Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire

Instructions and Guidelines

Version 1.1

February 2008

Table of Contents

About this Document

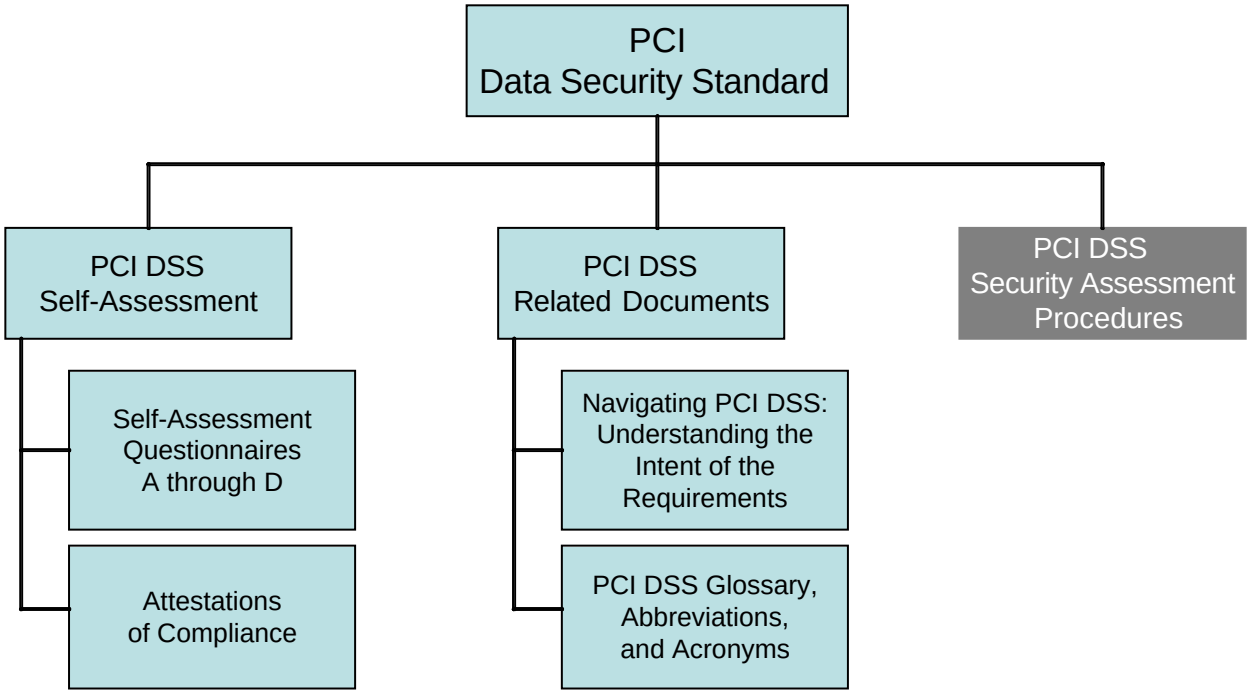
This document was developed to help merchants and service providers understand the PCI Data Security Standard (DSS) Self-Assessment Questionnaire (SAQ). Read this entire Instructions and Guidelines document to understand why PCI DSS is important to your organization, what strategies your organization can use to facilitate compliance validation, and whether your organization is eligible to complete one of the shorter SAQ versions. The following sections outline what you need to know about the PCI DSS SAQ.

- PCI Data Security Standard Self-Assessment: How it all fits together
- PCI Data Security Standard: Related Documents
- SAQ Overview
- Why is compliance with the PCI DSS important?
- General Tips and Strategies
- Selecting the SAQ That Best Applies to your organization
- Guidance for exclusion of certain, specific requirements
- How to Complete the Questionnaire

PCI Data Security Standard Self-Assessment: How it All Fits Together

The PCI Data Security Standard and supporting documents represent a common set of industry tools and measurements to help ensure the safe handling of sensitive information. The standard provides an actionable framework for developing a robust account data security process—including preventing, detecting and reacting to security incidents. To reduce the risk of compromise and mitigate its impacts if it does occur, it is important that all entities storing, processing, or transmitting cardholder data 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.



PCI Data Security Standard: Related Documents

The following documents were created to assist merchants and service providers in understanding the PCI Data Security Standard and the PCI DSS SAQ.

Document	Audience
PCI Data Security Standard	All merchants and service providers
Navigating PCI DSS: Understanding the Intent of the Requirements	All merchants and service providers
PCI Data Security Standard: Self-Assessment Guidelines and Instructions	All merchants and service providers
PCI Data Security Standard: Self-Assessment Questionnaire A and Attestation	Merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation	Merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation	Merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation	Service providers and all other merchants[1]
PCI Data Security Standard Glossary, Abbreviations, and Acronyms	All merchants and service providers

[1] To determine the appropriate Self-Assessment Questionnaire, see *PCI Data Security Standard: Self-Assessment Guidelines and Instructions*, "Selecting the SAQ and Attestation That Best Apply To Your Organization."

SAQ Overview

The PCI Data Security Standard Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard (PCI DSS). There are multiple versions of the PCI DSS SAQ to meet various scenarios. This document has been developed to help organizations determine which SAQ best applies to them.

The PCI DSS SAQ is a validation tool for merchants and service providers not required to undergo an on-site data security assessment per the PCI DSS Security Assessment Procedures, and may be required by your acquirer or payment brand. Please consult your acquirer or payment brand for details regarding PCI DSS validation requirements.

The PCI DSS SAQ consists of the following components:

1. Questions correlating to the PCI DSS requirements, appropriate for service providers and merchants: See "Selecting the SAQ and Attestation that Best Apply to Your Organization" in this document.
2. Attestation of Compliance: The Attestation is your certification that you are eligible to perform and have performed the appropriate Self-Assessment.

Why Is Compliance With PCI DSS Important?

The members of PCI Security Standards Council (American Express, Discover, JCB International, MasterCard, and Visa Inc.) continually monitor cases of account data compromise. These compromises cover the full spectrum of organizations, from the very small to very large merchants and service providers.

A security breach and subsequent compromise of payment card data has far-reaching consequences for affected organizations, including:

1. Regulatory notification requirements,
2. Loss of reputation,
3. Loss of customers,
4. Potential financial liabilities (e.g., regulatory and other fees and fines), and
5. Litigation.

Post-mortem compromise analysis has shown common security weaknesses that are addressed by PCI DSS, but were not in place in the organizations when the compromises occurred. PCI DSS was designed and includes detailed requirements for exactly this reason—to minimize the chance of compromise and the effects if a compromise does occur.

Investigations after compromises consistently show common PCI DSS violations, including but not limited to:

- Storage of magnetic stripe data (Requirement 3.2). It is important to note that many compromised entities are unaware that their systems are storing this data.
- Inadequate access controls due to improperly installed merchant POS systems, allowing hackers in via paths intended for POS vendors (Requirements 7.1, 7.2, 8.2 and 8.3)
- Default system settings and passwords not changed when system was set up (Requirement 2.1)
- Unnecessary and vulnerable services not removed or fixed when system was set up (Requirement 2.2.2)
- Poorly coded web applications resulting in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the web site (Requirement 6.5)
- Missing and outdated security patches (Requirement 6.1)
- Lack of logging (Requirement 10)
- Lack of monitoring (via log reviews, intrusion detection/prevention, quarterly vulnerability scans, and file integrity monitoring systems) (Requirements 10.6, 11.2, 11.4 and 11.5)
- Lack of segmentation in a network, making cardholder data easily accessible through weaknesses in other parts of the network (e.g., from wireless access points, employee e-mail, and web browsing) (Requirements 1.3 and 1.4)

General Tips and Strategies to Prepare for Compliance Validation

Following are some general tips and strategies for beginning your PCI DSS compliance validation efforts. These tips may help you eliminate 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 data that you do not need and/or isolating that data to defined and controlled areas, you can eliminate those systems and networks that no longer store, process, or transmit cardholder data from the scope of your self-assessment.

1. **Sensitive Authentication Data (includes the full contents of the magnetic stripe, card validation codes and values, and PIN blocks):**
   a. Make sure you ***never store this data.***
   b. If you don't know for sure, ask your POS vendor whether the software product and version you use stores this data. Alternatively, consider hiring a Qualified Security Assessor that can assist you in determining whether sensitive authentication is being stored, logged, or captured anywhere in your systems.

2. **If you are a merchant, ask your POS vendor about the security of your system, with the following suggested questions:**
   a. Does my POS software store magnetic-stripe data (track data) or PIN blocks? If so, this storage is prohibited, so how quickly can you help me remove it?
   b. Will you document the list of files written by the application with a summary of the content of each file, to verify that the above-mentioned, prohibited data is not stored?
   c. Does your POS system require me to install a firewall to protect my systems from unauthorized access?
   d. Are complex and unique passwords required to access my systems? Can you confirm that you do not use common or default passwords for mine as well as other merchant systems you support?
   e. Have default settings and passwords been changed on the systems and databases that are part of the POS system?
   f. Have all unnecessary and insecure services been removed from the systems and databases that are part of the POS system?
   g. 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?
   h. Have all the systems and databases that are part of the POS system been patched with all applicable security updates?
   i. Is the logging capability turned on for the systems and databases that are part of the POS system?
   j. If prior versions of my POS software stored track data, has this feature been removed during current updates to the POS software? Was a secure wipe utility used to remove this data?

3. **Cardholder data—if you don't need it, don't store it!**

   a. Payment brand rules allow for the storage of Personal Account Number (PAN), expiration date, cardholder name, and service code.

   b. Take inventory of all the reasons and places you store this data. If the data doesn't serve a valuable business purpose, consider eliminating it.

   c. Think about whether the storage of that data and the business process it supports are worth the following:

      i. The risk of having the data compromised.

      ii. The additional PCI DSS efforts that must be applied to protect that data.

      iii. The ongoing maintenance efforts to remain PCI DSS compliant over time.

4. **Cardholder data—if you do need it, consolidate and isolate it.**

   a. You can limit the scope of a PCI DSS assessment by consolidating data storage in a defined environment and isolating the data through the use of proper network segmentation. For example, if your employees browse the Internet and receive e-mail on the same machine or network segment as cardholder data, consider segmenting (isolating) the cardholder data onto its own machine or network segment (via routers or firewalls). If you can isolate the cardholder data effectively, you may be able to focus your PCI DSS efforts on just the isolated part rather than including all your machines.

5. **Consider Compensating Controls (applicable to SAQ D only)**

   a. Compensating controls may be considered for most PCI DSS requirements when an organization cannot meet the technical specification of a requirement, but has sufficiently mitigated the associated risk. If your company does not have the exact control specified in PCI DSS but has other controls in place that satisfy the PCI DSS definition of compensating controls (see the Appendix to SAQ D and the *PCI DSS Glossary, Abbreviations, and Acronyms* document at www.pcisecuritystandards.org), your company should do the following:

      i. In the compensating controls column of the SAQ, note the use of each compensating control used to satisfy a requirement.

      ii. Review "Compensating Controls" in the Appendix, and document the use of compensating controls by completing the Compensating Controls Worksheet.

         a) Complete a Compensating Controls Worksheet for each requirement that is met with a compensating control.

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

6. **Professional Assistance**

   a. If you would like to have a security professional's guidance to achieve compliance and complete the SAQ, you are encouraged to do so. Please recognize that, while you are free to use any security professional of your choosing, only those included on PCI SSC's list of Qualified Security Assessors (QSAs) are recognized as QSAs and are trained by PCI SSC. This list is available at https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm.

Selecting the SAQ and Attestation That Best Apply to Your Organization

According to payment brand rules, all merchants and service providers are required to comply with the PCI Data Security Standard in its entirety. There are five SAQ Validation categories, shown briefly in the table below and described in more detail in the following paragraphs. Use the table to gauge which SAQ applies to your organization, then review the detailed descriptions to ensure you meet all the requirements for that SAQ.

SAQ Validation Type	Description	SAQ
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. *This would never apply to face-to-face merchants.*	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Stand-alone dial-up terminal merchants, no electronic cardholder data storage	B
4	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (not included in descriptions for SAQs A-C above) and **all** service providers defined by a payment brand as eligible to complete an SAQ.	D

SAQ Validation Type 1 / SAQ A: Card-not-present, All Cardholder Data Functions Outsourced

SAQ A has been developed to address requirements applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises.

For a graphical guide to choosing your validation type, please see "SAQ Instructions and Guidelines—What is my Validation Type" on page 12.

Merchants in Validation Type 1 do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises, and must validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that**:**

- Your company handles only card-not-present (e-commerce or mail/telephone-order) transactions;
- Your company does not store, process, or transmit any cardholder data on your premises, but relies entirely on a third party to handle these functions;
- Your company has confirmed that the third party handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant;
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically; **and**
- Your company does not store any cardholder data in electronic format.

This option would never apply to merchants with a face-to-face POS environment.

SAQ Validation Type 2 / SAQ B: Imprint Merchant Only, 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 stand-alone dial-up terminals.

Merchants in Validation Type 2 only process cardholder data via imprint machines, and must validate compliance by completing SAQ B and the associated Attestation of Compliance, confirming that:

- Your company uses only an imprint machine to take your customers' payment card information;
- Your company does not transmit cardholder data over either a phone line or the Internet;
- Your company retains only paper copies of receipts; and
- Your company does not store cardholder data in electronic format.

For a graphical guide to choosing your validation type, please see "SAQ Instructions and Guidelines—What is my Validation Type" on page 12.

SAQ Validation Type 3 / SAQ B: Standalone, Dial-out Terminal Merchant, 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 stand-alone dial-up terminals.

Merchants in Validation Type 3 process cardholder data via stand-alone, dial-out terminals, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone order (card-not-present) merchants. Merchants in Validation Type 3 must validate compliance by completing SAQ B and the associated Attestation of Compliance, confirming that:

- Your company uses only standalone, dial-out terminals (connected via a phone line to your processor);
- 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 retains only paper reports or paper copies of receipts; and
- Your company does not store cardholder data in electronic format.

SAQ Validation Type 4 / SAQ C: Merchants with Payment Application Systems Connected to the Internet

SAQ C has been developed to address requirements applicable to merchants whose payment application systems (for example, point-of-sale or shopping cart systems) are connected to the Internet (via high-speed connection, DSL, cable modem, etc.) either because:

1. The payment application system is on a personal computer that is connected to the Internet (for example, for email or web browsing), or
2. The payment application system is connected to the Internet to transmit cardholder data.

Merchants in Validation Type 4 process cardholder data via payment application systems connected to the Internet, do not store cardholder data on any computer system, and may be either brick-and-mortar

(card-present) or e-commerce or mail/telephone-order (card-not-present) merchants. Merchants in Validation Type 4 must validate compliance by completing SAQ C and the associated Attestation of Compliance, confirming that:

- Your company has a payment application system and an Internet connection on the same device;
- The payment application system/Internet device is not connected to any other systems within your environment;
- Your company retains only paper reports or paper copies of receipts;
- Your company does not store cardholder data in electronic format; and
- Your company's payment application software vendor uses secure techniques to provide remote support to your payment application system.

For a graphical guide to choosing your validation type, please see "SAQ Instructions and Guidelines—What is my Validation Type" on page 12.

SAQ Validation Type 5 / SAQ D: All Other Merchants and All Service Providers Defined by a Payment Brand as Eligible to Complete an SAQ

SAQ D has been developed to address requirements applicable to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under Validation Types 1-4 above.

Service providers and merchants in Validation Type 5 must validate compliance by completing SAQ D and the associated Attestation of Compliance.

While many of the organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to wireless technology. See the guidance below for information about the exclusion of wireless technology and certain other, specific requirements.

Guidance for Exclusion of Certain, Specific Requirements

If you are required to answer SAQ D to validate your PCI DSS compliance, the following exceptions may be considered (you may mark these requirements N/A if they are not applicable to your environment):

- The questions specific to wireless only need to be answered if wireless is present anywhere in your network (Requirements 1.3.8, 2.1.1, and 4.1.1). Note that Requirement 11.1 (use of wireless analyzer) must still be answered even if wireless is not in your network, since the analyzer detects any rogue or unauthorized devices that may have been added without your knowledge.
- The questions specific to custom applications and code (Requirements 6.3-6.5) only need to be answered if your organization writes its own custom web applications.
- The questions specific to data centers (Requirements 9.1-9.4), only need to be answered if you have a dedicated data center or server room. A data center is defined by PCI SSC as a dedicated, physically secure room or structure where information technology infrastructure (application servers, database servers, web servers, and/or network devices) is centrally housed, whose main purpose is to store, process, or transmit cardholder data. "Data center" may be synonymous with server room, network operations center (NOC), and co-location facilities at an ISP or hosting provider.

Instructions for Completing the SAQ

1. Use the guidelines herein to determine which SAQ is appropriate for your company.
2. Use *Navigating PCI DSS: Understanding the Intent of the Requirements* to understand how and why the requirements are relevant to your organization.
3. Use the appropriate Self Assessment Questionnaire as a tool to validate compliance with the PCI DSS.
4. Follow the instructions in the appropriate Self-Assessment Questionnaire at PCI DSS Compliance – Completion Steps, and provide all required documentation to your acquirer or payment brand as appropriate.

SAQ Instructions and Guidelines—What is My Validation Type?