Charles J. Denyer, PCI-QSA | sitelink

PCI SAQ Certification Process in 10 Easy Steps

By Charles J. Denyer, PCI-QSA

PCI SAQ Compliance Certification Process in 10 Easy Steps

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

The following are steps for the Self-Assessment Questionnaires (SAQ) part of the PCI DSS (Payment Card Industry Data Security Standard) compliance certification process.

1. **Determine Appropriate Merchant and Service Provider Level.** Before you begin the PCI DSS compliance certification process for Self-Assessment Questionnaires (SAQ) A – D, P2PE-HW, please confirm that your transaction processing levels actually allow "self-assessing."

2. **Determine which Self-Assessment Questionnaire (SAQ) to use.** There are numerous PCI DSS Self-Assessment Questionnaires, specifically: SAQ A, SAQ B, SAQ C, SAQ C-VT, SAQ D, and SAQ P2PE-HW. Moreover, each one of these Self-Assessment Questionnaires (SAQ) contains numerous PCI DSS compliance requirements – some of which are considered relatively simple and straightforward (i.e., SAQ A), while others require a considerable amount of work to be done (i.e., SAQ C, SAQ C-VT, and D).

- **SAQ C for Merchants** (Merchants with payment application systems connected to the Internet, but with NO electronic Cardholder Data storage.)[1]
- **SAQ C-VT for Merchants** (Merchants using web-based virtual terminals, with NO electronic Cardholder Data storage.)[2]
- **SAQ D for Merchants and Service Providers** (for all other Merchants not included in the descriptions for SAQ A – C-VT, and for ALL service providers defined by a payment brand as being actually eligible to complete a Self-Assessment Questionnaire (SAQ), and the accompany Attestation of Compliance (AOC).[3]

Simply review the "Requirements for allowing Merchants" paragraph on each of the above sections to see if you in fact meet the stated requirements for utilizing the applicable questionnaire.

[1] SiteLink Note: This is what most Web Edition users would fill out as your data is encrypted and stored on SiteLink Servers.

[2] SiteLink Note: This would not typically be used by SiteLink Customer unless using the Virtual Terminal directly to process payments as the only payment method.

[3] SiteLink Note: This would be used for any software where the payment information is stored locally on your computer.

3. **Download the official SAQ Questionnaire and Attestation of Compliance (AoC).** The Payment Card Industry Security Standards Council (PCI SSC) is the official organization ultimately responsible for the development, management, education, and awareness of the PCI Security Standards. Their website, pcisecuritystandards.org, contains all essential PCI publications, including the actual SAQ Questionnaires and related forms. Simply visit the official PCI Security Standards Council website, and click on “PCI Standards & Documents”, then on the left-hand side, click on “Documents Library”, and finally, click on the“SAQs” tab, which is located on the top horizontal menu bar. When you arrive on this page, you’ll see a list of Self-Assessment Questionnaires, so simply pick the applicable SAQ and download the Microsoft Word document. Don’t forget that when you download the applicable SAQ document, also included is the “Attestation of Compliance” (AoC), which must eventually be completed (more on the AoC in a moment).

4. **Thoroughly Review the Applicable SAQ Questionnaire.** The PCI DSS compliance certification process for Self-Assessment Questionnaires now truly begins in earnest. Specifically, it’s time to thoroughly read whichever SAQ document you downloaded (A – D, or P2PE-HW) and begin to truly understand what’s needed for PCI compliance. Policies, procedures, and processes – that’s ultimately what PCI is all about – so it’s important that various personnel are assigned specific roles and responsibilities for assisting with compliance.

5. **Obtain PCI Policies and Procedures**. You’ll need assistance with PCI compliance, and that’s where we come in. Every one of the PCI Self-Assessment Questionnaires (SAQ), from A to D, and P2PE-HW, ultimately requires organizations to develop documented PCI policies and procedures for compliance. It’s a strict mandate.

6. **Get Compliant**. Policies, procedures, and processes - that’s what PCI compliance is all about, so do what’s needed to become compliant. Ultimately, this means reading the entire SAQ document, and doing exactly as it says, checking the boxes along the way (literally) as you’ve complete each step.

7. **Conduct Vulnerability Scans and Penetration Testing, if necessary.** Please note that your organization may have to undergo annual penetration tests and vulnerability scans for compliance, so please keep this in mind. For an ounce of clarity, just remember the following:

- PCI SAQ C - Vulnerability scans are required, but penetration tests are not.
- PCI SAQ C-VT - No vulnerability scans or penetration tests necessary
- PCI SAQ D - Vulnerability scans are required, along with penetration tests.

8. **Complete the Attestation of Compliance**. More commonly known as the AoC, this document was included within the actual Self-Assessment Questionnaire (SAQ) you downloaded, and it's to be completed once all the requirements for your applicable SAQ have been met. This document is often requested by payment processors, gateways, acquiring banks, customers, prospects and other interested parties wanting evidence of actual PCI DSS compliance and certification. Remember, the notion of "self-assessing" is easier said than done, as quite a bit of work can be involved, so be sure to seek out resources as necessary.

SiteLink Note: Steps 1-8 can be accomplish with SiteLink's new merchant services offering. We offer a portal that will step you through the PCI Process. Keep in mind it is a Card Brand (Visa, Mastercard, etc.) mandate that every merchant account is required to be PCI compliant. Ignoring this would be a liability to your business due to the possible PCI fines for not being compliant.

9. **Stay Compliant.** The Payment Card Industry Data Security Standards (PCI DSS) are a "moving target", something that organizations should be focusing on throughout the year. PCI compliance is a commitment that should never cease, so set aside the notion of "one and done."

10. **Practice What You Preach.** You've spent a considerable amount of time developing policies, procedures, and other standardized processes for PCI compliance, so follow them and stick to the best practices of information security!

Your software and processor selection play a role in your ability to meet the required PCI standards.

All merchant accounts are required to be PCI compliant. To ensure the highest level of security protection for credit card data it is important to understand how your software and payment processor handle data security.

Key considerations when reviewing software and payment processing providers

1) Select a software provider and merchant provider that is PCI Level 1 certified
2) All payment entities handling your account should be officially registered with Visa.
3) If possible, have a solution where you do not store the data locally. Solutions, like SiteLink, store the data encrypted for you in a secured data center. This simplifies your PCI compliance, as you are not storing credit card data locally.
4) Ensure that you complete PCI compliance for each of your merchant accounts.
5) Maintain PCI compliance annually

In reviewing SiteLink's software and SiteLink Merchant Services, they meet all of the security standards I like to see in a solution to help protect your business from a possible breach.

Click here for "The Payment Card Industry Data Security Standards (PCI DSS): A Comprehensive Overview," by Charles J. Denyer.

About Charles Denyer

Charles 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.