Document Changes

Date	Version	Description
October 1, 2008	1.2	To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 28, 2010	2.0	To align content with new PCI DSS v2.0 and clarify SAQ environment types and eligibility criteria. Addition of SAQ C-VT for Web-based Virtual Terminal merchants
June 2012	2.1	Addition of SAQ P2PE-HW for merchants who process cardholder data only via hardware payment terminals included in a validated and PCI SSC-listed PCI Point-to-Point Encryption (P2PE) solution. This document is for use with PCI DSS version 2.0.
April 2015	3.1	To align content with PCI DSS v3.1

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

About this Document

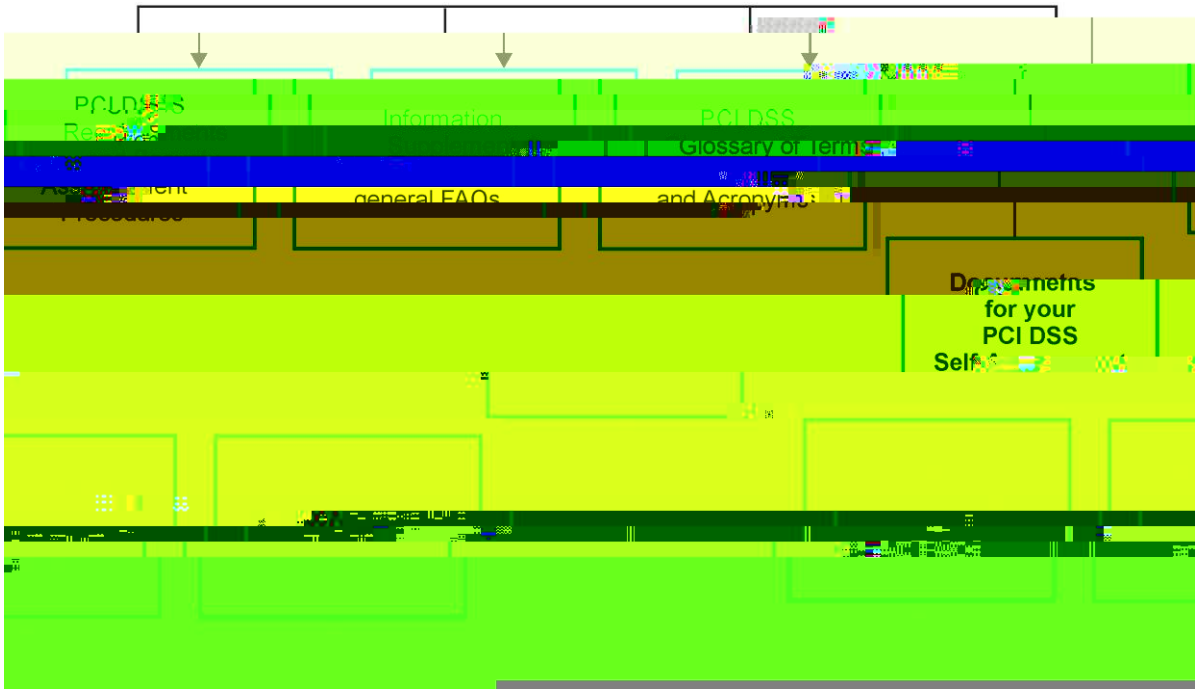
© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Self-Assessment: How it All Fits Together

The PCI DSS and supporting documents represent a common set of industry tools to help ensure the safe handling of cardholder data. The standard itself provides an actionable framework for developing a robust security process—including preventing, detecting, and reacting to security incidents. To reduce the risk of compromise and mitigate the impact if it does occur, it is important for all entities that store process, or transmit cardholder data to be compliant.

The chart below outlines the tools in place to help organizations with PCI DSS compliance and self-assessment.

These and other related documents can be found at www.pcisecuritystandards.org.



* *Note: Information Supplements provide supplemental information and guidance only, and do not replace or supersede any requirements in PCI DSS.*

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

SAQ Overview

The *PCI DSS Self-Assessment Questionnaires* (SAQs) are validation tools intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. There are multiple versions of the PCI DSS SAQs to meet various scenarios. This document has been developed to help your organization determine which SAQ(s) best applies to your environment.

The PCI DSS SAQ is a validation tool for merchants and service providers not required by their respective acquirers or payment brand(s) to submit a PCI DSS Report on Compliance (ROC). Please consult your acquirer or payment brand for details regarding PCI DSS validation requirements.

Each PCI DSS SAQ consists of the following components:

1. Questions correlating to the PCI DSS requirements, as appropriate for different environments: See “Selecting the SAQ and Attestation that Best Apply to Your Organization” in this document. This section also includes a column for “Expected Testing” which is based on the testing procedures in PCI DSS.
2. Attestation of Compliance: The Attestation includes your declaration of eligibility for completing the applicable SAQ and the subsequent results of a PCI DSS self-assessment.

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

Understanding the difference between compliance and security

It's important to recognize the difference between being compliant and being secure. Being compliant with PCI DSS at one point in time does not prevent things from changing in your environment, which—if the proper controls are not implemented—could impact your security. You should therefore ensure that PCI DSS controls continue to be implemented properly as part of business-as-usual (BAU) activities and as defined by your overall security strategy. This will enable you to monitor the effectiveness of your organization's security controls on an ongoing basis and maintain your PCI DSS compliant environment between PCI DSS assessments. Examples of how PCI DSS should be incorporated into BAU activities are provided in the "Implementing PCI DSS into Business-as-Usual Processes" section in the PCI DSS.

Additionally, the PCI DSS security requirements are intended for the protection of payment card data, and your organization may have other sensitive data and assets that need protecting which could be outside of the scope of PCI DSS. Therefore, while PCI DSS compliance, if properly maintained, can certainly contribute to overall security, it should not be viewed as a replacement for a robust, organization-wide security program.

General Tips and Strategies for PCI DSS Compliance

Following are some general tips and strategies for beginning your PCI DSS compliance efforts. These tips may help you eliminate storage of cardholder data you do not need, isolate the data you do need to defined and controlled centralized areas, and may allow you to limit the scope of your PCI DSS compliance validation effort. For example, by eliminating cardholder data that you don't need and/or isolating the data that you do need to defined and controlled areas, you can remove systems and networks that don't store, process, or transmit cardholder data—and that don't connect to systems that do—from the scope of your self-assessment.

1. **Sensitive Authentication Data (includes the full track contents of the magnetic stripe or equivalent data on a chip, card verification codes and values, PINs, and PIN blocks):**

   Make sure you ***never store this data*** after authorization:

2. **Ask your POS vendor about the security of your system, with the following suggested questions:**

   a. Have default settings and passwords been changed on the systems and databases that are part of the POS system?

   b. Do you access my POS system remotely? If so, have you implemented appropriate controls to prevent others from accessing my POS system, such as using secure remote access methods and not using common or default passwords? How often do you access my POS device remotely and why? Who is authorized to access my POS remotely?

   c. Have all unnecessary and insecure services been removed from the systems and databases that are part of the POS system?

   d. Is my POS software validated to the Payment Application Data Security Standard (PA-DSS)? (Refer to PCI SSC's list of Validated Payment Applications.)

   e. Does my POS software store sensitive authentication data

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

h. Does my POS software enforce complex and unique passwords for all user access?

i. Can you confirm that you do not use common or default passwords for access to my system and other merchant systems you support?

j. Have all the systems and databases that are part of the POS system been patched with all applicable security updates?

k. Is the logging capability turned on for the systems and databases that are part of the POS system?

l. If prior versions of my POS software stored sensitive authentication data, has this feature been removed during current updates to the POS software? Was a secure wipe utility used toature

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

c. Document each compensating control by completing a Compensating Controls Worksheet in Appendix B of the SAQ.

   A Compensating Controls Worksheet must be completed for each requirement that is met with a compensating control.

d. Submit all completed Compensating Controls Worksheets, along with your completed SAQ and/or Attestation of Compliance, according to instructions from your acquirer or payment brand.

6. Professional Assistance and Training

a. If you would like to engage a security professional for help with your self-assessment, we encourage you to consider contacting a Qualified Security Assessor (QSA). QSAs have been trained by PCI SSC to conduct PCI DSS assessments and are listed on the PCI SSC website.

b. The PCI SSC website is a primary source for additional resources, including:

   The *PCI DSS Glossary of Terms, Abbreviations and Acronyms*

   Frequently Asked Questions (FAQs)

   Webinars

   Information Supplements and Guidelines

   SAQ forms and Attestations of Compliance

Note: *Information Supplements complement the PCI DSS and identify additional considerations and recommendations for meeting PCI DSS requirements they do not change, eliminate, or supersede the PCI DSS or any of its requirements.*

c. PCI SSC also provides a number of training programs to help build awareness for an organization's personnel. Examples include PCI Awareness, the PCI Professional (PCIP) program, and the Internal Security Assessor (ISA) program.

   Please refer to www.pcisecuritystandards.org for more information.

d. Payment-related training programs and resources may also be available from the payment brands and/or your merchant acquirer.

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

Selecting the SAQ and Attestation that Best Apply to Your Organization

A

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

SAQ	Description
P2PE	Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce merchants.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete an SAQ.

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

SAQ B – Merchants with Only Imprint Machines or Only Standalone, Dial-Out Terminals. No Electronic Cardholder Data Storage

SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals.

SAQ B merchants may be either brick-and-mortar (card-present) or mail/telephone order (card-not-present) merchants, and do not store cardholder data on any computer system. SAQ B merchants will confirm that they meet the following eligibility criteria for this payment channel:

For a graphical guide to choosing your SAQ type,

Applies to My Envi on page 18.

Your company uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers' payment card information;

The standalone, dial-out terminals are not connected to any other systems within your environment;

The standalone, dial-out terminals are not connected to the Internet;

Your company does not transmit cardholder data over a network (either an internal network or the Internet);

Your company retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; **and**

Your company does not store cardholder data in electronic format.

This SAQ is not applicable to e-commerce channels.

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

SAQ B-IP – Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) terminals, No Electronic Cardholder Data Storage

SAQ B-IP has been developed to address requirements applicable to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction (POI) devices with an IP connection to the payment processor.

SAQ B-IP merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants, and do not store cardholder data on any computer system.

SAQ B-IP merchants will confirm that they meet the following eligibility criteria for this payment channel:

Your company uses only standalone, PTS-approved point-of-

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

11lTJETBT1 0 0 1 129.62 609.92 T48223083TJETBT1 0 0 1 19.34 634544 Tm5223083e4(ne)4(c)-5(ti)-5(on)-7(l)ed(on)21(e)-2(d TJEd8(m

SAQ C-VT – Merchants with Web-Based Virtual Terminals, No Electronic Cardholder Data Storage

SAQ C-VT has been developed to address requirements applicable to merchants who process cardholder data only via isolated virtual payment terminals on a personal computer connected to the Internet.

A virtual payment terminal is web-browser-based access to an acquirer, processor or third-party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Payment card transactions are entered manually.

SAQ C-VT merchants process cardholder data only via a virtual payment terminal and do not store cardholder data on any computer system.

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

SAQ P2PE – Merchants using Only Hardware Payment Terminals in a PCI SSC-listed P2PE Solution, No Electronic Cardholder Data Storage

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.