Exercise

Implementing the DFS security assurance Framework and audit guidelines

April 2022

Implementing the DFS security assurance framework and audit guidelines

This is a practice exercise on using the DFS security assurance framework and audit guideline to assess compliance.

Participants will be divided into four groups, looking at the security aspects below:

Part 1: Identify threats/vulnerabilities to DFS on/due to:

- *communication security* – ***Group 1***
- *consumer data privacy* – ***Group 2***

Part 2: Identify controls that need to implemented to mitigate the threats and vulnerabilities.

Part 3: Identify audit/assessment questions for the security audit checklist you would use to assess compliance to the controls.

Documents links: Digital Financial Services Security Assurance Framework & Digital Financial Services Security Audit guideline

Group 1: Communication Security

Synopsis: A Mobile Network Operator is concerned with providing secure communication for DFS transactions.

1. **Use the "DFS security assurance Framework" to identify:**
   a) risks & vulnerabilities to secure communications (atleast 3)
   b) Three controls that network providers and DFS providers should implement to mitigate vulnerabilities in (a) above

2. **Use the "DFS audit guideline" to:**
   a) to identify security policies/procedures that need to be in place to address risks above.
   b) Identify three questions to assess protection of communication infrastructure?

An example is provided on slide 4, to use as reference for this exercise.

Example: Group 1: Communication Security

Risks or vulnerability:

Unprotected sensitive traffic and weak encryption practices

Control:

C75: Control and monitor the use of MSC MAP tracing and protocol analysers on USSD, SMS infrastructure to internal limit access to plain text SMS and USSD traffic in transit.

Security policy:

A network security policy must be in place

Audit question:

Does the MNO operator have controls in place to limit access to MAP tracing and use of protocol analyzers on the internal network? (SMS and USSD messages are transmitted in plain text in the MAP protocol)?

Group 2: Protection of consumer data

Synopsis: A DFS provider is concerned with protecting consumer's financial data.

1. Use the "DFS security assurance Framework" to identify:
   a) 3 common threats & vulnerabilities to DFS consumer data.
   b) Three controls to mitigate threats in 1(a) above.

2. Use the "DFS audit guideline" to:
   a) identify security policies/procedures that need to be in place to protect consumer data.
   b) Identify three questions for a security checklist to identify gaps in protection of DFS consumer data?

An example is provided on slide 6, to use as reference for this exercise.

Example Group 2: Protection of consumer data

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.

Security policy:

Data protection policy

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?