Risk assessment guideline for PCI DSS

Performing an annual risk assessment is mandatory according to the PCI DSS requirement 12.0. Therefore, a risk assessment needed to be performed to analyze the possible threats for the critical assets regarding PCI DSS. Networks, Devices, Servers etc.

ISO 27005, OCTAVE or NIST SP 800-30 can be used to perform the risk assessment. In this toolkit the documents provided for the risk analysis are mainly based on OCTAVE allegro worksheets.

The required documents for the risk assessment are provided with the toolkit.

**Risk Assessment steps**

1. Create the Asset registry and Asset inventory

(Refer asset registry and asset inventory document)

1. Create the asset profiles

(Refer asset profile document)

1. Identify each threat for the assets and create threat profiles for each threat

(Refer Threat profile document)

Define a Risk tolerance (appetite) level. (Risk tolerance/appetite value is the value of the minimum risk score that the organization can tolerate)

1. In threat profiles document, template for an analysis for risk scores are provided. Calculate the relative risk scores.
2. Evaluate the identified risks and prioritize risks.

There are two methods that the risk evaluation needs to be performed.

* Qualitative
* Quantitative

1. Identify threats that are above risk tolerance level and suggest mitigations according to the threat countermeasures section in threat profiles and countermeasure document.
2. Risk assessment is a cyclical process. Therefore, for the mitigated threats, it is recommended to perform the risk analysis again and calculate new relative risk score values.
3. If the new values are still above the risk tolerance level, introduce and add new mitigations.
4. Repeat the process annually or quarterly.