DFS Audit guideline

Arnold Kibuuka
Project Officer, TSB, ITU

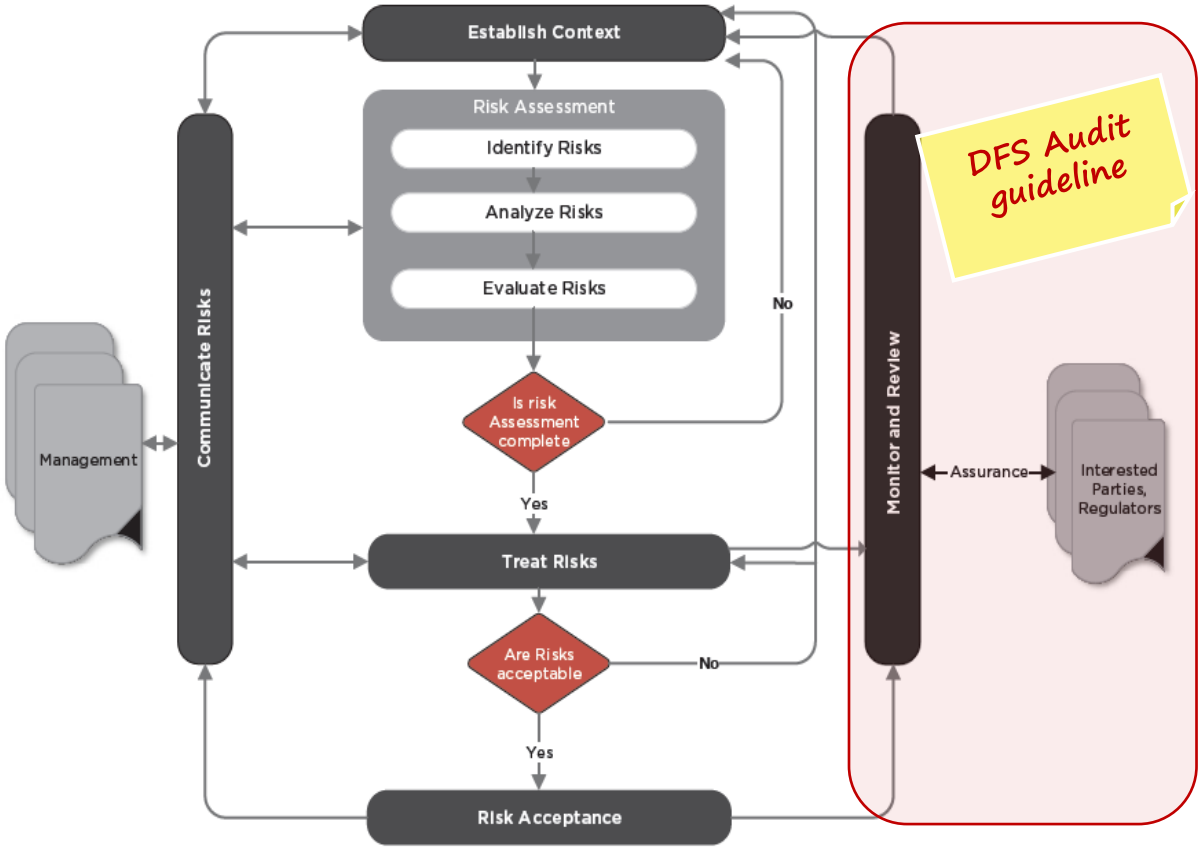
December 2021

Motivation

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

Doc Link: [Digital Financial Services security audit guideline]

Examples: DFS Audit guidelines



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:

Access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, privacy

.

Vulnerability

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

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

DFS Audit guideline - Examples

Network Security

C24: The DFS provider should protect against network attacks by use of firewalls and traffic filters and protect against DFS infrastructure threats by challenging suspicious traffic through network admission techniques and mechanisms such as CAPTCHAs.

Audit Validation: *Are there adequate protections against network attacks like firewalls and traffic filters with proper configurations?*

Policy/Procedure: Operations security: Protection from malware

C26: Set restrictive firewall rules by default, use ports whitelisting, use packet filters, and continuously monitor access to whitelisted/permitted ports and IP's.

Audit Validation: *Are the firewall rules adequately configured? (e.g., port whitelisting, packet filtering)*

Policy/Procedure: Operations security: Protection from malware

Example

Let's consider the threat: **malware.**

- How can the regulator check that DFS providers have some controls in place to avert this threat?
- How can the Telco operator ensure that infrastructure has controls in place to mitigate against these?

DFS Audit guideline

1. Identify the vulnerabilities that can be exploited by malware within the DFS entity.
   - Security assurance framework (see section 8.13)
2. Check whether the DFS provider has policies in place to protect against malware & how they should address vulnerabilities.
   - How do you know that is the right policy?

   The policy's "purpose" should describe requirements for preventing and addressing viruses, worms, spyware, malware, and other types of malicious software.
3. Identify controls that can mitigate the vulnerabilities
4. Assess implementation of the controls

Questions

Exercise

October 2021

Exercise

November 2021

Example:

Risks or vulnerability: Weak encryption algorithms used on data stored in the device and data transmitted.

Control: **C41**: Sufficiently secure encryption should be deployed for both data protection within the mobile application and communication with backend DFS systems and whenever possible, mask, truncate or redact customer confidential information.

Audit question: Have strong encryption ciphers and integrity protection mechanisms such as message authentication codes been used for data stored on the device and when data is communicated to backend DFS systems? Are policies in place to assure the protection of sensitive customer confidential information?

Additional checks for consideration:

What security policies/procedures are in place?

Exercise: Using the DFS security assurance Framework and audit guidelines

This exercise is to assist participants on how to use the DFS security assurance framework and audit guideline to assess compliance.

The participants will be divided into 4 groups, central Bank & telecom regulator, MNO and DFS provider to identify security risks vulnerabilities to:

- Consumer data privacy - Central bank group, DFS providers, PSP
- Communication security - Telecom regulator group, Telecom providers

Part 1: Identify controls that the DFS regulators need to implement in their countries to mitigate the vulnerabilities

Part 2: Identify the questions for the security audit that regulator would use to assess compliance of the DFS provider to the controls.

Documents links:

- Digital Financial Services Security Assurance Framework
- Digital Financial Services Security Audit guideline

Group 1: Telecom Regulator

Communication Security

Synopsis: Telecom regulators would be usually concerned whether network operators & DFS provider applications are providing secure communication for DFS transactions.

Question 1. Identify some of common risks & vulnerabilities to communication security in your country

Question 2. How would you audit the MNO to assess/evaluate compliance to the controls?

Group 2: Telecom Provider

Communication Security

Synopsis: Telecom regulators would be usually concerned whether network operators & DFS provider applications are providing secure communication for DFS transactions.

Question 1. Identify some of common risks & vulnerabilities to communication security in your country

Question 2. Identify at least 2 controls from "DFS security assurance Framework" that Mobile Network Operators in your country should adopt to assure communication security.

Group 3: Central Bank

Protection of consumer data

Synopsis: Central Banks are generally concerned with whether DFS providers are adequately protecting consumer's financial data.

Question 1 . Identify common risks & vulnerabilities to DFS consumer data in your country (1 or 2

Question 2. How would you assess/audit/evaluate the DFS provider to compliance to the above controls?

Group 4: DFS provider

Protection of consumer data

Synopsis: Central Banks are generally concerned with whether DFS providers are adequately protecting consumer's financial data.

Question 1 . Identify common risks & vulnerabilities to DFS consumer data in your country (1 or 2

Question 2 . Identify at least 2 controls from DFS security assurance that DFS providers in your country should adopt to protect digital financial services data.

Thank you!