**4 Simple Ways to Become PCI Compliant**

The PCI DSS 3.1 will expire on the 31st of October, 2016. After this date, organizations will need to follow PCI DSS 3.2 and achieve compliance to this version by 1st of February, 2018. Ever since the release of the latest version of PCI DSS, businesses have begun to bring about the required security and compliance changes in their operations. Organizations that have still not achieved compliance to PCI DSS 3.1 have now become soft targets for malicious attackers.

It is therefore, very important for businesses to understand in simple steps, how they can become PCI compliant. The first step towards doing anything is to plan it properly, and the following steps will help businesses understand how to go about achieving PCI compliance.

1. **Document all your Work**

It is important to keep a track record of all your policies and procedures and all decisions made during the normal course of business operations. This helps in future to find out a particular information about an event, and may in turn help employees understand what they need to do in case a similar problem arises again. If the decision made earlier turned out to be fruitful you may follow the same procedure again. If it did not, you may try a different response.

Documentation is important because it can help you in the following ways:

* It helps you identify the problems that are still prevalent in your organization.
* It increases the uniformity and quality of your compliance process.
* It ensures absolute accountability by serving as a standardized reference.
* Documentation of the entire PCI DSS process also ensures that you stay secure every step of the way.

1. **Assess your Scope**

It saves a lot of time for businesses if they assess their scope in the start and move ahead towards achieving compliance accordingly. Scope includes all people, processes and components that are directly or indirectly involved in storing, processing or transmitting cardholder data.

It is important to determine scope in order to be able to fully protect all areas where the cardholder information may lie. The best way to do so is to create a cardholder data flow diagram for all entities, inputs and outputs. This helps illustrate where and how your data is stored, received or transmitted.

Assessing PCI DSS scope will bring you the following benefits:

* Time reduction in achieving PCI DSS compliance certification
* Efficient utilization of resources resulting in greater Return on Investment (RoI)
* Implementation of only those controls that are required, thus reducing complexity and cost
* Development of groundwork for remediation planning
* Identification and protection of all cardholder data resulting in greater customer satisfaction

It is also a good practice to reduce your scope of PCI DSS, which will minimize your PCI compliant areas. Scope reduction can be achieved through network segmentation, in which cardholder data is separated from rest of the business network.

1. **Conduct Staff Trainings and Awareness Sessions**

Employees are the biggest loopholes that come in the way of keeping your organizational data secure. In fact, 60% of data breaches result due to negligence on part of employees or corporate partners. Many employees, though may know the nature of sensitivity of information, are not very vigilant or careful when handling such data. Despite this, many organizations do not spend enough money and resources to properly train their staff.

Trainings should not be generic. Rather each employee role should be given customized training that caters to their specific role in the organization. Rather than annual trainings, monthly trainings should be conducted to keep the staff in touch with the security requirements at all times. Constant reminders will help them retain useful information.

Create a means of accountability for the employees in case of security breach. This will ensure vigilance on their part and protection of your business and customer information on your part.

In general, security awareness trainings can help you in the following ways:

* Provide better protection of organizational assets by preparing employees to respond to real and potential security threats and keeping them up to date on new risks as they emerge.
* Boost employee morale by rewarding and recognizing employees who show good security behavior in times of need and otherwise.
* Save financial and reputational costs by reducing the number of security breaches. The sooner an incident gets identified, the less costly will it be to remediate it.

1. **Get Help from Security Professionals**

Getting help from security professionals such as Qualified Security Assessors can be a good way to ensure that you don’t miss out on any area. Even if you are already compliant, consult them in case there is a new update to the standard, such as the release of version PCI DSS 3.2.

Businesses usually don’t invest in resources such as these, however, security professionals are experienced in their area and have undergone rigorous trainings to master all aspects of PCI DSS and information security. They are also technically qualified and experienced to assist you in achieving compliance. QSA’s can provide merchants with a number of services such as PCI Audits or onsite Data Security Assessments, Gap Analysis, PCI Remediation Services and any other PCI consultation and advice in general.

Below we look at the pros and cons of “doing it yourself” versus “getting it done from a professional”.

***Doing it Yourself*:** It may seem more economical than hiring a professional, however, it makes it difficult for merchants to keep pace with all the requirements of PCI DSS and they may find themselves missing key controls. Again, in an attempt to keep up with the missing areas, the company may end up spending more money on internal resources.

***Hiring a Professional*:** It may be more costly but it provides a third party validation to the company. However, in case of a security breach, the liability still lies on you and not the QSA. But, it ensures that all key areas and controls are catered for and provides a complete solution at the hands of experienced professionals. They can also provide unbiased recommendations free of internal disagreements and make positive use of their experience working previously with a company in a similar industry as yours.