**PCI DSS Audit and Certification Checklist: Getting Ready For the Final Audit**

For organizations that are new to the process of achieving and maintaining PCI DSS, compliance may seem like a tedious and costly task. However, if most of the small and medium enterprises are able to put the right tools and practices in place, the process can be made much simpler. Before you make the final call to the auditor, make sure that you have marked and conformed to all the points in your compliance checklist. If you are not making use of a hosted solution, you need to fulfill all the 12 requirements of PCI DSS at all times in addition to a number of other key points that ensure your readiness for the final audit.

The following list of check points will help you prepare your organization for PCI compliance audit.

1. **Categorize the Level of your Organization.**

The foremost important step is to categorize your merchant and service provider level. This is important because it will help you decide whether you need to work on a Self-Assessment Questionnaire (SAQ) or if you need Level 1 Onsite Assessment done by a Qualified Security Assessor (QSA).

1. In case of SAQ compliance, determine the platforms that you need to be compliant with. This can be determined by visiting [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) and finding out which scenario fits the best for your organization. Based on the scenario, you can choose from a number of SAQ platforms such as A, B, C, C-VT, D, P2PE-HW.
2. In case of Level 1 Onsite Assessment, get a Qualified Security Assessor who can ensure good quality of work along with a good fee.
3. **Develop the Scope of PCI DSS for your Organization**

Though it may seem easy at first, it is one of the most daunting tasks to develop and maintain a track of all credit card assets and locations. You must know the business process that involve the use of cardholder data, its storage location, its access mechanism, the ports and protocols applied when transferring cardholder data from one location to another, etc. Update this inventory on an ongoing basis.

Many organizations fail to achieve PCI compliance when they try to implement the standard across the entire organization instead of focusing only on the areas involved in dealing with cardholder data. Scoping your organization for PCI DSS helps save a lot of time, cost and effort for both the organization and its QSA. With minimized scope you are able to effectively concentrate on compliance areas only. Make sure that you include only those processes in compliance scope that are directly or indirectly involved in storing, processing and/or transmitting cardholder data.

1. **Install and Keep an Updated Firewall**

Although it may seem like an easy task at first, most of the organizations fail to comply with the very basic requirement of PCI DSS. This normally happens due to misconfigured firewall. Hence, it is very important to keep an updated firewall between the public network and cardholder data.

1. **Ensure the Implementation of Strong Access Control**

Protection of data is ensured with regular implementation of strong access control measures. Make sure that you have deployed digital certificates and other widely used cryptographic techniques for authentication purposes. Additional security is also desirable where access to data decryption keys is limited to a “need-to-know” basis.

1. **Strictly Consider Compliance as an Ongoing Process**

New threats keep on emerging every day just as compliance requirements keep evolving. To ensure compliance at all times, it is important to conduct regular monitoring and testing of networks. Review your PCI scope at least every three months and make use of data loss prevention and event monitoring tools to analyze the safety of your data in real time. Also verify that all your third parties that deal with storing, processing and transmitting cardholder data are also PCI Compliant and ask for a written proof.

Often organizations that achieve one time compliance fail to maintain and operationalize their PCI compliant policies and procedures. Though the intent to remain compliant never diminishes, gradual change of environment leads towards nonconformance. Some of the factors may be new employees, turnovers, or promotions. Many auditors see this as a general weakness in organizations where they lack the willingness to keep up with controls. To ensure long-term success of your PCI DSS agenda, you must include these checkpoints in your final list every time:

* Awareness and support of senior leadership in terms of cardholder data security and contractual responsibility.
* Role awareness and implementation of all control owners that are assigned to every PCI control.
* Written procedures to manage control processes as outlined by PCI DSS.
* Existence of automated tools such as SIEM, File Integrity Monitoring, etc. to help operationalize security controls.
* Existence of automated tools to monitor and measure the effectiveness of security controls.

Some of the processes that can be automated with the application of correct tools are:

* File Integrity Monitoring
* Incident Response
* Vulnerability Management
* Asset Identification and Management
* Logging and Security Event Monitoring
* Default Password Checking
* Firewall Rule Review
* Access Provisioning and Access De-provisioning
* Wireless Rogue Detection

1. **Keep your Policies and Procedures Updated**

It is important to keep a track of changes and updates in organizational policies and procedures, to make it easier for the auditor to understand the changes. The Information Security Policy, in particular, should be maintained and communicated to all employees to keep them knowledgeable about information security threats. Regular trainings and awareness sessions on information security must also be conducted.

1. **Conduct Internal Audit**

To ensure all your controls are working effectively, always conduct an internal assessment or audit prior to the final audit. Often the IT controls implemented for ensuring compliance do not work as expected and internal audit can help fix these errors to put all controls in place.

1. **Communicate with your Qualified Security Assessor through the Year**

You must always stay in contact with your QSA throughout the year, especially in times of major environmental changes. This helps to keep them updated and also allows you to proactively deal with any potential new issues rather than dealing with them after implementation. With their years of experience they can provide you with valuable and meaningful advice right when the problems arise and help you solve them there and then.