5 Essential Steps to Sustainable PCI DSS Compliance

How to Focus an Organization's Efforts for the Best, Most Cost-Effective Results

Like it or not, the Payment Card Industry Data Security Standard (PCI DSS) isn't going away. In fact, Version 3.0, in effect since January 1, 2014, imposes new requirements on all entities handling cardholder data.

What's worse, the data-thieves who are after customers' card numbers, expiration dates, and security codes are working harder and becoming smarter than ever. Recent massive and well-publicized data breaches have made it all too clear how much damage a credit card breach can do to a company's sales, reputation, and stock price.

For many companies, PCI DSS compliance seems so daunting and complex that they only follow the letter of the regulations, without focusing on the subtle areas that provide the most protection.

"Compliance" is no guarantee a company won't get hacked.

In fact, as the PCI Security Standards Council reported, "Lack of education and awareness around payment security and poor implementation and maintenance of the PCI DSS Standards leads to many of the security breaches happening today."[1] That makes it even more important for anyone handling customer data to do a better job protecting it.

For many companies, PCI DSS compliance seems so daunting and complex that they only follow the letter of the regulations, without focusing on the subtle areas that provide the most protection. This E-book describes the five "must-do" steps that help assure the effectiveness of a company's PCI DSS compliance program.

1 Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard Version 3.0 Change Highlights

SUNGARD® AVAILABILITY SERVICES™

E-BOOK

Sustainable PCI DSS Compliance

Step One: Overcome the culture of undocumented changes

Nobody likes documenting changes to servers, networks, or Access Control Lists (ACLs.) Figuring out what needs to be changed, and why, and then reconfiguring the systems is difficult enough without having to update a configuration control system or network configuration log.

But such tracking is essential to avoiding a data breach that could ruin the financial quarter for an organization, or a career for an IT or compliance professional. One reason documentation is critical is that an organization can't protect what it doesn't know is there. What needs protecting is, of course, cardholder data (CHD), and the PCI DSS requirements kick in for any system that stores or processes such data. Without complete and up-to-date documentation an organization has no way of knowing where CHD sits in its far-flung infrastructure, and thus how much of it needs protection. In fact, one of the changes in PCI DSS 3.0 is a requirement for "a current diagram that shows cardholder data directional flows" as part of the organization's network diagrams, as well as maintaining "an inventory of system components in scope" for compliance.

The second reason to document is that the auditors will demand proof that any organization handling CHD has the proper security processes, including documentation, in place. Documentation is seldom a favorite task for an IT staff, but it becomes more stressful in the middle of an audit with the chief security officer, chief risk officer, or other C-level executive watching and asking why it wasn't done sooner.

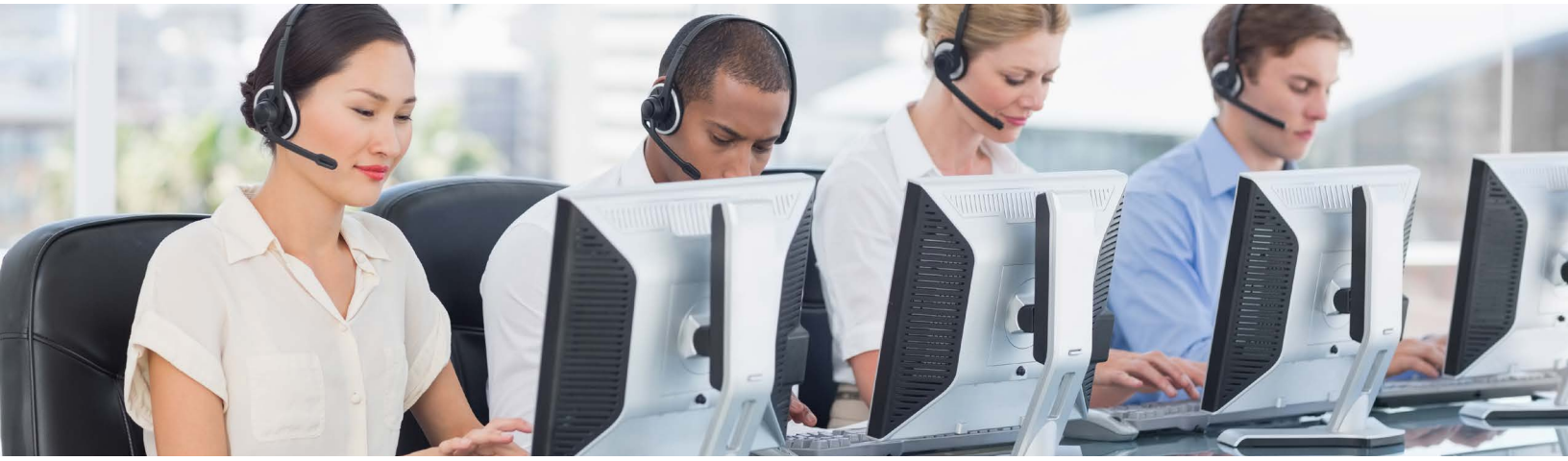
Finally, documentation is the only way to evaluate and assure PCI DSS compliance. This is especially true if the people who designed an organization's network or card-handling applications have since left the company. Just as with documentation, trying to re-create CHD flows in the middle of an audit is no easy task.

This configuration documentation should cover all network devices, such as all routers and switches, not just those configured as firewalls. Again, note that compliance must be ongoing and sustainable. The documentation must be updated as patches are applied, new applications added, old apps decommissioned, and business partners and sales channels changed. Entity-relationship diagrams are useful for identifying which databases and other systems process and store CHD. But again, these are only useful to the extent they are current and accurate.

That's why PCI DSS requires that this documentation be completed, updated, and reviewed annually. One way to ensure this happens is to assign responsibility to a team or individual. Remember also that organizations need to create not only high-level policies, but also specific procedures for PCI DSS compliance steps, such as documentation reviews.

Finally, remember that even if everything is perfectly configured, an organization still must assign staff to watch the monitoring devices and software, something too many organizations fail to do. A device can flag something, but a person has to determine specifics such as, "What port is open? What's being attacked? How do we stop it and how do we prevent it from happening again?" While this step is often outsourced, the merchant must still stay aware of alerts and communicate with the service provider to understand how it responded to them.

Without complete and up-to-date documentation an organization has no way of knowing where CHD sits in its far-flung infrastructure, and thus how much of it needs protection.



Step Two: Shrink the cardholder data environment

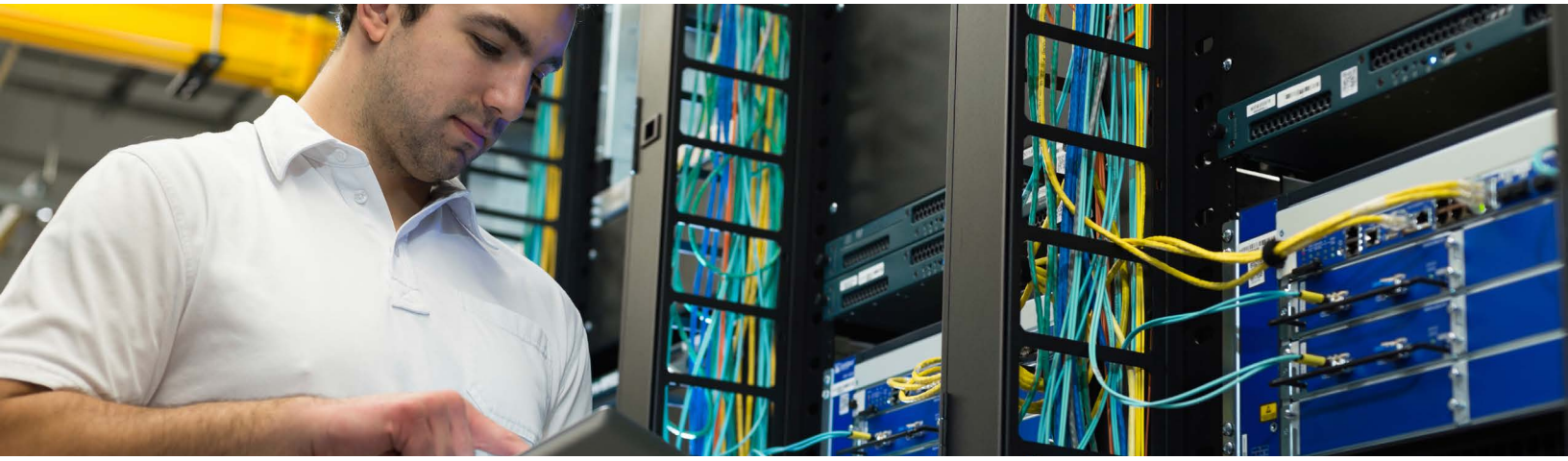
Today's information systems are incredibly complex, as are the relationships that companies have with their credit card processors. Knowing what parts of the IT infrastructure are touched by CHD, even for a split second, is important, because any devices that are not touched *don't* need to meet the long list of PCI DSS requirements, as long as the proper parameters are in place to physically and logically separate them from the rest of the network.

Unfortunately, many companies have no clear idea of how far their cardholder data environment (CDE) extends. For example, one company assumed that its call center employees were entering credit card numbers from customers directly into a system owned (and thus kept compliant) by an outside processor. It instead maintained an internal application at the call center where employees were entering the credit card numbers. This unknown portion of the CDE would have been a target for hackers — and surely drawn unwanted negative press.

Once an organization has identified all the end-user devices, servers, storage, and networks in its CDE, it should shrink it as much as possible by putting all those elements on a logically separated network segment that is invisible to the rest of the organization. If a merchant does this, it can focus its PCI assessment and compliance on only that network segment.

QSA Tip

If an organization is not sure the documentation of its CDE is complete, it can run a regular expression configured to look for suspicious patterns, such as 16-figure numbers, expiration dates, and security codes, to help discover where the credit card data really lives.



Step Three: Make network segmentation rock-solid

Once sensitive data is isolated on a limited network segment, it's tempting to focus only on the configuration of the devices within that segment. But first, it's important to check the quality of the segmentation, as the entire PCI compliance effort is dependent on isolating the segment that contains CHD. If any CHD can leak from the "safe" environment or another segment can touch that data, the organization is out of compliance and at risk of a breach.

Remember, for example, that firewalls are required on every port from the external Internet to the internal environment (all ingress and egress points), so no traffic is unchecked. ACLs must also be secured, so no traffic goes through a non-secured protocol, and unneeded services, such as Telnet (a method to connect to a system remotely), must be turned off so they can't be used by attackers.

QSA Tip

Inadequately configured ACLs are a common PCI DSS weak point. If only three of the four ingress points to the "CDE are secured by firewalls and the fourth only by routers or switches, unauthorized traffic could still get through. Remember also to "harden" all servers by turning off unneeded services and implementing two-factor authentication for all administrator access, and complex authentication for all other access to company systems.

Step Four: Know what to ask a cloud service provider

Moving selected data or a portion of its credit card processing to a PCI DSS compliant cloud can seem like a tempting way for an organization to ease its compliance burden. And it can help, but there are limits to how much responsibility the cloud vendor can handle. In addition, not all "compliant" cloud providers are created equal.

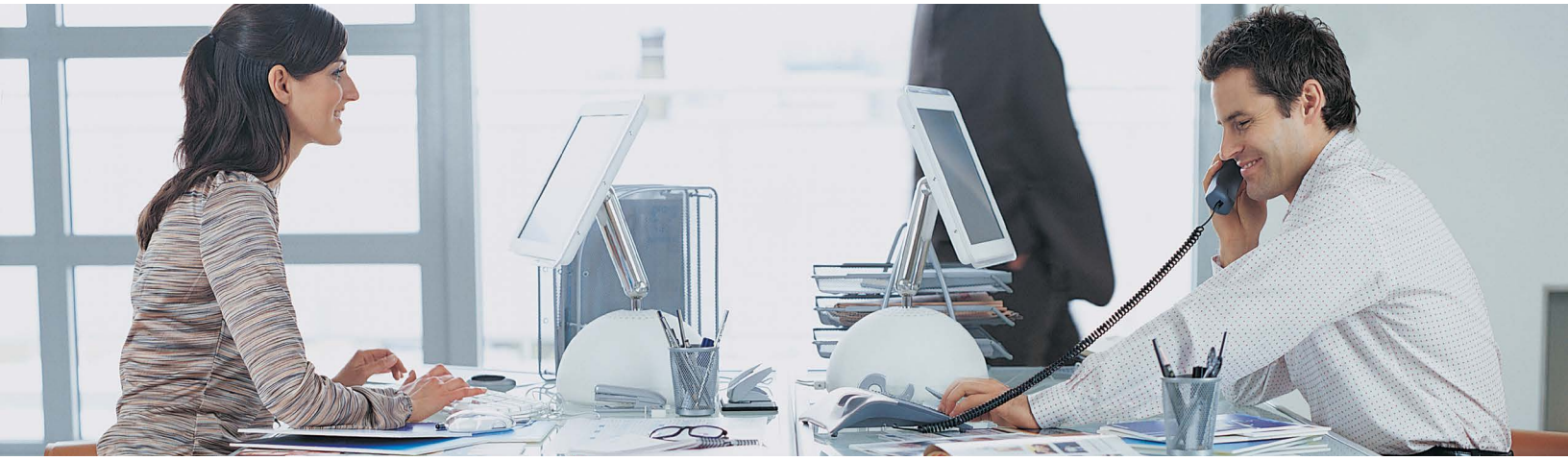
With those complexities in mind, among the questions to ask a prospective cloud provider are:

- What security certifications do you have and what audits have your cloud platform undergone? (PCI DSS Certification, SSAE 16 Type 2, ISO 20000-1, etc.)
- Specifically how do you segment your network to segregate traffic from different customers?
- Specifically how do you ensure all cardholder data is masked while at rest, and encrypted while in transit
- How much experience do you have with businesses like ours and with PCI DSS compliance specifically?
- What PCI-related policies and processes do you have in place? How do you ensure your staff follows them?
- Can you help us identify and address gaps in our current PCI DSS compliance plan?
- How and by whom is the compliance and certification process handled within your company?
- Do you have PCI DSS experts on staff that understand the audit process and provide documentation for your areas of responsibility?

QSA Tip

Just because an organization has signed with a "PCI DSS Compliant" cloud provider doesn't mean it can stop thinking about compliance. The cloud provider is responsible for protecting CHD only from the point it enters its network environment until the point it leaves. Once that data moves from the provider to the public Internet, or back to the customer's internal environment, the cloud provider is not responsible for it. Version 3.0 of the PCI DSS standard requires that if a third party "undergoes their own PCI DSS assessment, they should provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place." It also requires companies to "maintain information about which PCI DSS requirements are managed by service providers and which are managed by the (customer)."

If any CHD can leak from the "safe" environment or another segment can touch that data, the organization is out of compliance and at risk of a breach.



Step 5: Assure the needed skills in-house

Everyone involved with creating or supporting PCI compliant systems should be trained to perform daily tasks with a "PCI-centric" mindset. These range from network and UNIX administrators to Windows developers and administrators, as well as security teams.

Certifications, such as Cisco Certified Internetwork Expert and Cisco Certified Design Professional are, of course, a first step toward assuring an organization's administrators can handle important work, such as configuring firewalls and routers to securely segment networks.

It is even more desirable if the administrators are familiar with at least the basics of PCI DSS. One step to assess this would be asking a candidate how they would go about configuring firewalls to meet the PCI network administration requirements. If the candidate cannot even begin to answer, their skills are clearly in question.

QSA Tip

An Internal Security Administrator (ISA) is the in-house equivalent of the QSA who comes in from the outside to assess an organization's level of PCI DSS compliance. Bringing on an ISA, at least on a part-time basis, can help make sure that internal processes and documentation are up to specification before they are assessed for real. An ISA can also help train staff members so they can do more of this work on their own in the future. Another benefit is that an ISA can act as the point person during the full QSA PCI review, answering any questions and working with the external QSA to make sure the review runs smoothly.

Everyone involved with creating or supporting PCI compliant systems should be trained to perform daily tasks with a "PCI-centric" mindset.

5 Essential Steps to Sustainable PCI DSS Compliance

How to Focus an Organization's Efforts for the Best, Most Cost-Effective Results

Conclusion

The legal and regulatory pressures driving the need for PCI DSS compliance are only growing. So are the efforts of hackers to steal and misuse CHD, with new and more varied attacks being launched almost every day.

The millions of organizations covered by PCI DSS must understand that compliance is not just an unavoidable expense. It can also help assure their reputation and relationship with their customers. There are no "one stop" solutions for PCI DSS compliance. It requires ongoing effort, commitment, and discipline.

But taking these five steps will at least help ensure an organization is using its valuable time and staff effectively to stay compliant and, more importantly, to avoid a data breach.

There are no "one stop" solutions for PCI DSS compliance. It requires ongoing effort, commitment, and discipline.

Additional reading

Security in the Cloud

Cloud Solution Brief

About Sungard Availability Services

At Sungard Availability Services, we continuously refine our infrastructure and processes to support our customer's compliance requirements. Our **Managed Cloud** and **Managed Private Cloud** platforms have been rigorously built and tested to comply with the PCI DSS cloud service provider standards.

As a long-time Qualified Security Assessor, Sungard AS has the personnel, methodologies, tool sets, and experience to highlight security holes, provide recommendations, and implement fixes for your cardholder data environment.

Sungard AS will work with you to:

- Perform a gap analysis to identify and prioritize PCI-DSS issues.
- Mitigate gaps through process reengineering, solution implementations, and training.
- Rationalize the use of credit cards via tokenization, segmentation, storage, etc.
- Develop policies and procedures for security appliance configuration management.
- Conduct auxiliary reviews, including: penetration testing, scanning requirements, web application reviews (white and/ or black box testing), vendor eviews, etc.

To learn more about our PCI-DSS Compliant Managed Cloud or Managed Private Cloud, visit **http://www.sungardas.com/Solutions/Cloud/IaaS/Pages/InfrastructureasaService(IaaS).aspx**.

About Sungard Availability Services
Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

To learn more, visit **www.sungardas.com** or call **1-888-270-3657**

Connect with Us