Skillmine
Technology • Consulting • Services

PCI - DSS

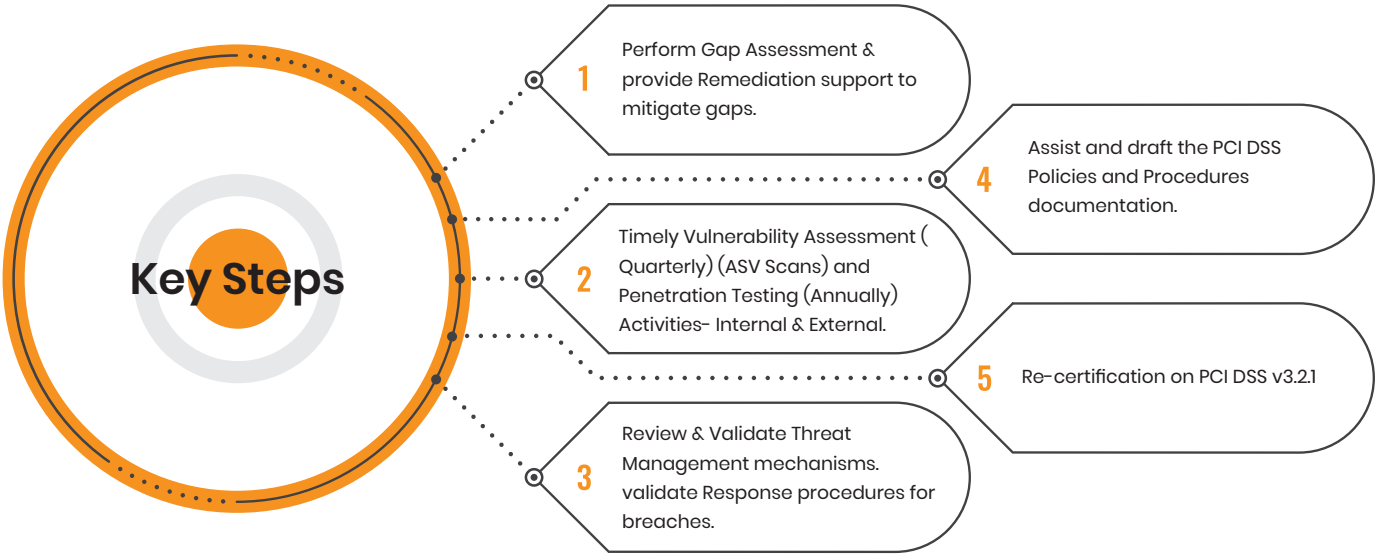
Approach Paper

Exec Summary & Key Steps

The Payment Card Industry Data Security Standard (PCI DSS) is a well-defined structure providing 12 Control Sets for securing cardholder data that is stored, processed and/ or transmitted by banks, organizations and merchants.

We follow the Industry defined Best Practices and create, maintain, measure and continuously improve the below prioritized key security milestones:

1. Secure payment card applications, processes and underlying systems & networks.
2. Protect Card Holder Data, remove sensitive data storage and limit data retention.
3. Control Access & Monitor.
4. Ability to respond to Breach.
5. Continuously Improve Policies & Processes.



Phased Approach

Assessment Phase

Project Kick Off

The project starts with a formal introduction with the delivery team and people involved.
The meeting also helps to set and lay down the expectations for each milestones' dates and parameters.

PCI DSS Scoping

The objective of this step is to identify all the applications, system components and departments having access to cardholder information in-order to scope them for PCI DSS certification.

Network Segmentation

This phase helps to reduce the PCI DSS scope which in result helps in reduced effort to implement the PCI DSS requirements.
This phase also enhances the network security of an organization.

PCI DSS Gap Assessment

Conducting a Gap Assessment helps to identify all possible threats, exposure point, gaps, loops in respect to PCI DSS requirements. A gap assessment report to be presented with the findings after conducting gap analysis.

Remediation and Certification Phase

Remediation

On completion of Gap Assessment Phase, work with the client to mitigate and remediate all gaps that were identified in the Gap Assessment.

Additional Services

PCI DSS certification requires few additional activities such as Vulnerability Assessment and Penetration Testing. This Phase covers all the requirements.

Pre audit & Final Certification

The phase covers the final review of the require-ments for PCI DSS which is followed by the Final Audit and it's deliverables. ROC, AOC & COC

Assessment Phase

PCI DSS Scoping

- The cardholder data environment is comprised of people, processes and technology that handle cardholder data or sensitive authentication data.
- The PCI DSS applies to all system components included in or connected to the cardholder data environment.
- The PCI DSS also applies to all systems involved in managing the security of other in-scope systems (i.e. authentication servers, log management servers, IDS management consoles, etc.).
- Improper scoping may result in not identifying cardholder data (CHD) or intended/accidental cardholder data leakage.

CHD contains

Primary Account Number, Card Holder Name, PIN, Service Code, Expiry Date, CVV, Magnetic Strip Data – Track1 & 2
Document, where is the Data

Data storage locations.

Entry and Exit points to the application.

Processes That process cardholder data.

Networks Over which cardholder data is transmitted.

Data Flow related for Payments, Interfaces, Merchants.

Understand data residing in

1. Cardholder database
2. Transaction logfiles
3. Auditdumps and audit-trails
4. Backup media
5. Application trace files

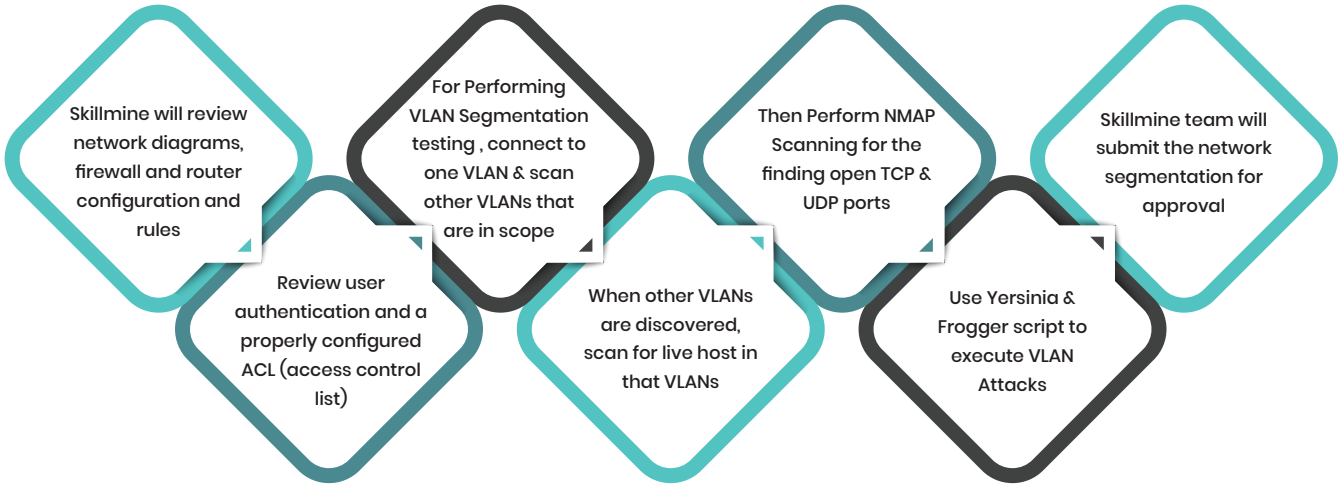
Deliverables for PCI DSS Scoping

- List of processes in PCI-DSS scope
- List of processes out of PCI-DSS scope with business justification
- Dataflow diagram for each process.
- List of assets in the scope: This includes people, processes, systems, applications, databases, security solutions etc.
- List of locations where card holder data is stored

Network Segmentation

Segmentation can be achieved in several ways. The aim will be to minimize the scope of overall project by understanding Network segment to derive CDE where CHD is stored

Our Approach



Deliverables for Network Segmentation

Network segmentation.

PCI DSS Gap Assessment

Gap analysis is conducted to assess the compliance level of the PCI-DSS scoped environment. During gap assessment, various teams will be interviewed to understand business processes, systems and technical controls analysis will be conducted. Detailed report highlighting non-compliant requirements along with recommendation will be submitted to the client.

Our Approach

01 Skillmine's team will involve the core PCI team from Client and conduct the gap assessment.

02 Skillmine will dedicate a senior PCI DSS advisor to Client. He will conduct the gap assessment phase and will act as a project manager and assure that the activities are conducted as per the agreed timelines.

03 Evidence will be collected and a gap assessment report called Action Tracker will be submitted to Client.

04 The deliverables for gap assessment will be a detailed gap assessment report and agreed Action Tracker, which will list down all the action points pertaining to the gaps as per the latest version of PCI DSS, action points which need to be taken for remediation.

05 Skillmine and Client to have multiple online meetings to discuss the gaps and understand the business justification for them and discuss solutions to mitigate the gaps. Once a mutually agreed plan has been approved, Skillmine will start the remediation phase and help client to mitigate the identified gaps.

Deliverables for PCI DSS Gap Assessment

- Gap Assessment Audit
- Gap Assessment Report – Action Tracker
- Presentations on the findings
- Mutually agreed plan to mitigate the plans

Remediation & Certification Phase

Remediation

- This phase helps to provide unlimited assistance to the client for achieving PCI DSS re-certification.
- Skillmine is focused on building a robust framework that contains security, policies, testing mechanisms and procedures to ensure true security.
- The non-compliant areas identified during Gap Analysis phase with possible solutions and timelines would be followed up for progress in the remediation and supported by Skillmine.
- Skillmine will evaluate the risk of sensitive data and protect data by providing technical expertise in identifying and evaluating product vendors for technology solutions like (but not limited to) encryption, file integrity monitoring which would be required for adhering to PCI DSS Requirements.
- Skillmine will monitor and support the progress of findings based on the gaps identified as a part of the management of remediation activities.
- Skillmine's PCI team will conduct weekly online meetings and understand the progress during the remediation phase and provide unlimited support for mitigating the gaps.
- Skillmine's advisory team will work parallelly on activities such as policy and procedures to store and process card holder data.
- The PCI DSS applies to all system components included in or connected to the cardholder data environment.
- The PCI DSS also applies to all systems involved in managing the security of other in-scope systems (i.e. authentication servers, log management servers, IDS management consoles, etc.).
- Improper scoping may result in not identifying cardholder data (CHD) or intended/accidental cardholder data leakage.

Deliverables

- Dedicated one QSA, 2 consultants and PMO team to mitigate gaps. QSA can be independently appointed by Client as per preference.
- Mutually agreed processes and procedures for mitigating gaps.
- Report on progress of mitigating gaps.

Pre-Audit & Final Certification

This is the final phase of the PCI-DSS Project. This phase is only commenced after consistent interactions with client. The final certification phase is initiated upon mutual consent of Skillmine and client. The Review and Certification involves another assessment of the organization's infrastructure, process and policies as per the requirements of the PCI-DSS. Once the organization is found to be compliant with all 12 requirements of the standard, the organization is declared as a PCI DSS Certified Organization.

Approach

Skillmine would review the existing security policies and procedures in place with Client Team.

The consultant from Skillmine would provide a detailed feedback on the current policies & procedures based on the review.

The consultant would be communicating dedicatedly with the Client team to make the necessary revisions in the documentation (if required)

Deliverables for Certification

- Report on Compliance (ROC)
- Attestation of Compliance (AOC)
- Certificate of Compliance (COC)
- Digitally signed compliance seal for websites: Skillmine provides digitally signed logo for client's web sites

Maintenance

Skillmine is committed to work with Client as their cyber security partner. Maintaining PCI DSS compliance can be difficult throughout the year. Constant maintenance and continued vigilance is required to promote best practices across the organization and to prevent a security breach or data compromise. Compliance is an ongoing process and monitoring of systems should be proactive. Skillmine's focus is on building a culture of security while helping to protect Client's assets and IT infrastructure.