**PCI Quick Reference Guide: Discover How the PCI DSS Applies To Your Environment**

The Payment Card Industry Data Security Standard (PCI DSS) is based on a number of requirements that are necessary to be fulfilled by all organizations that store, transmit or process cardholder data. These requirements aim to keep cardholder data secure during the process of storing, transmitting and processing cardholder data and provide a consistent framework for keeping data secure at global level. Breach of information has been a common problem for many years and poses serious threat to organizations and card owners. PCI DSS is thus, applicable to merchants, service providers, issuers, processors and all other third parties as well.

**Levels of PCI Compliance**

Merchants are divided into four categories based upon their annual transaction volume, as defined by Visa. Transaction volume includes all debit, credit and prepaid transactions carried out by a merchant. These levels can be best explained through the chart below:

|  |  |
| --- | --- |
| **Merchant Level** | **Criteria** |
| 1 | * Any merchant that processes more than 6 million transactions per year, regardless of acceptance channel. * Any merchant that experienced a security breach that resulted in data compromise. |
| 2 | * Any merchant that processes 1 to 6 million transactions per annum. |
| 3 | * Any merchant that processes 20,000 to 1 million transactions per annum. |
| 4 | * All those merchants that do not fall under level 1, 2, or 3, regardless of their acceptance channel. |

According to MasterCard, any Third Party Processor (TPP) is considered as Level 1 Service Provider while Data Storage Entities (DSEs) are considered as Level 1 or 2 Service Providers, depending upon their annual volume of MasterCard transactions.

|  |  |
| --- | --- |
| **Service Provider Level** | **Criteria** |
| 1 | * All Third Party Processors * All Data Storage Entities with more than 300,000 total combined annual transactions of MasterCard and Maestro |
| 2 | * All DSEs with 300,000 or less total combined annual MasterCard and Maestro transactions. |

**Validation of Compliance at Each Level**

Every merchant and service provider must fulfill at least two validation requirements to authenticate their compliance with PCI DSS. Validation requirements for each level can be best understood as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Merchant Level** | **On-Site Security Audit** | **Network Scan** | **Self-Assessment Questionnaire** | **3rd Party Payment Application Validation** |
| 1 | Required Annually | Required Quarterly |  | Required |
| 2 | Required Annually | Required Quarterly |  | Required |
| 3 |  | Required Quarterly | Required Annually | Required |
| 4 |  | Required Quarterly | Required Annually | Required |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service Provider Level** | **On-Site Security Audit** | **Network Scan** | **Self-Assessment Questionnaire** | **3rd Party Payment Application Validation** |
| 1 | Required Annually | Required Quarterly |  | Required |
| 2 | Required Annually | Required Quarterly |  | Required |

**Security Controls and Requirements of PCI DSS**

The aim to develop PCI DSS was to enforce secure controls for cardholder data and to reinforce consistent and worldwide adoption of these security controls. An overview of its security controls, along with the 12 requirements, is given below in brief:

|  |  |
| --- | --- |
| **Security Control** | **Requirement** |
| **Build and Maintain a Secure Network and Systems** | 1. Install and maintain a firewall configuration to protect cardholder data 2. 2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | 1. Protect stored cardholder data 2. Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | 1. Protect all systems against malware 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. Identify and authenticate access to system components 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 |

**Achieving PCI DSS Compliance**

As already mentioned, it is mandatory all merchants, service providers and third parties that are involved in storing, processing or transmitting cardholder data to comply with PCI DSS. Without compliance, these organizations cannot carry out their credit or debit card activities. Although the PCI Security Standards Council manages the PCI DSS, every card brand has its own strategy to enforce compliance to its clients. Requirements for validation of compliance vary for each card brand, but in general, the level of the organization determines what path it is supposed to take to achieve PCI DSS Compliance.

Usually the following steps must be taken by an organization in order to achieve PCI compliance:

1. Determine the scope of PCI DSS in relevance to the organization.
2. Test compliance to the standard on a sample of system components.
3. Get compensating controls validated by QSA in case the organization cannot meet a particular requirement due to a documented or technical business constraint.
4. Submit report on compliance.
5. Clarify any ambiguities in the report if requested by the bank.

**PCI DSS Requirements Scope**

Achieving PCI DSS compliance can be a daunting process, and much more than that if proper scoping is not done before starting to complete the requirements. It is very important for organizations to understand and minimize the scope of PCI in order to make the process as easy as possible. Cardholder Data Environment (CDE) forms the scope of PCI DSS and consists of processes, people and technology used for storing, processing and transmitting cardholder data. Similarly, all system components are also included in the scope and consist of servers, network devices, computer systems, applications, and any other components that are connected to cardholder data.

Once scope is defined, it must be checked for accuracy to ensure that all flows and locations of cardholder data are included in the scope. The following steps should be carried out:

* + Identify and document the flows in CDE and verify that no data exists outside the currently defined CDE
  + Any data not currently defined as a part of scope should be either be deleted, safely migrated elsewhere or included in the scope
  + Keep all documentation showing how scope was determined to hand it over to assessor for scope verification

**Choosing a Qualified Security Assessor for your PCI DSS Compliance**

Once an organization has taken all measures to implement PCI DSS to its system, it needs to hire the services of a Qualified Security Assessor to conduct on-site compliance verification and security assessment. QSA firms are trained and also certified by the PCI SSC.

The QSA serves to verify a merchant’s compliance to PCI DSS by filling out a Report on Compliance (ROC), which is then sent to acquiring bank of the merchant. The bank sends it to relevant credit card company to verify compliance.

Always select a QSA that has past experience of working with similar organizations and understands your business well. Also, maintaining goodwill and long term relationship with your QSA is important to help you with ongoing vulnerability assessments and remediation measures.

**Who Are We?**

Stickman Consulting has been certified by PCI Security Standards Council as a Qualified Security Assessor for PCI DSS. This has been possible with the help of a hardworking and experienced team after thorough inspection and scrutiny of PCI SSC. We carry out certifications and assessments for merchants, service providers, acquirers and issuers in Asia Pacific, Africa and Middle East.

**How can we help you?**

As a Qualified Security Assessor company, we can help you in:

* Verifying the technical information provided by merchant
* Providing support in achieving compliance
* Carrying out independent assessment to confirm compliance
* Defining assessment scope
* Ensuring observance of PCI Security Assessment Procedures.
* Providing onsite validation of compliance
* Evaluating compensating controls
* Producing final report

At Stickman Consulting, we ensure to equip our clients with the necessary knowledge, tools and processes that are needed to develop a secure network. Our specialist team of consultants have years of experience in providing services to banks, government, service providers and retailers.