**Project Managing a PCI DSS Implementation**

The Payment Card Industry Data Security Standard (PCI DSS) is developed by the PCI Security Standards Council, and aims to promote the security of cardholder data. It has been developed as a result of joint collaboration of four credit card organizations that include Mastercard, VISA, American Express and JCB. The standard presents a set of twelve requirements, the compliance of which ensures security of cardholder data and prevention of potential data breaches.

|  |  |
| --- | --- |
| **Goals** | **Requirements** |
| Build and Maintain a Secure Network. | 1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security perimeters. |
| Protect Cardholder Data | 1. Protect stored cardholder data. 2. Encrypt transmission of cardholder data across open public networks. |
| Maintain a Vulnerability Management Program | 1. Use and regularly update anti-virus software or programs. 2. Develop and maintain secure systems and applications. |
| Implement Strong Access Control Measures | 1. Restrict access to cardholder data by business need to know. 2. Assign a unique ID to each person with computer access. 3. Restrict physical access to cardholder data. |
| Regularly Monitor and Test Networks | 1. Track and monitor all access to network resources and cardholder data. 2. Regularly test security systems and processes. |
| Maintain an Information Security Policy | 1. Maintain a policy that addresses information security for all personnel. |

**The Project Management Approach to PCI DSS Compliance**

The implementation of PCI Data Security Standard can be seen by organizations as an ongoing project that requires regular monitoring and updating after first time completion. Initially, a Gap analysis is conducted to find out the deficiencies of an organization in terms of its cardholder data security and helps to understand the current standing of the organization by measuring the gap between the current situation and the required standard. After the Gap Analysis, the remediation phase attempts to fill in the gaps by taking measures to achieve the compliance requirements. An assessment of the controls is then performed either by qualified internal personnel or by Qualified Security Assessors (QSA). The assessment phase is then followed by the sustenance phase of controls to ensure that the security measures are consistent and continuous for the cardholder data. The validation phase then ensures with evidence that the controls are well sustained.

**Benefits of the Project Management Approach:**

1. **Increased Reliability of the PCI DSS Compliance**

With the help of already developed methodologies of project management, an organization is better able to perform the annual validation. The project management approach helps to clearly define the scope and objectives in the start, while its tools such as project charter help to build up timelines and milestones. Work is broken down in an organized manner through the Work Breakdown Structure WBS. Risks are identified and reported for mitigation. The earned value analysis helps to monitor planned activities against actual activities. Hence, all these tools and methodologies help to build up a systematic approach towards PCI DSS Compliance.

1. **Risk Reduction**

Risk management is one of the areas of Knowledge Management of project management. Risks are constantly there in the payment card industry and with the help of proper management of triple constraint of Time, Scope and Cost, a project manager can help to identify risks on time. Thus the validation of PCI compliance becomes easier when risk is identified early and mitigation measures are implemented soon enough to minimize the effects of associated risks.

1. **Correct Allocation of Resources**

Without a project management approach, key resources involved in PCI compliance validation are performing other key activities within the organization also, that are important for running day to day business. The project management approach makes optimal use of resources by applying techniques such as critical path analysis, activity sequencing, resource leveling and float calculation. This helps to avoid over allocation of the resources and saves time and money of the organization.

1. **Accountability**

The project management tools such as Project Dashboard, RACI, etc, help executives find out who is responsible and accountable for a certain event of mishap or breach of information.

**Managing a PCI DSS Compliance Implementation Project**

Just like any other project that is carried out under the project management approach, a PCI DSS compliance project can also be implemented in the following steps explained below.

1. **Initiate the Project**

Start the project by defining the objectives and the scope of the project. The objectives definition includes the compliance to all the twelve requirements of the PCI DSS, while the scope definition identifies the applicable areas of compliance and the deliverables of the project. A time frame also needs to be set to identify the different phases and completion date of the project. When the project scope, objectives, and time are developed, set them up on a project charter. The project charter should also include risks, assumptions, constraints and deliverables.

1. **Establish the Scope of Cardholder Data Environment**

Determining the scope of CDE is one of the difficult phases as it must cover everything that is directly or indirectly involved in storing, processing and transmitting cardholder data. This includes the processes, people and technology handling the data. A project manager is not the right person to conclude the scope of CDE and it must be done by a Qualified Security Assessor(QSA) or an Internal Security Assessor (ISA).

1. **Develop a Plan of Project Validation**

The project validation plan will provide details on when, how, where and what is being validated for the compliance achievement. The validation plan should also include assessment methodologies such as tests and interviews, incident handling protocol, assessment data transmission through trusted and untrusted medium, testing authorization, data and tools removal after validation.

1. **Assess the Implemented Actions**

Here the QSA will fully assess and inspect the controls to validate them against PCI DSS requirements. In order to be fully compliant, prove must be given regarding the ongoing compliance throughout the year, rather than only at the time of the audit.

1. **Analyze**

This phase aims to ensure that all findings of the assessment are correct and the testing was performed in an appropriate way. Sometimes an assessor might make the mistake of wrongly interpreting the results or might give the wrong evidence. The QSA therefore reviews the test results and also rechecks the control states and scope statements to make sure that they are according to what they actually observed.

1. **Remediate**

Based upon the gaps identified in the gap analysis, this phase should implement the following remedial action plans:

* Develop a risk treatment plan
* Develop a prioritized action plan
* Perform a risk review with the bank
* Carry out the remediation actions
* Assess the remediation plan
* Present the results to the acquiring bank and the top management.

1. **Report**

At this phase, the process of PCI validation is complete and now needs to be documented. Before submitting complete documentation to the acquiring bank, the following reports must be prepared:

* Take the inventory of the Book of Evidence from the assessor as it might be required by the acquiring bank.
* Submit an Attestation of Compliance (AOC), Self Assessment Questionnaire (SAQ), and the Report on Compliance (RoC) to the Acquiring bank.
* Submit the final assessment documents to management for approval.
* Submit the approved set of documents to the acquiring bank.