Charles J. Denyer, PCI-QSA

The Payment Card Industry Data Security Standards (PCI DSS): A Comprehensive Overview

By Charles J. Denyer, PCI-QSA

The Payment Card Industry Data Security Standards (PCI DSS): A Comprehensive Overview

By Charles J. Denyer, PCI-QSA (cdenyer@ndbcpa.com)

Expert Advice from a PCI-QSA in Understanding the Importance of Cardholder Data Security and Other Critical Decisions

PCI DSS (Payment Card Industry Data Security Standards) compliance for all merchants regarding the newly updated version 3.0 PCI DSS standards can be an incredibly challenging and complex undertaking - one that needs to be clearly defined and understood for ensuring a smooth and seamless transition from version 2.0 to 3.0. With many software vendors, payment processors, and other parties now heavily involved in the world of PCI compliance for merchants, it's important to understand roles, responsibilities, and overall scope requirements for all parties involved in the entire PCI DSS lifecycle.

Migration from PCI DSS 2.0 to 3.0 | What Is the Difference?

As one of North America's longest-licensed PCI-QSA's, I've been involved with PCI DSS compliance since 2008, and I consider the changes from 2.0 to 3.0 to be better in some regards, but these changes require merchants to place a greater focus on the concept of risk, developing additional policies and procedures, along with other important measures. More specifically, the biggest differences I see from 2.0 to 3.0 are:

- Increased clarity and transparency on reporting in regards to the requirements and the actual testing procedures. There has been a removal of the "vagueness" that once plagued the standards.
- More detailed than before, which is probably the single reason why organizations consider 3.0 much more comprehensive because it requires more effort than 2.0.
- Enhanced flexibility in reporting, along with a clarification on the all-important topic of "scope."
- Additional requirements for documentation (i.e., policies, procedures, and more).
- Ultimately, reporting with a greater emphasis on the concept of risk, but one that still comes with a laundry list of "prescriptive" mandates, such as policies, security awareness training, password rules, and a laundry list of other items.

Information security evolves over time, and various benchmarks, standards, and frameworks also change, hence the reason from 2.0 to 3.0. These changes came about because of concerns noted within the payment industry. The PCI council noted the following challenges and compliance concerns still persisted, even years after the launch of the initial PCI DSS framework. These challenges include:

- Inadequate, missing, and inconsistent security awareness training mandates.
- Weak access control initiatives.
- Weak documentation in regards to information security and operational policies and procedures.
- No initiatives for assessing risk.
- Third-party security concerns.

Qualitative Ingredients for PCI Success for SiteLink Merchants

All merchants should take note of the following factors for ensuring successful PCI compliance endeavors for 2015 and beyond.

- **Policies and Procedures:** Quite possibly the biggest and most demanding mandate for PCI compliance is developing comprehensive information security and operational specific policies, procedures, and other supporting documentation. Sure, PCI is technical, as discussions on firewalls, encryption, audit logs and other technical considerations always seem to be high on everyone's list, but don't lose sight of the need for in-depth policies and procedures. Authoring PCI specific documentation is incredibly time-consuming, so the obvious choice is sourcing high-quality PCI templates and compliance toolkits. Find a high-quality, industry leading set of policies, such as those available at pcipolicyportal.com, and you should be fine.

- **Security Awareness Training:** Security awareness training is an explicit mandate for PCI DSS certification and should be undertaken annually, at a minimum, for all merchant employees and other workforce members. Companies spend massive amounts of money on the latest and greatest hardware and software solutions for protecting cardholder data – and that's fine – but don't lose sight of the fact that security awareness training is mandated, relatively inexpensive, and highly beneficial. When it comes to ROI in terms of PCI certification, security awareness training, when done properly, is a real winner. Also, it is important to test one's knowledge on security awareness training subject matter, so a short quiz is a really good idea for ensuring that

employees and other workforce members truly understand and retain critical information.

> "When it comes to ROI in terms of PCI certification, security awareness training, when done properly, is a real winner."

- **Risk Assessments.** Assessing one's risk on an annual basis, while a mandate for PCI DSS compliance for some merchants, is also a best practice that just makes sense. Think about it – isn't it just a good idea for merchants to assess and evaluate critical risks, issues, and other factors that could potentially jeopardize short-term and long-term growth, profits, and viability? Sure it is. More important, assessing risks for merchants doesn't have to be a laborious and time-consuming process: just obtain an easy-to-use, yet comprehensive, tool designed specifically for merchants. You'll be amazed at the number of helpful tips, recommendations, and action plans that come out of comprehensive readiness assessment, no question about it.

- **Quarterly Vulnerability Scans:** Both internal and external network scans are also mandated for PCI compliance, thus it's important to properly define scope, from an IP perspective, and also utilize tools and services that provide scanning on a regular basis, preferably on a monthly basis. Remember that a notable area of PCI compliance is passing quarterly scans, but it's important to run such scans prior to the quarterly deadline to ensure that any vulnerabilities have been identified, giving merchants much-needed time to correct any issues. While external scanning is relatively straightforward, internal scanning often proves challenging as vulnerabilities arise from outdated system and applications. It's therefore a good idea to patch all internal systems – possibly even purchasing a configuration management tool for helping pass internal mandated PCI DSS vulnerability scans.

- **Reach Out to an Expert**. Speaking with a Payment Card Industry Qualified Security Assessor (PCI-QSA) is a good idea, particularly when it comes to important scope and technical issues regarding PCI compliance. Remember also that the Self-Assessment Questionnaires (SAQ) can be challenging and confusing at times, so getting good advice and some straight-talk from a Payment Card Industry Qualified Security Assessor (PCI-QSA) is highly recommended, especially with all the changes in the PCI standards.

- **Choosing the Right Payment Processor.** Look for a payment processor or a provider of such services that is fully integrated – and PCI DSS compliant – that way merchants gain efficiencies of scale regarding PCI DSS compliance, along with added security enhancements from the provider themselves.

> "The bottom line is merchants should strive to avoid a breach at all costs, and utilizing services from proven providers, such as SiteLink, is a step in the right direction."

What Happens If There Is a Breach? Who's responsible?

Everyone is brought into scope if there is a breach, starting with the merchant, and all the way up to the major payment brands. It's not fun, and nobody wants to be breached. As a result, picking and choosing the right platform for securing and processing credit cards is now more important than ever. From the merchant banks to acquiring banks, and even the possible forensic investigative units from the major cardholder brands, everyone is truly involved. Fines and heavy penalties could possibly await merchants who suffer breaches, if they are found to be negligent, such as not being PCI DSS compliant, for starters. An advantage of using a platform, such as SiteLink's, means that many of its core components have undergone rigid compliance testing, ultimately helping ensure the safety and security of merchant cardholder data.

> "Fines and heavy penalties could possibly await merchants who suffer breaches, if they are found to be negligent, such as not being PCI DSS compliant, for starters."

The bottom line is merchants should strive to avoid a breach at all costs, and utilizing services from proven providers, such as SiteLink, is a step in the right direction.

Understanding PCI Requirements | What Is Involved?

What is PCI? What are the PCI compliance requirements for merchant service providers, and other organizations having a credible nexus with cardholder data?

Let's try and answer some of these questions, hopefully providing you with much-needed clarity regarding the Payment Card Industry Data Security Standards (PCI DSS) provisions.

PCI, according to the Payment Card Industry Security Standards Council, is the following:

> *"The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data"* (http://www.pcisecuritystandards.org/security_standards/pci_dss.shtml).

In simpler terms, PCI DSS is about ensuring the protection of cardholder data being stored, processed, and/or transmitted by merchant and service providers, and other affiliated entities. Stop and think about all the organizations that "touch" credit cards, and you can quickly see how widespread the adoption of PCI actually is. Name an industry or business sector, and chances are highly likely – almost certain – that PCI is a large and notable presence, one that requires constant effort and attention.

The actual PCI DSS requirements consist of what is known as twelve core requirements or mandates for protecting cardholder data. Within these twelve requirements are provisions for various policies, procedures, forms, etc. to be in place.

The Twelve PCI Requirements Include:

Build and Maintain a Secure Network

1: Install and maintain a firewall configuration to protect cardholder data.

2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3: Protect stored cardholder data.

4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

5: Use and regularly update anti-virus software.

6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7: Restrict access to cardholder data by business need-to-know.

8: Assign a unique ID to each person with computer access.

9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

10: Track and monitor all access to network resources and cardholder data.

11: Regularly test security systems and processes.

Maintain an Information Security Policy

12: Maintain a policy that addresses information security.

Policies, procedures, and processes - that's what PCI compliance is all about, so do what's needed to become compliant. In reviewing SiteLink's software and SiteLink

Merchant Services, it meets all of the security standards I like to see in a solution to help protect your business from a possible breach.

Click here to read "10 Easy Steps to PCI SAQ Certification," by Charles J. Denyer.

About Charles J. Denyer

Charles J. Denyer is one of North America's longest licensed Payment Card Industry Qualified Security Assessor (PCI-QSA), working with merchants and service providers all throughout the globe in achieving PCI DSS compliance efficiently, cost-effectively, and in a comprehensive manner. He is the recipient of numerous accounting and technology certifications along with a Masters in Information and Telecommunication Systems from Johns Hopkins University and a Masters in Nuclear Engineering from the University of Tennessee at Knoxville. His expertise includes information security, cyber security, national security and homeland defense, and he conducts independent research projects on specific subject matter for various entities. Charles can be contacted at cdenyer@ndbcpa.com or at 800-277-5415-ext.705