**Your PCI DSS Compliance Checklist**

Achieving Payment Card Industry Data Security Standard compliance and then maintaining it is not an easy task and is also costly. But for most of the small and medium enterprises, it does not necessarily need to be too hard if the correct tools and plans are put in place. If you are not utilizing a hosted solution, all the 12 requirements of PCI DSS need to be fulfilled. The requirements of PCI DSS must be met at all times for total compliance and annual audit must be conducted to ensure compliance. However, a compliance checklist for PCI DSS can help to keep all the important steps necessary to achieve compliance, besides meeting all the twelve requirements of PCI DSS.

To ensure ongoing compliance, the following actions of the checklist must be carried out every year.

* Determine the scope of PCI DSS for your organization and perform all necessary actions to reduce the scope. Reduction in scope is important for easy achievement of PCI Data Security Standard compliance.
* A Risk Assessment of the cardholder data environment must be conducted every year.
* If you consider the compliance to all requirements by yourself as a difficult task, take the services of a web host that deals in payment card industry and can help you in complying with the standard.
* Do not store cardholder data in your office computers or network systems. If you do so, that would bring your whole network under the scope of PCI Data Security Standard compliance which would be very difficult to evade.
* If you need to access credit card numbers for some legitimate reason, using a system which takes the data on run time without storing will save it from being compromised at the hands of a malicious user in many ways.
* Get help of a Qualified Security Assessor (QSA) to complete your annual Report on Compliance. If you are a small merchant and fall into the level 4 merchant category, you can also fill out a questionnaire known as Self Assessment Questionnaire (SAQ). It is also important to hold a PCI scan of network holding cardholder data after every quarter.
* Verify that all external parties that are involved in storing, processing and transmitting cardholder data or are indirectly linked with cardholder data are complying with the PCI Data Security Standard and demand written proof of their compliance.
* Conduct regular bi-annual trainings to your staff to aware them of PCI DSS requirements and how to comply at personnel level.
* Ensure that incase a third party payment application is being used, the version and product in use is PA DSS (Payment Application Data Security Standard) compliant and all instructions given by the supplier are being followed accordingly.
* Keep only that data which is required and save it in encrypted or masked format so that it is unreadable to a malicious individual.
* Apply strict security measures to your e-commerce environment. Regularly monitor and control it.
* Hire help from an Approved Scanning Vendor (ASV) to conduct regular network scans. Network scanning must be carried out in every quarter of the year.
* Secure your network by using updated and PCI compliant antivirus and firewalls at all times.
* Patch your shopping cart application with the most recent available version.
* Conduct PIN Entry Device (PED) tests once a year and also after any noteworthy change to the cardholder data environment.
* Make sure that your web hosting service provider has secured systems that are in compliance with international standards for system hardening. All database and web servers need to be hardened to disable unwanted services and default setting.
* Choose only that hardware or software for processing transactions that are approved by the PCI Security Standards Council. To ensure this, check the SSC list for approved products by approved vendors.
* Create an inventory of all locations and assets that store, process or transmit cardholder data. This inventory must be prepared after addressing the following questions:
* Which processes of the business use cardholder data?
* Where is the CHD (Cardholder Data) stored?
* Which protocols and ports are used while transmitting the cardholder data?
* How is it accessed?
* Which technological assets are used when storing, processing and/or transmitting cardholder data?

To validate your inventory list, choose a sample of your networks, systems and components and make sure that the list covers everything that plays a role in the flow of cardholder data. Determine if any cardholder data is present outside the list you created and regularly keep on updating your inventory list depending upon any technological or business changes.

* Maintain the state of PCI compliance once it has been achieved. Compliance is not a onetime process as control activities may change over the passage of time such as employee turnover or promotion or a change in organizational priority. It is thus very important to operationalize security objectives. To achieve this, the following questions must be catered for:
* Are there any documented procedures for managing control objectives of the PCI Data Security Standard?
* Are there any automated tools to engage the current security practices? (E.g. Vulnerability Management, Penetration Testing, SIEM, etc.)
* Are there any automated tools to examine the usefulness of these control activities?
* Automate control processes for compliance management to rule out the possibility of human error. The following checklist of processes can be automated with the right tolls and technology:
* Asset Discovery and Management
* Vulnerability Management
* Default Password Checking
* Firewall Rule Reviews
* Wireless Rogue Detection
* Access Provisioning and De-provisioning
* Logging and Security Event Monitoring
* File Integrity Monitoring
* Incident Response Tracking

Tools for vulnerability scanning and Security Information and Event Management (SIEM) help to produce vulnerability remediation and incidence response reports, system hardening compliance reports, access management reports, traffic flow reports and data flow reports, etc. These reports can then be used during PCI compliance audits with your Qualified Security Assessor.