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

## Instructions and Guidelines

**Version 2.0**

October 2010

## 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.<br>Addition of SAQ C-VT for Web-based Virtual Terminal merchants |

# Table of Contents

## About this Document

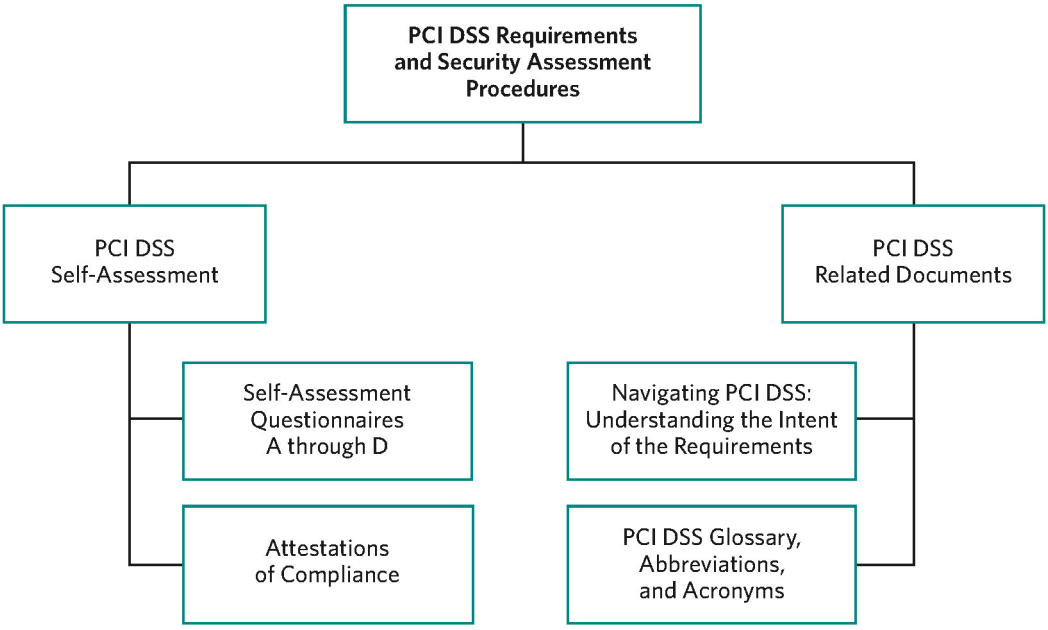
This document was developed to help merchants and service providers understand the Payment Card Industry Data Security Standard (PCI DSS) Self-Assessment Questionnaire (SAQ). Read this entire Instructions and Guidelines document to understand why PCI DSS is important to your organization, what strategies 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 DSS Self-Assessment: How it All Fits Together
- PCI DSS: Related Documents
- SAQ Overview
- Why is Compliance with PCI DSS Important?
- General Tips and Strategies to Prepare for Compliance Validation
- Selecting the SAQ and Attestation that Best Apply to your Organization
- Guidance for Non-Applicability of Certain, Specific Requirements
- Instructions for Completing the SAQ
- Which SAQ Best Applies to My Environment?

## PCI DSS Self-Assessment: How it All Fits Together

The PCI DSS 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 DSS and the PCI DSS SAQ.

| Document | Audience |
|---|---|
| *PCI Data Security Standard: Requirements and Security Assessment Procedures* | 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* | Eligible merchants[1] |
| *PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation* | Eligible merchants[1] |
| *PCI Data Security Standard: Self-Assessment Questionnaire C-VT and Attestation* | Eligible merchants[1] |
| *PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation* | Eligible merchants[1] |
| *PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation* | Eligible merchants and service providers[1] |
| *PCI Data Security Standard and Payment Application Data Security Standard: Glossary of Terms, Abbreviations, and Acronyms* | All merchants and service providers |

[1] To determine the appropriate Self-Assessment Questionnaire, see "Selecting the SAQ and Attestation That Best Apply to Your Organization," on page 12 of this document.

## SAQ Overview

The *PCI DSS Self-Assessment Questionnaire* (SAQ) 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 submit an on-site data security assessment Report on Compliance (ROC) per the *PCI DSS Requirements and Security Assessment Procedures,* and as 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 self-certification that you are eligible to perform and have actually performed a PCI DSS self-assessment.

## Why Is Compliance with PCI DSS Important?

The members of PCI Security Standards Council (American Express, Discover, JCB, MasterCard, and Visa) 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 (for example, 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 malicious users 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 insecure services not removed or secured when system was set up (Requirements 2.2.2 and 2.2.4)
- 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)
- Poorly implemented network segmentation resulting in the cardholder data environment being unknowingly exposed to weaknesses in other parts of the network that have not been secured according to PCI DSS (for example, from unsecured wireless access points and vulnerabilities introduced via employee e-mail and web browsing) (Requirements 1.2, 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 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 chip, card verification codes and values, PINs 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 data 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. Is my POS software validated to the Payment Application Data Security Standard (PA-DSS)? (Refer to PCI SSC's list of Validated Payment Applications.)
   b. 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?
   c. Does my POS software store primary account numbers (PANs)? If so, this storage must be protected, so how is the POS protecting this data?
   d. 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?
   e. Does your POS system require me to install a firewall to protect my systems from unauthorized access?
   f. 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?
   g. Have default settings and passwords been changed on the systems and databases that are part of the POS system?
   h. Have all unnecessary and insecure services been removed from the systems and databases that are part of the POS system?
   i. 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?
   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 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.**

   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 (for example, 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. **Compensating Controls**

   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 through alternative controls. 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 "Compensating Controls" in your applicable SAQ Appendix and the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* document at www.pcisecuritystandards.org), your company should do the following:

   a. Respond to the SAQ question as "YES" and in the "Special" column, note the use of each compensating control used to satisfy a requirement.

   b. Review "Compensating Controls" in Appendix B of the applicable SAQ, and document the use of compensating controls by completing the Compensating Controls Worksheet in Appendix C of the SAQ.

   c. Complete a Compensating Controls Worksheet 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, according to instructions from your acquirer or payment brand.

## 6. Professional Assistance and Training

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.

b. The PCI Security Standards Council (SSC) provides a variety of educational resources to further security awareness within the payment card industry. These resources include PCI DSS training for Internal Security Assessors (ISAs) and Standards Training. The PCI SSC website is also a primary source for additional resources, including:

- The *Navigating PCI DSS* Guide
- The *PCI DSS Glossary of Terms, Abbreviations and Acronyms*
- Frequently Asked Questions (FAQs)
- Webinars
- Information Supplements and Guidelines
- Attestations of Compliance

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

***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.*

## 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 DSS in its entirety. There are five SAQ 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 | Description |
|---|---|
| A | Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. *This would never apply to face-to-face merchants.* |
| B | Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage |
| C-VT | Merchants using only web-based virtual terminals, no electronic cardholder data storage |
| C | Merchants with payment application systems connected to the Internet, no electronic cardholder data storage |
| D | All other merchants not included in descriptions for SAQ types A through C above, and **all service providers** defined by a payment brand as eligible to complete an SAQ. |

### SAQ A – Card-not-present Merchants, 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 systems or premises.*

*For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page17.*

SAQ A merchants do not store cardholder data in electronic format, do not process or transmit any cardholder data on their systems or premises, and validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- Your company does not store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that the third party(s) 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 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 only process cardholder data via imprint machines or via standalone, dial-out terminals, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone order (card-not-present) merchants. Such merchants validate compliance by completing SAQ B and the associated Attestation of Compliance, confirming that:

*For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 17.*

- 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.

## 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 terminals on personal computers connected to the Internet.*

A virtual 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 terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.

*For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment" on page 17.*

These merchants process cardholder data only via a virtual terminal and do not store cardholder data on any computer system. These virtual terminals are connected to the Internet to access a third party that hosts the virtual terminal payment processing function. This third party may be a processor, acquirer, or other third-party service provider who stores, processes, and/or transmits cardholder data to authorize and/or settle merchants' virtual terminal payment transactions.

This SAQ option is intended to apply only to merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution.

SAQ C-VT merchants process cardholder data via virtual terminals on personal computers connected to the Internet, do not store cardholder data on any computer system, and may be brick-and-mortar

(card-present) or mail/telephone-order (card-not-present) merchants. Such merchants validate compliance by completing SAQ C-VT and the associated Attestation of Compliance, confirming that:

- Your company's only payment processing is done via a virtual terminal accessed by an Internet-connected web browser;
- Your company's virtual terminal solution is provided and hosted by a PCI DSS validated third-party service provider;
- Your company accesses the PCI DSS compliant virtual terminal solution via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems);
- Your company's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward);
- Your company's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached);
- Your company does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
- Your company retains only paper reports or paper copies of receipts; **and**
- Your company does not store cardholder data in electronic format.

**This option would never apply to e-commerce merchants.**

## SAQ C – Merchants with Payment Application Systems Connected to the Internet, No Electronic Cardholder Data Storage

*SAQ C has been developed to address requirements applicable to merchants whose payment application systems (for example, point-of-sale systems) are connected to the Internet (for example, via 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 e-mail or web browsing), or*
2. *The payment application system is connected to the Internet to transmit cardholder data.*

*For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 17.*

SAQ C merchants process cardholder data via POS machines or other 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. SAQ C merchants 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 and/or same local area network (LAN);
- The payment application system/Internet device is not connected to any other systems within your environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems);
- Your company store is not connected to other store locations, and any LAN is for a single store only;

- 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.

## 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 for all service providers defined by a payment brand as eligible to complete an SAQ, as well as SAQ-eligible merchants who do not meet the descriptions of SAQ types A through C, above.*

SAQ D service providers and merchants 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 managing wireless technology. See the guidance below for information about the exclusion of wireless technology and certain other, specific requirements.

## Guidance for Non-Applicability of Certain, Specific Requirements

**Exclusion:** If you are required to answer SAQ C or D to validate your PCI DSS compliance, the following exceptions may be considered. See "Non-Applicability" below for the appropriate SAQ response.

- Requirements 1.2.3, 2.1.1 and 4.1.1 (SAQs C and D): These questions specific to wireless only need to be answered if wireless is present anywhere in your network. Note that Requirement 11.1 (use of a process to identify unauthorized wireless access points) must still be answered even if wireless is not in your network, since the process detects any rogue or unauthorized devices that may have been added without your knowledge.
- Requirements 6.3 and 6.5 (SAQ D): These questions are specific to custom applications and code, and only need to be answered if your organization develops its own custom applications.
- Requirements 9.1 through 9.4 (SAQ D): These questions only need to be answered for facilities with "sensitive areas" as defined here. "Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store, but does include retail store back-office server rooms that store cardholder data, and storage areas for large quantities of cardholder data.

**Non-Applicability:** For all SAQs, these and any other requirements deemed not applicable to your environment must be indicated with "N/A" in the "Special" column of the SAQ. Accordingly, complete the "Explanation of Non-Applicability" worksheet in the SAQ Appendix for each "N/A" entry.

## 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. Assess your environment for compliance with the PCI DSS.
4. Use the appropriate Self Assessment Questionnaire as a tool to validate compliance with the PCI DSS.
5. 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.

## Which SAQ Best Applies to My Environment?