**How to Report on your PCI DSS Compliance**

The Payment Card Industry – Data Security Standard (PCI DSS) is a set of requirements for merchants and financial institutions, which helps them keep their cardholder data safe and secure. Once all requirements to achieve PCI DSS compliance have been met, an organization needs to deliver a Report on Compliance (RoC). The RoC is prepared at the time of the assessment of PCI compliance and comprehensively provides details about the assessment approach and compliance standing against each PCI DSS requirement. The PCI Security Standards Council (SSC) has provided a template for a Report on Compliance in its PCI DSS Requirements and Security Assessment Procedures.

**What is a Report on Compliance**

A Report on Compliance or ROC is basically a form that needs to be filled by Level 1 Visa merchants who are in the process of undergoing PCI DSS audit. Level 1 merchants are those merchants who carry out more than six million Visa transactions in one business year.

**Purpose of Report on Compliance**

The purpose of RoC is the verification of the merchant in terms of its compliance with the PCI Data Security Standard. This standard, which was formed with the collaboration of Master Card, Visa, American Express and Discover, has laid down some requirements based upon a set of policies and procedures to protect cardholder data from any potential fraud or information misuse.

The PCI DSS Report on Compliance is mostly prepared by a Quality Security Assessor who performs the compliance audit. The QSA then must verify and prove the methodology of performing the validation as well as the measuring of every entity against each requirement of the standard. This RoC is then submitted to the bank of the merchant so that it can be accepted. The bank, after accepting the RoC, further forwards it to Visa to verify for compliance.

**Contents of your PCI DSS Compliance Report**

According to the PCI DSS Requirements and Security Assessment Procedures document, RoC should consist of the following main contents.

**Section 1: Executive Summary**

In executive summary an assessor has to describe the exact role of the merchant in the payment card industry to describe:

* why it stores, processes and transmits cardholder data
* how payments are processed
* what payment mediums does it use for transmitting the data
* any other businesses that they are connected to, regarding the processing and transmission of data

The executive summary must also include a comprehensive network topological diagram to explain:

* All connections going in and out of the network
* Important devices including point-of-sale devices, web servers, databases, etc.

**Section 2: Description of Scope of Work and Approach Taken**

In this section the assessor has to validate the accuracy of the scope and include the following details:

* All the processes involved in the identification and documentation of cardholder data
* Evaluation and documentation of results
* Proof of verification of the effectiveness of the methods adopted for assessing
* Validation of accuracy and appropriateness of the scope of assessment
* The main focus area of the assessment
* Explanation of the network segmentation process , if used for reducing scope

In case if sampling is used by the assessor, the following details of the sample set must be included:

* Total population
* Sampling size
* Sampling methodology

The assessor must also include any entity involved in storing, processing or transmitting cardholder data that was excluded from the scope of work and the reason why it was excluded.

**Section 3: Details about Reviewed Environment**

Following important details must be documented in the section:

* All communication link diagrams, such as LAN and WAN
* Complete description of cardholder data environment or CDE
* List of tables and files that store cardholder data
* Methods adopted for securing the data
* List of all software and hardware used in the CDE and a description of their functionality
* List of third party payment applications
* List of interviewed individuals, along with their details
* List of all reviewed documentation

**Section 4: Contact Information and Report Date**

This section should contain the following important details:

* Contact details of merchant and the assessor
* The time period or the duration of the assessment
* The date of report

**Section 5: Quarterly Scan Results**

Here, the assessor needs to summarize the four recent ASV scan results. However, in case of a few exceptions, the assessor may not be required to complete these scans if they verify that:

* The recent scan was a passing one
* All policies and procedures of the organization have regulated a quarterly scan within the organization
* Vulnerabilities detected in the last scan have been fixed
* Four passing scans on a quarterly basis were conducted after initial PCI DSS review

The scan must include all IP addresses that are accessible externally.

**Section 6: Findings and Observations**

In this important section the assessor needs to:

* use the PCI DSS Requirements and Security Assessment Procedure template to document the findings on each requirement and sub-requirement
* make sure that all “not applicable” areas are well explained
* review and document all compensating controls, if used

**Compensating Controls Worksheets (if applicable)**

In this section, the assessor needs to attach compensating controls worksheets in an appendix. He has to give each compensating control a uniquely identifying appendix number. (For example, if Compensating Controls Worksheets are in Appendix A of the ROC, uniquely identify each worksheet as A-1, A-2, etc.) The compensating controls worksheets should follow the template given in appendix C of the PCI DSS Requirements and Security Assessment Procedures.

To summarize it all, in sections 1 to 5, the assessor has to assess the environment by first determining the scope of compliance and what approach is taken to achieve compliance against every requirement. The details of the environment reviewed are then provided by the assessor. The section 6, which includes the Findings and Observations, pertains to all requirements of the PCI DSS as well as additional requirements for Shared Hosting Providers. These findings need to be in consistence with the section 1-5 of the report. In the end, a complete worksheet for all the compensating controls for each requirement should be provided, the template of which can be obtained from appendices B and C of the PCI DSS.

A comprehensive and reliable report on compliance can only be achieved with the work papers generated by the assessor if he exercises detailed tests and assessments. These work papers are produced at every stage of assessment such as observations, configuration data, system testing, interview notes, references, etc. It would not be wrong to say that the RoC is actually a summary of all the work papers produced during each assessment activity.