Digital Financial Services Security Clinic

DFS Security Audit Guideline

Arnold Kibuuka
Project Officer, TSB, ITU

How can a regulator, DFS provider or MNO give assurance on the security of financial services?

Related report:
Digital Financial Services security audit guideline

Motivation

Are the controls in place working and effective?

Doc Link: [Digital Financial Services security audit guideline]

FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

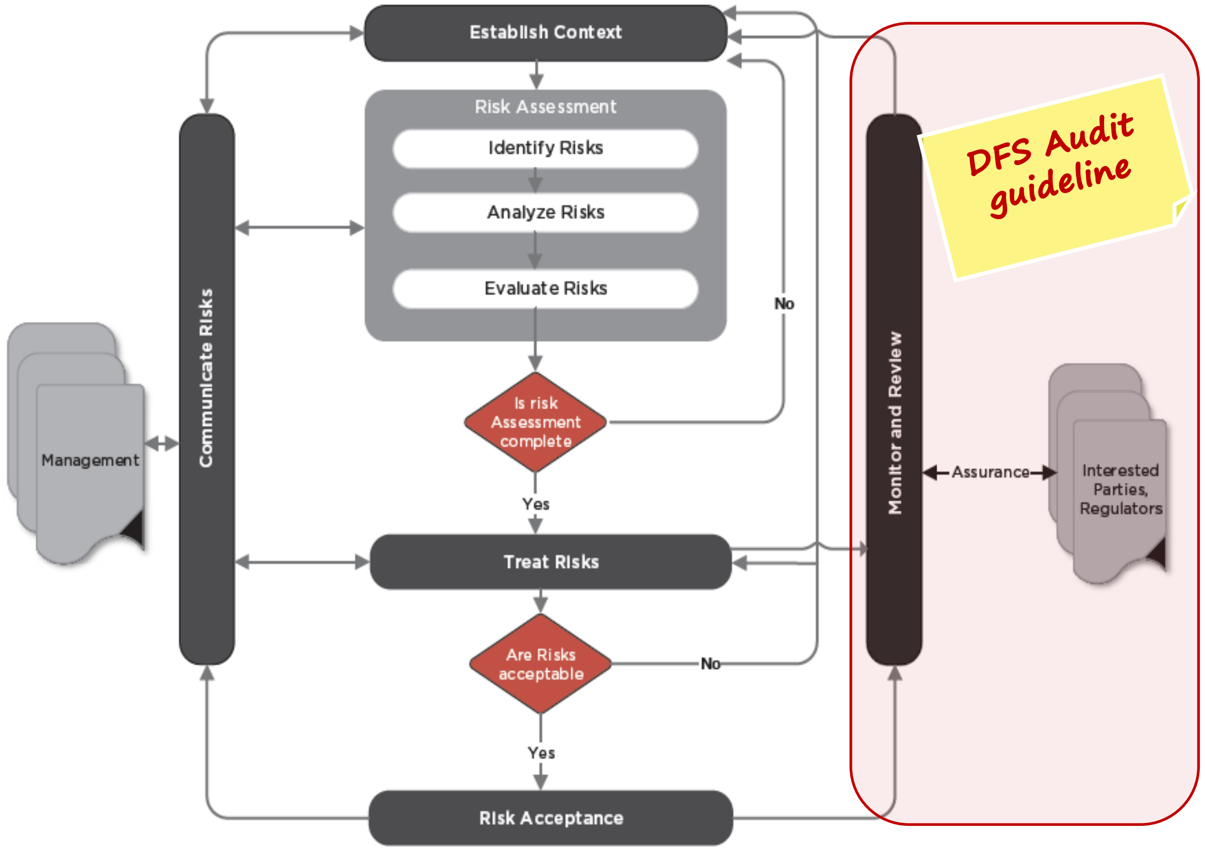
SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services
security audit guideline

REPORT OF SECURITY WORKSTREAM

ITU

DFS Audit guideline



- For each control, we have developed guidance for auditors to use in assessing whether the control is implemented and the policies, standards that need the provider needs to have in place.
- The purpose of the guideline is to assess whether basic controls are in place to give some assurance on the security of DFS services.
- From PDCA, monitor and review involves assessing and measuring security performance of DFS assets against security checklist.
- The DFS security audit guidelines are categorized into six different groups: *Access control, Authentication, Availability, Network security, Fraud detection , Privacy and confidentiality*

Introductory Concepts

ITU-T Rec. X.805

ITU-T Recommendation X.805 provides a foundation for the document, with eight *security dimensions* to address security:

1. *access control,*
2. *authentication,*
3. *non-repudiation,*
4. *data confidentiality,*
5. *communication security,*
6. *data integrity,*
7. *availability,*
8. *privacy*

Vulnerability

A weakness in a system that can be exploited by an adversary/hacker

Threat

the specific means by which a vulnerability is exploited

Risk

the consequences of a threat being successfully deployed

Control:
A *safeguard* or *countermeasure* prescribed to protect the **confidentiality**, **integrity**, and **availability** of information systems and assets to meet a set of defined security requirements.

Introductory Concepts

Policy

What and Why?: What is Management's intent for security?

Identifies the problem and an action that needs to be performed

Procedure

How do we implement a standard?

Outlines the steps to complete an action

Guideline

Provides recommendations and best practices

Security Audit

An evaluation of the security of a company's information system by measuring how well it conforms to an established set of criteria

Audit Guideline

The DFS security audit guidelines are categorized into six different groups

1. **Access control**

Audit guidelines in this group assess whether sufficient selective restrictions on appropriate access to DFS associated systems, services, resources, and controls are in place to guarantee protection against unauthorized use of network resource

2. **Authentication**

Audit guidelines in this group assess a DFS application's capability to verify the authenticity of the users.

3. **Availability**

Audit guidelines in this group assess the DFS infrastructure and application for reliability and ability to grant timely access to authorised DFS users. The application and infrastructure are validated for resistance to denial-of-service attack

Audit Guideline

4. Fraud detection

Audit guidelines in this group to assess the controls in place within the DFS systems to detect intentional and unlawful interception by internal or external entities to obtain customer personal data and steal customer funds from a DFS system.

5. Network security

Audit guidelines in this group assess the controls in place to protect the underlying network infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure. These can also be used to test whether information only flows between authorized endpoints without being diverted or intercepted.

6. Privacy and confidentiality

Audit guidelines in this group assess the controls in place to protect DFS participants/user's data from unauthorised disclosure, including data protection that might be derived from observing network activity

Questions

Contact: dfssecuritylab@itu.int

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