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

Instructions and Guidelines

Version 3.1

April 2015

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, including addition of SAQs A-EP and B-IP, and clarify eligibility criteria for existing SAQs.

Table of Contents

About this Document

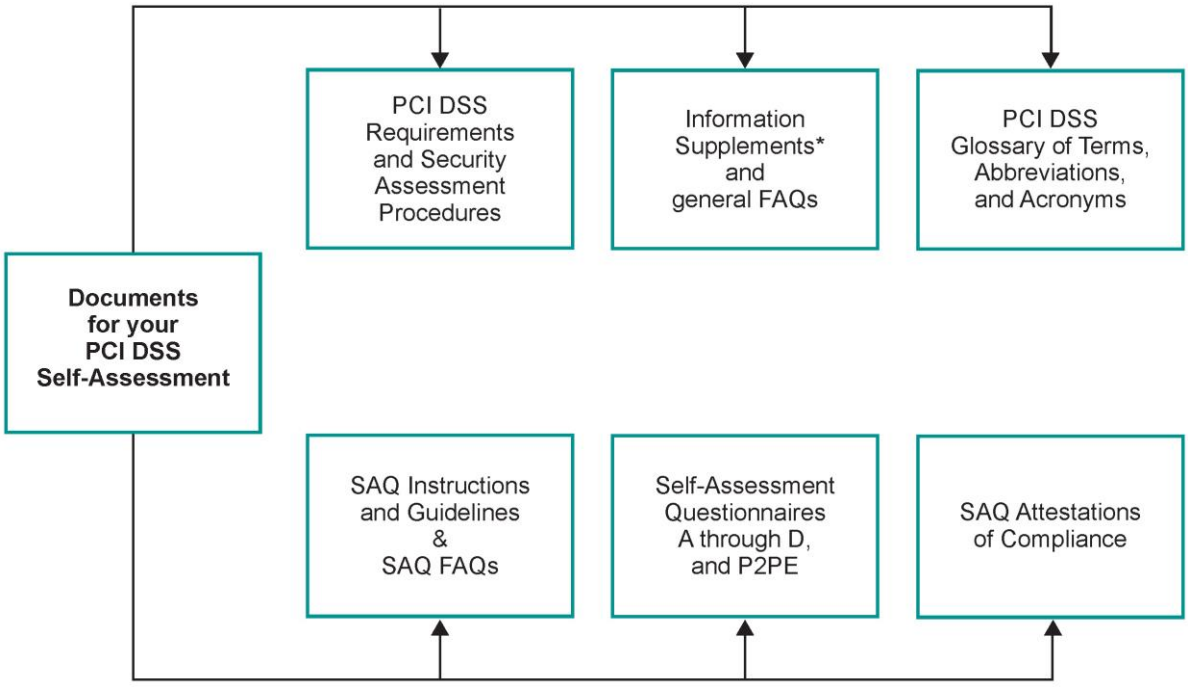
This document was developed to help merchants and service providers understand the Payment Card Industry Data Security Standard (PCI DSS) Self-Assessment Questionnaires (SAQs). In order to understand why PCI DSS is important to your organization, what strategies your organization can use to facilitate PCI DSS compliance validation, and whether your organization is eligible to complete one of the shorter SAQs, we recommend that you review this Instructions and Guidelines document in its entirety

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.*

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.

Why PCI DSS is Important

The members of the PCI Security Standards Council (American Express, Discover, JCB, MasterCard, and Visa) continually monitor occurrences of account data compromise. These compromises cover the full spectrum of organizations, from 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.

Forensic analysis of compromises has shown that common security weaknesses, which are addressed by PCI DSS controls, are often exploited because the PCI DSS controls either were not in place or were poorly implemented when the compromise 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.

Examples of common PCI DSS control failures include, but are not limited to:

- Storage of sensitive authentication data (SAD), such as track data, after authorization (Requirement 3.2). Many compromised entities were unaware that their systems were storing this data.
- Inadequate access controls due to improperly installed point-of-sale (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 the system was installed (Requirement 2.1).
- Unnecessary and insecure services not removed or secured when the system was installed (Requirements 2.2.2 and 2.2.3).
- Poorly coded web applications resulting in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the website (Requirement 6.5).
- Missing and outdated security patches (Requirement 6.2).
- 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).
- Poor scoping decisions—for example, excluding part of the network from PCI DSS scope due to inadequate network segmentation that was not verified to be effective. This results 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).

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, such as track data or PIN blocks? If so, this storage is prohibited: how quickly can you help me remove it?

   f. Does my POS software store primary account numbers (PANs)? If so, this storage must be protected: how is the POS protecting this data?

   g. Will you document the list of files written by the application with a summary of each file's contents to verify that the above-mentioned, prohibited data is not stored?

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 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 primary 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 legitimate 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 controls 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 organization 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 PCI DSS Appendix B, and also in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*), your organization should do the following:

a. Follow the procedures for compensating controls as outlined in PCI DSS Appendix B.

b. For all requirements that were met with the assistance of a compensating control, respond to the SAQ question by checking the "YES with CCW" column.

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

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.

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.*

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

Selecting the SAQ and Attestation that Best Apply to Your Organization

All merchants and service providers are required to comply with the PCI DSS as applicable to their environments at all times. There are a number of SAQ types, shown briefly in the table below and described in more detail in the following pages. Use the table to help determine which SAQ applies to your organization, and then review the detailed descriptions to ensure you meet all the requirements for that SAQ.

Note for all SAQs except SAQ D: These SAQs include questions that apply to a specific type of merchant environment, as defined in the related SAQ eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in a given SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No storage, processing, or transmission of cardholder data on merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: ▪ Imprint machines with no electronic cardholder data storage, and/or ▪ Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*

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.

SAQ A – Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced

SAQ A has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced to validated third parties, where the merchant retains only paper reports or receipts with cardholder data.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 18.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present) and do not store, process, or transmit any cardholder data in electronic format on their systems or premises.

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

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
- Your company does not electronically 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 all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of all payment pages delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

This SAQ is not applicable to face-to-face channels.

SAQ A-EP – Partially Outsourced E-Commerce Merchants Using a Third-Party Website for Payment Processing

SAQ A-EP has been developed to address requirements applicable to e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data.

SAQ A-EP merchants are e-commerce merchants who partially outsource their e-commerce payment channel to PCI DSS validated third parties and do not electronically store, 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 page 18.

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

- Your company accepts only e-commerce transactions;
- All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
- Your e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
- If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
- Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
- Your company does not electronically 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 all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

This SAQ is applicable only to e-commerce channels.

Note: *For the purposes of SAQ A-EP, PCI DSS requirements that refer to the "cardholder data environment" are applicable to the merchant website(s). This is because the merchant website directly impacts how the payment card data is transmitted, even though the website itself does not receive cardholder data.*

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, please see "Which SAQ Best Applies to My Environment?" 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.

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.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 18.

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-interaction (POI) devices (excludes SCRs) connected via IP to your payment processor to take your customers' payment card information;
- The standalone, IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs);
- The standalone, IP-connected POI devices are not connected to any other systems within your environment (this can be achieved via network segmentation to isolate POI devices from other systems);
- The only transmission of cardholder data is from the PTS-approved POI devices to the payment processor;
- The POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor;
- 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.

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.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment" on page 18.

SAQ C-VT merchants process cardholder data only via a virtual payment 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 may be brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants.

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

- Your company's only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser;
- Your company's virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider;
- Your company accesses the PCI DSS-compliant virtual payment 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 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.

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.).

SAQ C merchants process cardholder data via a point-of-sale (POS) system 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.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 18.

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

- 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);
- The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single store only;
- Your company retains only paper reports or paper copies of receipts, 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.

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

SAQ P2PE has been developed to address requirements applicable to merchants who process cardholder data only via payment terminals included in a validated and PCI SSC-listed Point-to-Point Encryption (P2PE) solution.

SAQ P2PE merchants do not have access to clear-text account data on any computer system, and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution. SAQ P2PE merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive cardholder data on paper or over a telephone, and key it directly and only into a P2PE validated hardware device.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 18.

SAQ P2PE merchants will confirm that they meet the following eligibility criteria for this payment channel:

- All payment processing is via a validated PCI P2PE solution approved and listed by the PCI SSC;
- The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices which are approved for use with the validated and PCI-listed P2PE solution;
- Your company does not otherwise receive or transmit cardholder data electronically.
- There is no legacy storage of electronic cardholder data in the environment;
- If your company stores cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically; **and**
- Your company has implemented all controls in the *P2PE Instruction Manual (PIM)* provided by the P2PE Solution Provider.

This SAQ is not applicable to e-commerce channels.

SAQ D for Merchants – All Other SAQ-Eligible Merchants

SAQ D for Merchants applies to SAQ-eligible merchants not meeting the criteria for any other SAQ type.

Examples of merchant environments that would use SAQ D may include but are not limited to:

- E-commerce merchants who accept cardholder data on their website;
- Merchants with electronic storage of cardholder data;
- Merchants that don't store cardholder data electronically but that do not meet the criteria of another SAQ type;
- Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 18.

SAQ D for Service Providers – SAQ-Eligible Service Providers

SAQ D for Service Providers applies to all service providers defined by a payment brand as being SAQ-eligible.

Note for SAQ D for Merchants and SAQ D for Service Providers: While many 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 specific guidance in the respective SAQ D for information about the exclusion of other, specific requirements.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on page 18.

Which SAQ Best Applies to My Environment?