**Business process**

This document contains the process of referring this toolkit documents. In each step users must read the instructions and refer mentioned document from the toolkit to implement the document.

1. Refer the PCI DSS requirements checklist (Requirement’s checklist document)
2. Create the asset inventory regarding all information assets and related of the organization (Asset inventory document)
3. Define PCI DSS implementation scope and identify the environment (Context establishment document)
4. Refer risk assessment guidelines document and perform a risk analysis of the organization’s assets.

In risk analysis refer

Asset profile

Threat profile

Risk treatment documents to perform the risk analysis

1. Perform a gap analysis by referring the Gap analysis document.
2. Develop an information security policy in order to secure the PCI DSS implementation environment. (Information security policy layout document) refer the content topics provided in order to develop the information security policy.
3. Internal VAPT should be carried out in order to identify regular vulnerabilities and abnormal behaviors of the systems.
4. Monitor and store logs related to incidents and events related to card holder data after implementation and maintain monitoring continuously. (Incident monitoring and logging document)