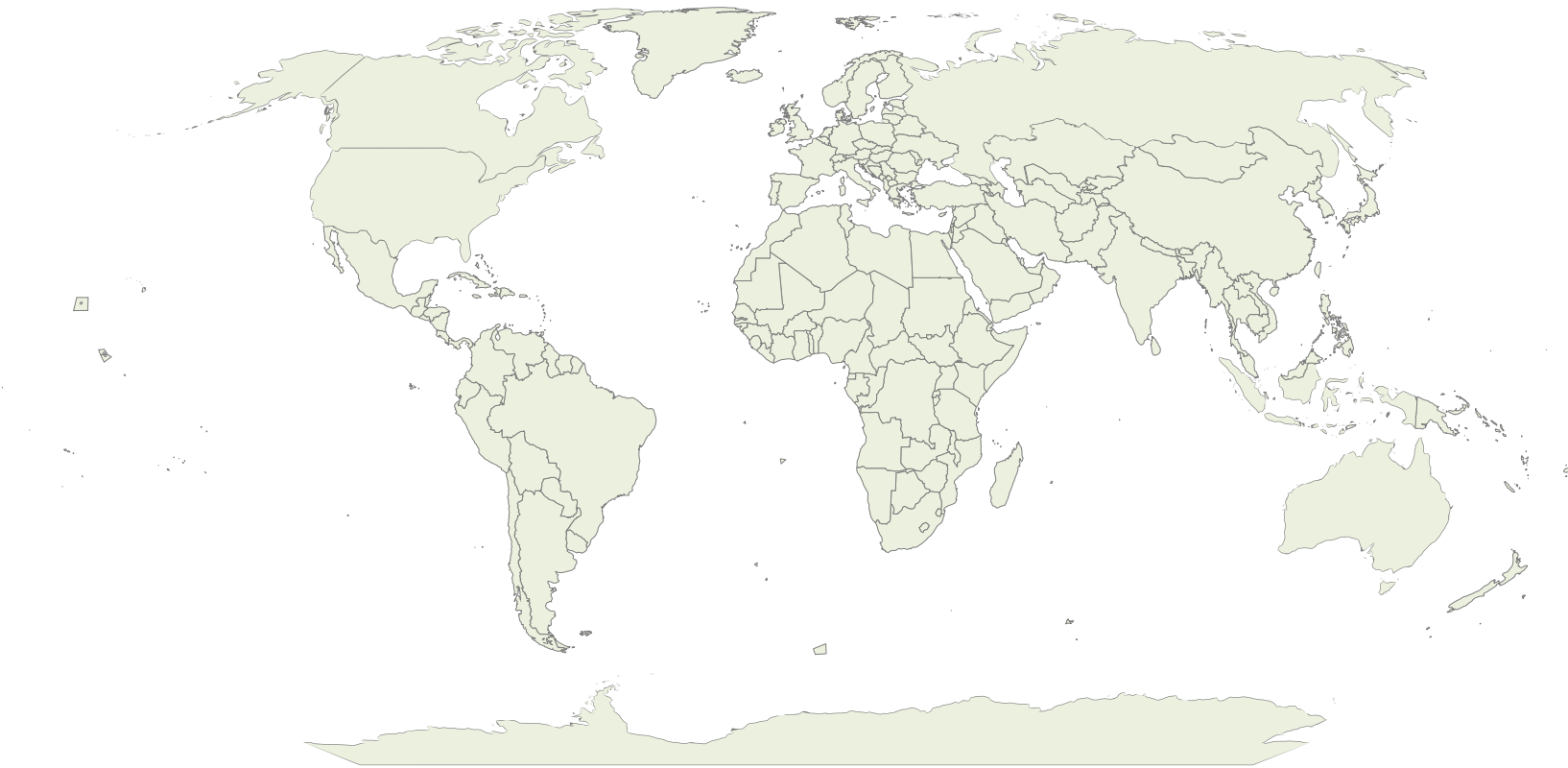
- Organise training on iOS, Android and USSD security testing
- Independent testing by Lab team
- Report on testing done

Phase 4

- 6-9 months period of oversight by ITU
- Mobile payment app testing reviewed by ITU
- Lessons learned of new threats and vulnerabilities

Actions being implemented

1. Organisation of DFS Security clinics with a focus on knowledge sharing on DFS security recommendations from FIGI
2. Knowledge transfer for regulators of Tanzania, Uganda and Peru to set up DFS Security Lab
3. Guidance on implementing recommendations DFS security recommendations
4. Conduct security audits of mobile payment applications and SIM cards (Zambia, Zimbabwe, The Gambia, Peru, Tanzania and Uganda).
5. ITU Knowledge Sharing Platform for Digital Finance Security
6. ITU Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructure

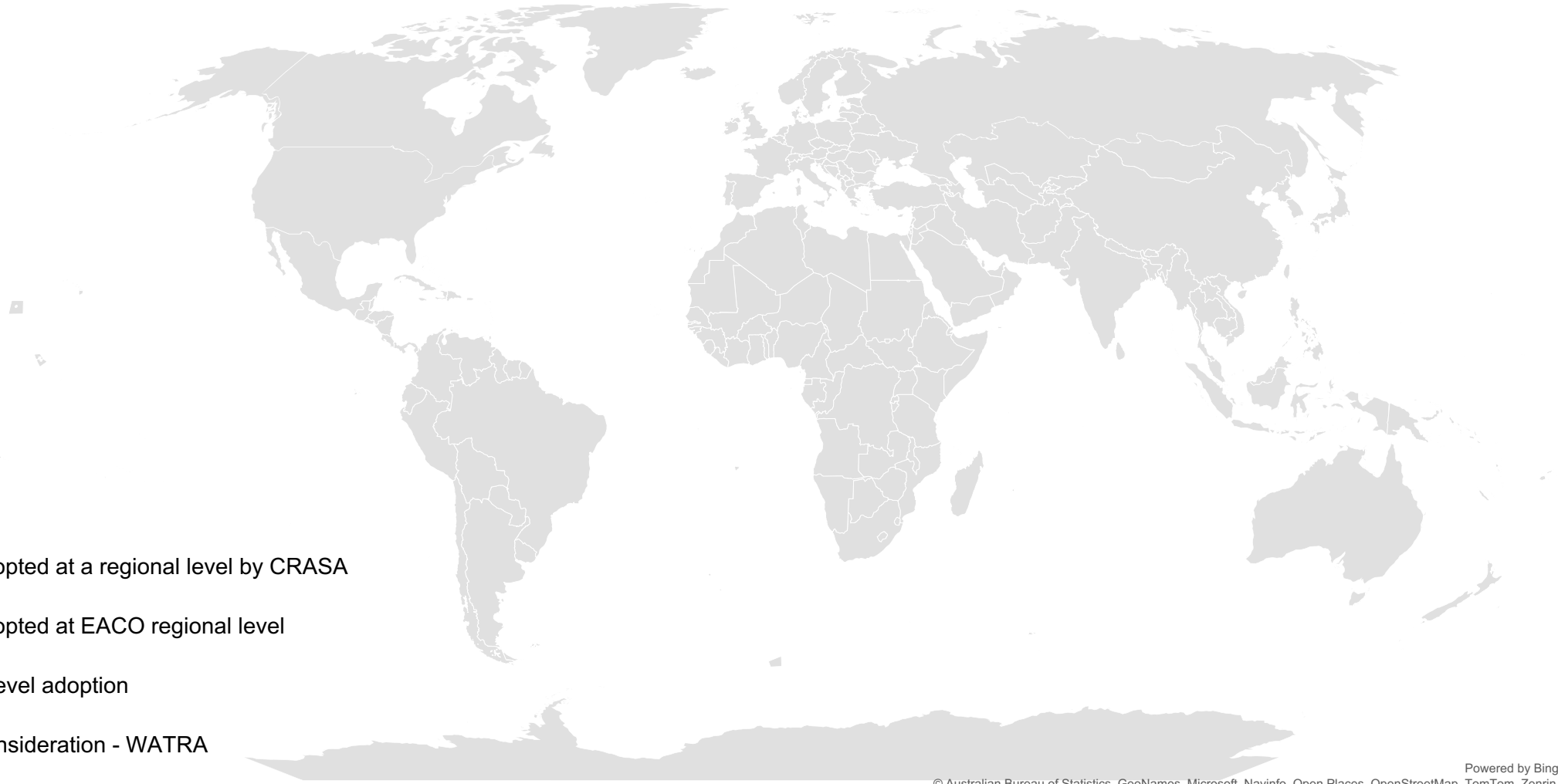


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

DFS security clinics held in 2021, 2022, 2023

Security Clinics were held in some 18 countries

Countries and Regions adopting the recommendations



- Being adopted at a regional level by CRASA
- Being adopted at EACO regional level
- Country level adoption
- Under consideration - WATRA

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

Examples: Adoption of the recommendations



Business Rules & Operational Processes for
Implementation of the SIM Replacement Guidelines 2022

April 2022

[NCC Sim replacement rules](#)

The screenshot shows the State Bank of Pakistan website. The header includes the SBP logo and name in Urdu and English, along with social media icons and a search bar. The navigation menu includes Home, About SBP, Laws & Regulations, Circulars/Notifications, Monetary Policy, Financial Markets, Publications, and Economic Data. The main content area is titled "Circulars/Notifications - Payment System Department" and features a circular titled "PSPOD Circular No 01 of 2022" dated April 26, 2022. The circular is addressed to the Presidents/CEOs of all banks, MFIs, PSOs, PSPs, and EMIs. It discusses the growing use of mobile payment applications and the need for security guidelines. The circular includes four numbered points: 1. Mobile payment applications (mobile apps) have become an alternate payment channel for a growing number of users. SBP regulated entities have been offering innovative products and services through mobile applications. Consequently, opportunities for the fraudsters to exploit vulnerabilities in mobile apps and defraud the customers have also increased manifold. 2. In line with international standards and best practices, SBP has developed comprehensive Mobile App Security Guidelines (the "Guidelines") providing baseline security requirements for app owners in order to ensure confidentiality and integrity of customer data and availability of app services in a secure manner, when developing payment applications for mobile or other smart devices. 3. App owners shall use these Guidelines for the architecture, design, development and deployment of mobile 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 with the requirements of these Guidelines latest by December 31, 2022. The circular concludes with the text "Enclosure: Mobile Applications (Apps) Security Guidelines" and is signed by Shoukat Bizinjo, Additional Director.

SBP Mobile Application security guidelines

ITU Knowledge Sharing Platform for Digital Finance Security



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

Objective

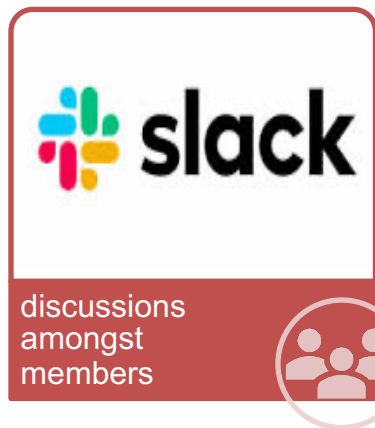
- Collaborate with ITU to keep up to date the DFS security assurance framework security controls and DFS security recommendations.
- Share experiences, challenges, and lessons learned from the implementation of security measures across various jurisdictions.
- Communicate directly with their peers on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



[Knowledge Sharing Platform for Digital Finance Security \(itu.int\)](https://itu.int)

ITU Knowledge Sharing Platform for Digital Finance Security

The collaboration tools



Visit website to find more on how to join:

[Knowledge Sharing Platform for Digital Finance Security \(itu.int\)](https://staging.itu.int/en/ITU-T/dfs/Pages/share-platform.aspx)

https://staging.itu.int/en/ITU-T/dfs/Pages/share-platform.aspx



Knowledge Sharing Platform for Digital Finance Security

YOU ARE HERE ITU > HOME > ITU-T > DFS > KNOWLEDGE SHARING PLATFORM FOR DIGITAL FINANCE SECURITY

SHARE    

The ITU Knowledge Sharing Platform for Digital Finance Security is designed to foster collaboration among regulators and other stakeholders in the development and implementation of security guidelines and best practices for Digital Financial Services (DFS).

The WTS-20 Resolution 89 instructs the Director of the Telecommunication Standardization Bureau, in collaboration with the Directors of the other Bureaux to establish a platform or, where possible, connect to those already existing, for peer learning, dialogue and experience-sharing in digital financial services among countries and regions, regulators from the telecommunication and financial services sectors, industry experts and international and regional organizations; PP-22 Resolution 204 further instruct pertinent ITU-T study groups to participate in global initiatives aimed at enhancing the cybersecurity and resiliency of the digital finance ecosystem. This involves developing international standards and industry best practices to ensure a secure and robust digital financial landscape.

The ITU Knowledge Sharing Platform is a component of the ITU DFS security lab, which provides resources for conducting security tests for Mobile payment applications as well as developer resources for Fast Identity Online (FIDO) implementation of strong consumer authentication.

The Objectives of the Knowledge Sharing Platform are as follows:

- Collaborate with ITU to keep up to date the DFS security assurance framework security controls and DFS 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.

ITU Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructures

Objectives

- 1. Facilitate Cyber Resilience Self-Assessments:** To empower DFS entities, users, and actors to proactively assess their existing security protocols and identify potential vulnerabilities.
- 2. Enhance DFS Infrastructure Resiliency:** Reinforce both peripheral and internal defences of the DFS infrastructure, bolstering resistance against potential cyber threats.
- 3. Provide Stakeholder Education:** Equip stakeholders from various sectors within the DFS ecosystem, including telecommunications and finance, with the knowledge to prepare for and defend against malicious cyber operations and unauthorized access attempts.
- 4. Establish Best Practices:** Encourage the adoption and implementation of effective cyber defence practices tailored to each DFS entity's unique needs

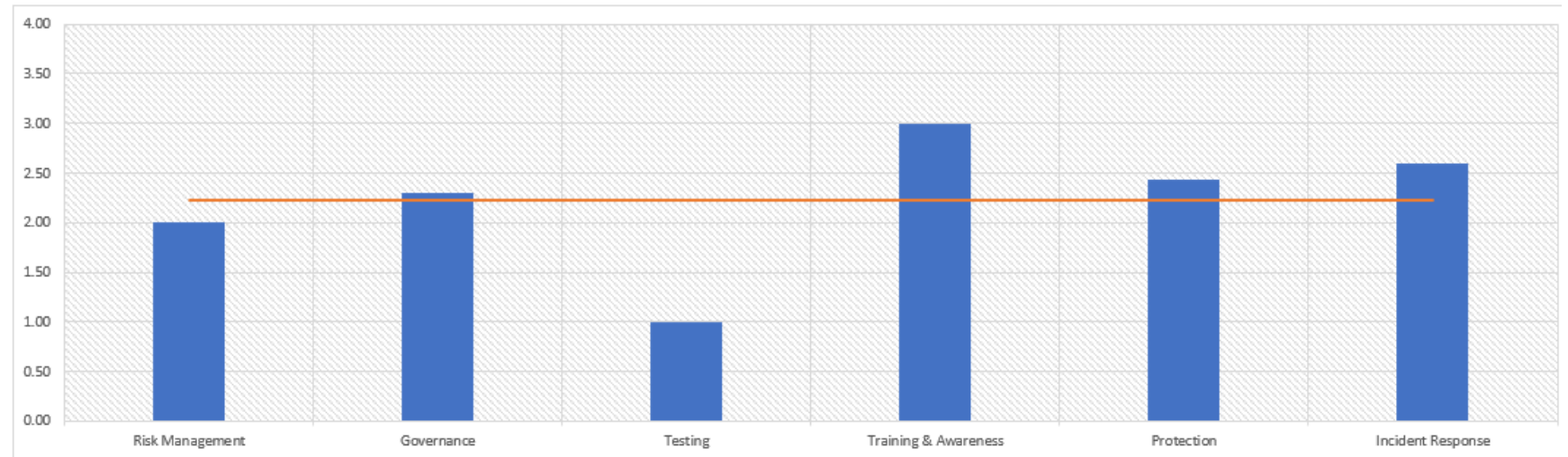
Results assessment summary: Cyber Security Resilience Assessment toolkit



Results Summary

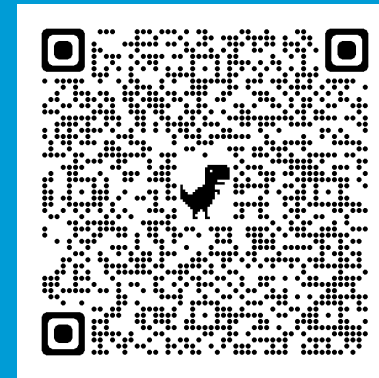
This section provides an overview of the results and lays the foundation for a mitigation roadmap to be identified, structured, and presented to the decision-maker. All results presented here aggregate the sub-pillars of each methodological question. For a more granular results, the user is advised to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





Questions



Contact: dfssecuritylab@itu.int

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

