MAINTAINING A PCI DSS COMPLIANCE

PCI Maintenance IS Terribly Important

Why Maintain Regularly?

Achieving PCI DSS Compliance for your organization is a challenging task. However, the story does not end here. Maintaining a PCI DSS compliance is even more challenging, involves a series of activities to perform in defined timelines and hence, prone to failure if not managed effectively.

Effective maintenance of PCI DSS is necessary to:

- Verify compliance with the requirements of PCI standard and organizational security policies and procedures
- Ensure protection against emerging security threats.
- Include, changes if any in the applicable regulatory standards and
- Address internal information technology changes that may compromise cardholder data

Why PCI DSS Maintenance Fails?

There are several reasons why normally organizations fail to sustain a PCI DSS Compliance. Some of them are listed below:

- Lack of awareness about the compliance activities to perform
- Missing out the timelines for the compliance activities.
- Missing out to implement the applicable PCI controls on the new systems in scope
- Failure to detect / implement changes if any, in the applicable regulatory standards or PCI DSS itself.

In 2016, for the first time, more than half (55.4%) of organizations were fully PCI DSS (see below) compliant at interim validation—compared with 48.4% in 2015. Full compliance has increased almost five-fold compared to our analysis of 2012 assessments

Despite this general improvement, the control gap of companies failing their interim assessment has actually grown worse. In 2015, companies failing their interim assessment had an average of 12.4% of controls not in place (6.8% across all companies). In 2016, this increased to 13.0% (5.8%).

Many of the security controls that were not in place cover fundamental security principles that have broad applicability. Their absence could be material to the likelihood of an organization suffering a data breach. Indeed, no organization affected by payment card data breaches was found to be in full compliance with the PCI DSS during a subsequent Verizon PCI forensic investigator (PFI) inquiry.

Source: Verizon 2017 – Payment Security Report

MAY - 2018 | PCI DSS MAINTENANCE

- Failure to detect and address internal information technology changes that may affect PCI DSS certification scope environment.

Consequences of failure to maintain PCI DSS?

- Missing out the date of PCI DSS re-certification
- Failure to submit the timely compliance reports
- Increased risk of security breaches due to vulnerable systems
- Business and financial implications
- Reduced customer trust
- Legal or contractual actions

What is PCI DSS? The Payment Card Industry Data Security Standard (PCI DSS) was set up by the leading card brands to help businesses that take card payments reduce fraud. While it's focused on protecting card data, it's built on solid security principles that apply to all kinds of data. It covers vital topics like retention policies, encryption, physical security, authentication and access control.

Find out more: PCISecurityStandards.org

How to successfully maintain PCI DSS Compliance?

It all starts with an efficient planning, accurate assignment of responsibility, accountability an timely monitoring.

A. Efficient Planning:

- Identify and document the daily, weekly, monthly, quarterly, biannual and annu activities.
- Define the PCI DSS Compliance Calendar.

B. Accurate Assignment of Responsibilities and Accountability:

- Define the clear responsibility and accountability against each activity identified in th PCI DSS Compliance Calendar.
- Identify dependencies, if any for completion of each activity.

C. Timely Monitoring:

- Monitor timely completion of activities, their compliance status.

Must Do Activities as per PCI DSS:

1. Patch management Every Month for all critical systems in PCI DSS Scope
2. Quaterly internal vulnerability assessment for servers and network devices.
3. Quaterly external ASV scanning on all public ip-addresses.
4. Quaterly user account privileges review and removal of users not logged in last 90 days.
5. Half-yearly firewalls and routers rule set reviews.
6. Annual risk assessment for the environment in PCI DSS scope as applicable.

Additional activities that you might consider performing:

1. Quaterly card holder data search on desktops, file servers and databases etc.,
2. Quaterly information security awareness training
3. Half yearly policies, procedures review and update as applicable
4. Half yearly incident reposne training
5. Annual internal and external penetration testing
6. Vendor evaluation as and when required

QRC
Quality • Risk • Compliance
QRC Consulting & Solutions Pvt Ltd

Already PCI DSS Certified? Wondering what to do next to maintain the compliance? Want to know the current Compliance Posture w.r.t PCI?

Here are some of our services can help:

1. Quaterly Health Check
2. PCI DSS Gap Assessment
3. Vulnerability Assessment and Penetration Testings
4. Data Discovery Scans
5. Firewall and Router Rule Set Reviews
6. Awareness Trainings

Get all these services in one go with our “PCI DSS Annual Maintenance Service”.

Contact Us Now at vamsikrishna.m@qrcsolutionzcom | +91-9324-813-180

Visit us On: https://www.qrcsolutionz.com