**How to Comply to Requirement 6 of PCI DSS**

The Payment Card Industry – Data Security Standard or PCI DSS is a standard developed by the PCI Security Standards Council, and aims to protect debit and credit card data from fraud at the hands of scammers. The requirements laid down by the PCI DSS help organizations that deal with card payments, serve the purpose of protecting cardholder data by complying with the standard. The standard consists of a total of 12 requirements, each of which have further been broken down into further requirements.

The requirement 6 of the PCI DSS deals mainly deals with applications that store, process or transmit cardholder data. The compliance to this requirement therefore, is mainly the responsibility of software developers and hence revolves around the provision of IT services.

Below we will discuss the requirement 6 of the PCI DSS and how to comply to each requirement

**PCI requirement 6: Develop and maintain secure systems and applications**

The requirement 6 of PCI DSS relates to the development of all external and internal applications that are involved in storing, processing and transmitting cardholder data. All payment applications are required to be in compliance with the Payment Application Data Security Standard (PA-DSS)

**6.1 Establish a process to identify security vulnerabilities, by using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as 'high,' 'medium,' or 'low') to newly discovered security vulnerabilities.**

For complying with the requirement 6.1, the following measures should be kept in mind:

* Identify and document a list of all software assets that are used for developing the applications, along with an explanation of which function every asset provides. Moreover, this list should always be checked for time to time and kept updated.
* Develop a system that monitors every item for any possible vulnerabilities on a regular basis. This monitoring must be done by some reliable source which can be attained by signing up with newsgroups, RSS feeds, email lists and reliable websites that provide tools for development.

**6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.**

Based upon the vulnerabilities discovered in requirement 6.1, if discovered, this requirement needs the vulnerabilities to be resolved with a patch. High level rated vulnerability should have a patch applied within a month whereas low rated ones can have their patches applied within 2 to 3 months. However, it is better to apply the patch as soon as it is possible. For monitoring and building evidence, a patching audit log must be maintained.

* 1. **Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:**
* **In accordance with PCI DSS (for example, secure authentication and logging)**
* **Based on industry standards and best practices**
* **Incorporating information security throughout the software-development lifecycle**

For compliance to this requirement, all applications should be developed according to a best practice software development lifecycle. This lifecycle needs to be documented to prove how the PCI DSS requirements are met during the defining, designing, analyzing and testing phase of development.

The documentation of application development must cover how the application is supposed to store, process and transmit cardholder data.

* + 1. **Remove development, test and custom application accounts, user IDs, and passwords before applications become active or are released to customers.**

In order to comply with this requirement, develop a process that verifies the removal of all developer accounts from the applications. The process should be documented and an audit record should be included.

* + 1. **Review custom code prior to release to production or customers to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following.**

A code review should be conducted as part of this requirement, by reviewers who have expertise in coding technology and a well developed understanding of PCI DSS. The reviewers should verify the documentation process of requirement 6.3.1. Complete documentation of the code review process should also be conducted and it should be approved before the release of the application.

**6.4 Examine policies and procedures to verify that the following are defined.**

* **Development/test environments are separate from production environments with access control in place to enforce separation.**
* **A separation of duties between personnel that are assigned to the development/test environments and those persons assigned to the production environment.**
* **Production data (live PANs) is not used for testing or development.**
* **Test data and accounts are removed before a production system becomes active.**
* **Change control procedures that are related to implementing security patches and software modifications are documented.**

According to PCI DSS, development and test environments are never secure enough for holding cardholder data. These environments should thus be kept separate from production environments. A good way to keep them separate is through network segmentation. To achieve this segmentation, an Access Control List (ACL) on a switch or a firewall can be used. Similarly, to achieve compliance, personnel involved in development and test environment should not be in touch with that of production environment.

**6.5 Address common coding vulnerabilities in software-development processes as follows.**

* **Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.**
* **Develop applications based on common coding guidelines.**

This requirement of PCI DSS asks for training of developers in learning secure coding methods for application coding. To achieve compliance, these coding techniques should follow best practices and should be documented so that developers follow them accordingly. If a developer can identify and sort coding vulnerabilities after training, he is said to be complying according to the PCI DSS. But these trainings must be conducted with every new hiring and on an annual basis to ensure ongoing compliance. To further ensure effective developer trainings, it is recommended to have new hires sign a compliance agreement or make them pass a test to evaluate their understanding towards compliance with the requirement.

**6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods.**

* **Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.**
* **Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.**

This requirement can be met with the help of a Web Application Vulnerability Scanning or a Web Application Firewall. However, organizations commonly apply both controls to ensure maximum security.

A Web Application Vulnerability Scanning enables vulnerability testing throughout the lifecycle of software development whereas a Web Application Firewall should be able to prevent all web application vulnerabilities laid down in requirements 6.5.1. to 6.5.10. This firewall should not be confused with a traditional network layer firewall, because it also checks traffic at application layer, unlike the network firewall.

**6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.**

As we went underway from requirement 6.1 to 6.6, all compliance measures taken were recommended to be documented. Requirement 6.7 requires that this documentation is properly managed and made available to all the concerned parties. To make sure that all the required documentation stays updated, it is recommended to conduct an annual review and document the review process as well. All documentation must be accessible to all the involved personnel and any changes in policies and procedures should also be communicated to the concerned individuals.