Regional Digital Financial Services Security Clinic Draft Programme

April 24-25, 2024

Draft Programme

DAY 1: April 24 2024	
08:30 - 9:00	**Registration / Participants' check-in**
09:00 - 09:30	**Welcome and opening remarks** • Mr. Seizo Onoe, Director TSB, ITU • FNSV
09:30 - 10:00	**Fintech Security** (Keynote speech on the regional context)
10:00 – 10:30	**Group Photo and coffee break**
10:30 - 11:30	**Introduction to ITU DFS Security Lab and ITU activities in the region on Digital Finance.** This session will provide a general overview of the ITU DFS Lab and the assistance that it provides to developing countries to adopt the DFS Security recommendations. The ITU DFS Security Knowledge Sharing Platform 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 session will also provide an overview of the activities of the ITU on Digital Finance and highlight how the State Bank of Pakistan has implemented the ITU DFS security recommendations. **Moderator:** • FNSV **Speaker:** • Vijay Mauree, Programme Coordinator, TSB, ITU • ITU Regional Office Asia Pacific Region • Rehan Masood, Assistant Director, State Bank of Pakistan
11:30 - 12:30	**Blockchain Secure Authentication (BSA) and deployment for passwordless authentication for DFS** The objective of this session is to provide an overview of Blockchain Secure Authentication technology and how it can be used for passwordless authentication in mobile payments. The session will also introduce the ITU developer resources for BSA. **Moderator:** ITU Regional Office Asia Pacific Region **Speaker:** • FNSV • FNSV • Arnold Kibuuka, Project Officer, TSB, ITU
12:30 – 13:00	**Introduction to the ITU BSA Application Challenge.**

	Speaker: • Vijay Mauree, Programme Coordinator, TSB, ITU • Ariff Olan, FNSV
13:00 - 14:00	**Lunch**
14:00 -15:30	**Fintech Security and Digital Financial Inclusion in Asia Pacific Region** This session will provide an overview of the Fintech security measures implemented in different countries in the Asia Pacific region. **Moderator:** FNSV **Speakers:** • Rehan Masood, Assistant Director, SBP • Heung Youl Youm, Chairman of ITU-T Study Group 17, ITU-T Study Group 17
15:30 -15:45	**Coffee Break**
15:45-17:30	**DFS security recommendations** This session will highlight the security best practices and standards to be implemented by DFS regulators and providers as mentioned in the ITU DFS security recommendations to secure the applications layer, telecom infrastructure and payment system infrastructure. In particular, the following measures will be presented: • Security recommendations to protect against DFS SIM risks and SIM swap fraud • Template for a Model MOU between a Telecommunications Regulator and Central Bank on Digital Financial Services Security • Recommendations for regulators to mitigate SS7 vulnerabilities • DFS consumer competency framework • Application Security best practices The session will also delve into mobile device security best practices. **Moderator:** Vijay Mauree, Programme Coordinator, TSB, ITU **Speakers:** • Arnold Kibuuka, Project Officer, TSB, ITU • Kevin Butler, Director, Florida Institute for Cybersecurity (FICS) Research
DAY 2: April 25 2024	
08:30 - 9:00	**Registration / Participants' check-in**
09:00-10:00	**Managing risk in digital financial services** DFS providers should put in place adequate measures to address the security threats and vulnerabilities and demonstrate compliance against regulatory measures. This session will consider the various threats and vulnerabilities that can impact the confidentiality, integrity, and availability of digital financial services from a value chain perspective. The session will also highlight mitigation measures that DFS providers can implement to reduce the impact of these risks and discuss a

	framework that can be implemented by DFS providers to better manage the risks and show compliance. Moderator: FNSV Speakers: • Vijay Mauree, Programme Coordinator, TSB, ITU • Rehan Masood, Assistant Director, SBP • *Heung Youl Youm, Chairman of ITU-T Study Group 17, ITU-T Study Group 17 (tbc)*
10:00 – 10:45	**DFS cyber resilience toolkit tabletop exercice (Part 1)** This session will introduce the ITU DFS cyber resilience toolkit for regulators to safeguard critical digital finance infrastructure. This session will also include an exercise designed as an interactive tabletop session, where participants were organized into groups, each focusing on a distinct aspect of cyber security: Risk management, governance, testing, training & awareness, protection and incident response. **Speaker**: • Arnold Kibuuka, Project Officer, TSB, ITU
10:45 - 11:00	**Coffee Break**
11:00 – 13:00	**DFS cyber resilience toolkit tabletop exercise (Part 2)** This exercise is designed as an interactive tabletop session, where participants will be organized into groups, each focusing on a distinct aspect of cyber security: Risk management, governance, testing, training & awareness, protection and incident response. (Prerequisites for participants and details – see below) **Facilitators**: • Vijay Mauree, Programme Coordinator, TSB, ITU • Arnold Kibuuka, Project Officer, TSB, ITU
13:00 - 14:00	**Lunch**
14:00-15:00	**DFS cyber resilience toolkit tabletop exercise (Part 3)** **Facilitators**: • Vijay Mauree, Programme Coordinator, TSB, ITU • Arnold Kibuuka, Project Officer, TSB, ITU
15:00-15:15	**Coffee Break**
15:15-17:15	**BSA sandbox bootcamp** **Speakers:** • FNSV
17:15 – 17:30	**Closing of the Security Clinic** **Speakers:** • FNSV • Vijay Mauree, Project Officer, TSB, ITU

Digital Financial Services Security Cyber Resilience Toolkit Exercise Overview

The DFS Cyber Resilience Toolkit facilitates DFS cyber resilience self-assessment and improves the overall digital financial services infrastructure posture by identifying vulnerabilities, assessing peripheral and internal defences, and designating attack scenarios. The toolkit addresses DFS entities, users, and actors that may be part of the telecommunication sector of the DFS ecosystem.

The toolkit promotes a more structural preparation against malicious cyber operations, establishes best practices to fend off unauthorised access attempts, and suggests potential security measures that can be implemented to improve the cybersecurity maturity of the targeted entity.

This exercise is designed as an interactive tabletop session, where participants will be organized into groups, each member of a group will focus on a one of the following aspects of cyber resilience:

1. Risk Management
2. Governance
3. Testing
4. Training & Awareness
5. Protection
6. Incident Response

Group members respond to their assigned categories in the Excel sheet and the group results are collectively viewed in the 'Results Summary' sheet. This analysis will help rank and pinpoint critical focus areas, which also emerge from the sub-pillars, and specific aspects to be addressed can be identified from the responses to the questions.

Task Flow:

1. **Group Formation**: Participants will be divided into groups, each representing a Digital Financial Services (DFS) ecosystem player.
2. **Toolkit Distribution**: Teams are provided with the Excel toolkit which contains the questions and the various 'Pillars'. Each group can access the toolkit in their groups folder, members should answer the toolkit online to allow for collaboration: Access to toolkit here: xxx
3. **Pillar Assignment**: Each team member will be assigned to a specific Pillar to focus on.
4. **Individual Exercise**:

- Members then respond to questions in the toolkit by choosing the resilience level that best represents their “situation,” marking their answers in the adjacent column.

5. **Pillar Analysis**: Each team performs this analysis on their assigned Pillar sheet to identify Critical Sub pillars. The toolkit then auto-calculates the cyber resilience score, shown in the 'Results Summary' sheet.
6. **Vulnerability Assessment**: Post-completion, teams will examine their data to identify potential weaknesses. They will prioritize which pillars and sub-pillars are crucial in the roadmap to enhance cyber security.
7. **Insight Aggregation**: The findings from all teams will be combined to create an overall assessment of the country's cyber resilience level.

- An appointed participant from the group will share the group's Summary results for aggregation at: https://www.menti.com/al1sncnfxu8p

Outcome:

By merging the insights from all teams, we will obtain an overarching view of the cyber resilience stature. This consolidated data will be instrumental in identifying systemic vulnerabilities at a national level and in crafting tailored cyber resilience strategies moving forward.