**How to Comply to Requirement 12 of PCI DSS**

**Requirement 12: Maintain a policy that addresses information security for all personnel.**

A well developed, comprehensive information security policy serves as a basis for PCI compliance of an organization. However, many organizations make the mistake of making a one-time security policy and move on. For the policy to be effective, it is important that it is effectively communicated to all the personnel, whether full time, part time or temporary. Moreover, management of the information security policy is also very important and the policy needs to be reviewed and updated regularly to properly align with the changing business environment and the changes in the organization.

The requirement 12 of the PCI DSS has further been broken down into ten sub-requirements and compliance to each of them is explained in detail.

**12.1 Establish, publish, maintain, and disseminate a security policy.**

Any information security policy must be in accordance with the PCI DSS compliance but at the same time it is important to develop a comprehensive policy that addresses other regulatory compliance and organizational requirements. Organizations that have an information security policy only specific to PCI compliance will find it hard to maintain multiple policies and might risk themselves in having policies that malign with business processes, thus incurring additional cost.

The information security policy should be examined for being a comprehensive policy that covers all other organization level issues and it should be ensured that the policy is updated at least once a year or in case of any changes to the business processes.

**12.2 Implement a risk-assessment process that:**

* **Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),**
* **Identifies critical assets, threats, and vulnerabilities, and**
* **Results in a formal risk assessment.**

Risk assessment process is important to identify any potential threats and vulnerabilities that could eventually harm your business. Organizations should monitor their environment continuously, develop a risk assessment process, and implement controls that address those threats and vulnerabilities discovered in the process. Since technology is advancing at a very rapid rate, new threats and vulnerabilities keep on emerging quickly and performing risk assessments at least annually helps to successfully complete the risk assessment in a timely manner.

**12.3 Develop usage policies for critical technologies and define proper use of these technologies.**

Formal policies must be documented for the usage of critical devices and technologies. These policies should either prohibit personnel from using these technologies, unless advised otherwise, or guide them about how to use them correctly. In the absence of such policies, personnel may use them incorrectly, thus giving a chance to malicious criminals to gain access to your cardholder data.

To achieve compliance, the following verifications must be done:

* There should be a process that explicitly approves user to access a system.
* Access to these devices and technologies must be done with a username and password or any other identification method.
* There should be a list of personnel who are authorized to access the devices and technologies.
* The usage policies must define a method to label the owner of the devices to prevent malicious users from accessing the technologies with their own devices.
* The policies must define the acceptable uses, network locations and a list of approved products for the technology. This ensures that a “back door” is not open for a malicious individual to enter and gain access to the systems.
* The usage policies should mention a mechanism to automatically disconnect a session that has remained inactive for a certain period of time.
* They must allow vendors and business partners remote access only when it is needed and the access should be discontinued immediately after usage.
* The policies must prohibit a user from storing, copying and moving cardholder to their personal portable devices.

**12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.**

The real strength of an information security policy lies in its ability to clearly define the roles and responsibilities of the personnel and to communicate the requirements of the policy effectively so that all personnel understand and follow it accordingly. If roles and responsibilities are not defined accurately, it becomes very difficult to hold any employee or contractor accountable in case of breach of security.

A sample of personnel should be interviewed to test and verify that they understand their roles and responsibilities.

**12.5 Assign to an individual or team the following information security management responsibilities:**

Every individual or team of individuals must be well aware of their responsibilities regarding information security management with the guidance of a proper policy. The following responsibilities must be verified for every individual or team in order to achieve compliance:

* Responsibility of assignment of establishment, documentation and distribution of security policies and procedures.
* Responsibility of monitoring and analysis of security policies and distribution of information to the concerned personnel.
* Responsibility of assignment of incident response and escalation procedures.
* Responsibility of assignment of administering user accounts and their authentication.
* Responsibility of assigning monitoring and control of all data accessed by users.

**12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.**

A formal security awareness program is necessary to ensure that all employees are fully aware of their responsibilities regarding the security of cardholder data. It also helps to create a security-minded culture within the organization and the employees start looking at information security as a priority.

To achieve compliance, the security awareness programs must be examined and the following should be ensured:

* New employees must be given security awareness training through letters, memos, web-based trainings, meetings, etc.
* Security awareness sessions must be carried out for new hires as well as at least once a year for old employees as well to refresh their memories.
* A sample of employees should be interviewed to find out their level of understanding regarding the security awareness within the organization.
* A written or electronic acknowledgement must be undertaken by all personnel once a year which should state that they understand the security policies and procedures of the organization.

**12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)**

Hiring the wrong person for a key position that deals with cardholder data can lead the organization to face dire consequences. A newly hired employee may access PANs and misuse this information for his own malicious purpose. Conducting a thorough background check is thus very important to rule out the possibility of hiring an individual with a criminal background.

To achieve compliance, coordinate with the human resource department to verify that thorough background checks of potential candidates are done before hiring.

**12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data:**

Formal policies and procedures must be developed for service providers having access to cardholder data. To achieve compliance, thoroughly review policies, procedures and supporting documentation to ensure that processes are put into practice to manage service providers having access to cardholder data.

The following measures must be carried out to comply with this requirement:

* A list of all service providers should be maintained. This helps to keep a track of areas where potential risks are associated.
* Verify that a written agreement is provided by all service providers, acknowledging responsibility of security of cardholder data. This proves that the service providers are committed to keeping the cardholder data secure.
* Before collaborating with a service provider, policies and procedures should be documented and put into practice. Examples include incident response procedure, notification of data breach, PCI DSS compliance procedure, etc.
* Verify that a procedure should exist to check the PCI DSS compliance maintenance of the service provider at least once a year.

**12.9 Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.**

This requirement intends to reinforce that the service provider should acknowledge in the form of a written agreement that it will secure the cardholder data of the customers in every possible way and will meet all PCI DSS requirements applicable to it. The written method of acknowledgement should be agreed upon by both the provider and its customers.

**12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.**

In case of an incident, it is important to come up with an immediate remediation plan to minimize the effect. If a proper incident response plan is not devised, there will be difference of opinion and it will waste further time by all the parties to come up with a single escalation plan. It is therefore necessary to verify that an incident response plan exists and that the organization is well prepared in case of breach of data.

To achieve compliance, the incident response plan must be verified for the following:

* It must mention the roles, responsibilities and communication procedures in case of breach of data.
* It must mention business continuity procedure, data backup process, coverage of critical system components, and incident response procedures of the payment brands.
* It must be tested at least once a year.
* Interviews of personnel should be conducted to verify that in previous incidents, the documented procedures were actually followed according to the plan.
* Staff members who are responsible for the incidence response should be trained regularly and should be available 24/7 for incidence response coverage.