Payment Card Industry Data Security Standard

Self-Assessment Questionnaire Instructions and Guidelines

Version 4.0

September 2023

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.
May 2016	3.2	Updated to align with PCI DSS v3.2 and clarify eligibility criteria for existing SAQs.
June 2018	3.2.1	Minor updates to align with PCI DSS v3.2.1.
September 2023	4.0	Updated to align content with PCI DSS v4.0, clarify eligibility criteria for existing SAQs, incorporate content from *Understanding SAQs for PCI DSS v3.0*, and include the addition of SAQ SPoC.

Contents

About this Document

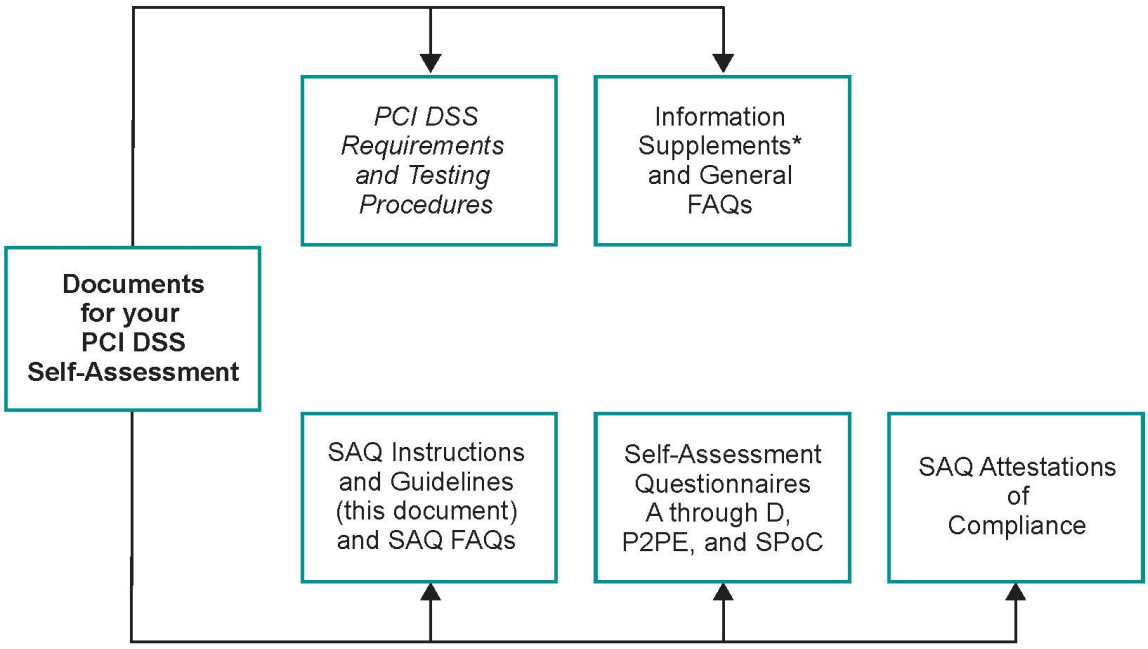
This document was developed to help merchants and service providers understand the Payment Card Industry Data Security Standard (PCI DSS) Self-Assessment Questionnaires (SAQs). To understand the SAQs, which strategies your organization can use to facilitate the completion of a PCI DSS SAQ, and which SAQ your organization is eligible to complete, we recommend that you review this Instructions and Guidelines document in its entirety.

PCI DSS Self-Assessment: How it All Fits Together

PCI DSS and its supporting documents represent a common set of industry tools to help ensure the safe handling of cardholder account 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 account data to protect that data by implementing applicable PCI DSS requirements.

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

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 for use by SAQ-eligible merchants and service providers in performing and reporting the results of their PCI DSS self-assessment. There are multiple versions of the PCI DSS SAQs to meet various merchant scenarios. This document has been developed to help SAQ-eligible organizations determine which SAQ(s) best applies to their environments.

The PCI DSS SAQs are alternate validation tools for merchants and service providers that are not required by an acquirer or payment brand(s) to submit a PCI DSS Report on Compliance (ROC). Being "SAQ-eligible" means that the merchant or service provider:

- Is eligible to conduct self-assessments to validate their PCI DSS compliance, according to payment brand compliance programs,
- Meets the SAQ Eligibility Criteria specified in the chosen SAQ.

Organizations are responsible to confirm they meet all eligibility criteria for a particular SAQ before commencing their self-assessment.

Note: *All entities completing SAQs are encouraged to contact the organizations that manage compliance programs and to which the SAQ will be submitted—for example, an acquirer (merchant bank) or the payment brands—to confirm they are eligible to complete an SAQ to validate PCI DSS compliance, and to understand any specific requirements or instructions*.

Each PCI DSS SAQ consists of the following sections:

1. Completing the Self-Assessment Questionnaire: This section includes the eligibility criteria for that specific SAQ, along with completion instructions and guidance to assist with the self-assessment process. See "Selecting the SAQ and Attestation that Best Apply to Your Organization" in this document for the eligibility criteria for each SAQ.

   In addition, each SAQ includes Self-Assessment Completion Steps, Expected Testing activities, Requirement Responses options, Guidance for Not Applicable Requirements, use of Legal Exception, and Additional PCI SSC Resources.

2. Attestation of Compliance: The Attestation is the entity's declaration of eligibility to complete the applicable SAQ and their attestation to the results of a PCI DSS self-assessment. The Attestation of Compliance in each SAQ consists of Section 1: Assessment Information and Section 3: Attestation and Validation Details.
3. PCI DSS Requirements: Section 2 of each SAQ consists of the applicable PCI DSS requirements for the environment identified in the SAQ eligibility criteria, along with a place for the entity to record responses for each requirement. This section also includes applicable appendices for that SAQ (for example, for documenting use of compensating controls, and for describing any Not Applicable responses).

Compensating Controls

Compensating controls may be considered when an organization cannot meet a PCI DSS requirement as stated due to legitimate and documented technical or business constraints, but has sufficiently mitigated the associated risk by implementing alternative controls. To implement a compensating control for one or more PCI DSS requirements, your organization should do the following:

1. Follow the procedures for defining and documenting compensating controls as outlined in PCI DSS Appendix B, "Compensating Controls," including completion of a Compensating Control Worksheet (CCW) for each requirement met with a compensating control.
2. Document each compensating control by completing Appendix B: Compensating Controls Worksheet in the SAQ.

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

   Additional Compensating Control Worksheets can be found on the PCI SSC website.

3. For each requirement that was met with a compensating control, respond to that requirement in the SAQ by checking the "In Place with CCW" column.

Professional Assistance and Training

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.

- 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
  - Small merchant resources.
- PCI SSC also provides several 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.
- Payment-related training programs and resources may also be available from the payment brands and/or your merchant acquirer.

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

Understanding the SAQs for PCI DSS v4.0

There are several SAQ types summarized 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 that follow to ensure you meet all the eligibility criteria for that SAQ.

Note: *All entities completing SAQs are encouraged to contact the organizations that manage compliance programs and to which the SAQ will be submitted—for example, an acquirer (merchant bank) or the payment brands—to confirm they are eligible to complete an SAQ to validate PCI DSS compliance, and to understand any specific requirements or instructions.*

For service providers eligible to conduct a self-assessment, the only applicable SAQ is SAQ D for Service Providers.

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that completely outsource all account data functions to PCI DSS validated and compliant third parties. No electronic storage, processing, or transmission of account data on their systems or premises. *Not applicable to face-to-face channels. Not applicable to service providers.*
A-EP	E-commerce merchants that partially outsource payment processing to PCI DSS validated and compliant third parties, and with a website(s) that does not itself receive account data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the customer's account data. No electronic storage, processing, or transmission of account data on the merchant's systems or premises. *Applicable only to e-commerce channels. Not applicable to service providers.*
B	Merchants using only: ▪ Imprint machines with no electronic account data storage, and/or ▪ Standalone, dial-out terminals with no electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
B-IP	Merchants using only standalone, PCI-listed approved PIN Transaction Security (PTS) point-of-interaction (POI) devices with an IP connection to the payment processor. No electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
C-VT	Merchants that manually enter payment account data a single transaction at a time via a keyboard into a PCI DSS validated and compliant third-party virtual payment terminal solution, with an isolated computing device and a securely connected web browser. No electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
C	Merchants with payment application systems connected to the Internet, no electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*

SAQ	Description
P2PE	Merchants using only a validated, PCI-listed Point-to-Point Encryption (P2PE) solution. No access to clear-text account data and no electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
SPoC*	Merchants using a commercial off-the-shelf mobile device (for example, a phone or tablet) with a secure card reader included on PCI SSC's list of validated SPoC Solutions. No access to clear-text account data and no electronic account data storage. *Not applicable to unattended card-present, mail-order/telephone order (MOTO), or e-commerce channels.* *Not applicable to service providers.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types. *Not applicable to service providers.*
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete an SAQ.

** New SAQ for PCI DSS v4.0*

What's new for the PCI DSS v4.0 SAQs?

The v4.0 SAQs have been updated to provide more guidance, reporting information, and resources to support entities completing the self-assessment process. Generally, each SAQ was updated to reflect changes made to requirements in PCI DSS v4.0, to restate each SAQ requirement to mirror the wording used in PCI DSS, and to align the reporting responses for each SAQ requirement with those used in the PCI DSS v4.0 Report on Compliance Template. For more details about general changes made to all SAQs, see Appendix A: How SAQs Changed for PCI DSS v4.0.

Why some PCI DSS requirements in SAQs include multiple response checkboxes

For most PCI DSS requirements in the SAQs, there is only a single checkbox for an entity to select; however, a few requirements include a checkbox for each bullet of that requirement (for example, PCI DSS Requirement 6.4.3). This approach was taken only for certain requirements in the SAQs, usually for new and/or complex requirements where each bullet requires a different testing approach, and to emphasize that each bullet should be considered on its own.

Additional guidance and information about SAQ format is provided in the "Completing the Self-Assessment Questionnaire" section of each SAQ.

How will the SAQ updates impact my organization?

With PCI DSS v4.0, there is a new SAQ as well as clarified eligibility criteria for existing SAQs. Organizations will need to review the eligibility criteria to understand which SAQ is right for them. For example, the new SAQ may be better aligned with an organization's particular environment than the SAQ used previously. Similarly, an organization that previously completed one type of SAQ will need to review the updated eligibility criteria for that SAQ to determine whether it is still appropriate for their environment.

Some SAQs were updated to include additional PCI DSS requirements that were not in that SAQ for PCI DSS version 3.2.1. This will impact how the merchant approaches their self-assessment.

To understand why new requirements were added to SAQ A for PCI DSS v4.0, see *Overview: SAQ A and SAQ A-EP* below.

Merchants should continue to choose an applicable SAQ based upon the defined eligibility criteria for each SAQ, and according to instructions from their acquirer or payment brand(s). Merchants are encouraged to read the relevant PCI DSS v4.0 SAQ to 1) confirm the merchant still meets the eligibility criteria and 2) to familiarize themselves with all the updated wording and all requirements included in that SAQ.

Merchants should not assume that a particular SAQ for both PCI DSS v3.2.1 and v4.0 are the same.

SAQ SPoC – The New SAQ for PCI DSS v4.0

SAQ SPoC (Software-based PIN entry on COTS) is a new SAQ for merchants that use a commercial off-the-shelf mobile device (for example, phone or tablet) with a secure card reader that is part of a SPoC Solution on PCI SSC's list of validated Software-based PIN Entry on COTS (SPoC) Solutions. To be eligible for this SAQ, merchants must only enter account data via a secure card reader PIN (SCRP) as part of a validated PCI SSC SPoC Solution.

The listing of SPoC Solutions can be found here: PCI SPoC Solutions

What is the intent of SAQ SPoC?

SAQ SPoC was developed for card-present merchants using general purpose commercial off-the-shelf (COTS) mobile devices. This means that the mobile device (for example, a phone or tablet) does not have to be used only for payment nor does the mobile device have to be dedicated to a payment channel. The COTS mobile device is used along with a PCI-listed Secure Card Reader-PIN (SCRP) device as part of a PCI SSC SPoC Solution to securely process account data. Note that this SAQ is not applicable for SPoC solutions with non-PTS listed magnetic-stripe readers (MSRs). This SAQ may be used with PTS-listed SCRPs that include MSR functionality.

SAQ SPoC significantly reduces the number of applicable PCI DSS requirements for merchants using a PCI SSC listed SPoC solution.

How does SAQ SPoC compare to SAQ P2PE?

The following table provides a high-level overview of some of the key similarities and differences between SAQ P2PE and SAQ SPoC.

	SAQ P2PE	**SAQ SPoC**
	PTS approved POI device in a PCI-listed P2PE Solution	**COTS device and a PTS approved SCRP device in a PCI-listed SPoC Solution**
Applies to:	**Card-present** or **card-not-present** (mail/telephone order) merchants	**Attended card-present** merchants only (contact chip, contactless, SCRP-based magnetic stripe)
Payment Terminals	Payment is processed via a **PTS-approved POI** as part of a PCI-listed P2PE solution	Cardholder data is entered into a **PTS-approved SCRP device** as part of a PCI listed SPoC solution
Account Data Transmissions	Only from a PTS POI device as part of a **validated PCI-listed P2PE solution**	Only with a PTS SCRP device as part of a **validated PCI-listed SPoC solution**
Merchant Systems	No access to clear-text account data on any computer system Merchant does not otherwise store, process, or transmit account data electronically	
Data Retention	Merchant retains only paper reports or receipts with account data, and these documents are not received electronically	

This table is intended to provide a comparison between SAQ P2PE and SAQ SPoC and does not supersede or replace the eligibility criteria for either SAQ.

P2PE and SPoC Acronyms, Standards, and Listings

Acronyms	Definition and Related Standards	Solution/Device Listing*
P2PE	Point-to-Point Encryption Standard	PCI P2PE Solutions
PTS POI	PIN Transaction Security (PTS) Standard Point-of-Interaction (POI) Approval Class	Approved PTS Devices
SPoC	Software-based PIN Entry on COTS (commercial off-the-shelf) Standard	PCI SPoC Solutions
PTS SCRP	PIN Transaction Security (PTS) Standard Secure Card Reader-PIN (SCRP) Approval Class	Approved PTS Devices

* Listed solutions and devices are confirmed to meet the requirements defined within that PCI Standard and related Program Guide.

Overview: SAQ A and SAQ A-EP

SAQ A is intended for card-not-present (mail/telephone order or e-commerce) merchants that have completely outsourced all account data functions to a PCI DSS validated and compliant third-party service provider (TPSP). SAQ A merchants do not electronically store, process, or transmit any account data on their systems or premises.

SAQ A-EP is intended for merchants that have partially outsourced management of their e-commerce transactions but have functionality on their websites that impacts the security of the payment transaction.

As with SAQ A, SAQ A-EP merchants do not electronically store, process, or transmit any account data on their systems or premises, but rely entirely on a TPSP to handle these functions. All processing of account data is outsourced to a PCI DSS validated TPSP/payment processor for both SAQ A and SAQ A-EP.

SAQ A-EP includes additional security controls needed to secure merchant websites that control or manage the payment transaction, even though these websites do not store, process, or transmit account data. This is to reduce the likelihood that breaches of these websites can be used to compromise account data.

What types of e-commerce implementations are eligible for SAQ A vs. SAQ A-EP?

To be eligible for SAQ A, e-commerce merchants must meet all eligibility criteria detailed in SAQ A, including that there are no programs or application code that capture payment information on the merchant website. Examples of e-commerce implementations addressed by SAQ A include:

- Merchant has no access to their website, and the website is entirely hosted and managed by a compliant TPSP/payment processor.
- Merchant website contains a URL link redirecting users from merchant website to a PCI DSS compliant TPSP/processor facilitating the payment process.
- Merchant website provides an inline frame (iframe) to a PCI DSS compliant TPSP/processor facilitating the payment process.

If any element of a payment page delivered to consumers' browsers originates from the merchant's website, SAQ A does not apply; however, SAQ A-EP may be applicable. Examples of e-commerce implementations addressed by SAQ A-EP include:

- Merchant website creates the payment form, and the payment data is delivered directly from the consumer browser to the payment processor (often referred to as "Direct Post").
- Merchant website loads or delivers a script(s) that runs in consumers' browsers (for example, JavaScript) and provides functionality that supports creation of the payment page and/or how the data is transmitted to the payment processor.

The following table illustrates the common e-commerce methods and which SAQ may apply:

E-commerce Method	SAQ Type for Eligible Merchants	Number of PCI DSS v4.0 Requirements
Fully outsourced. Merchant has no access to own website.	SAQ A	11*
Fully outsourced. Merchant website redirects customers to a compliant TPSP (for example, a URL redirect).		27*
Fully outsourced. Merchant website includes a compliant TPSP's embedded payment page/form (for example, an iframe).		29*
Fully outsourced, except for the payment page. Merchant website creates the payment form, and payment data is delivered directly from the consumer browser to the TPSP (often called a "Direct Post").	SAQ A-EP	139
Fully outsourced, except for the payment page. Merchant website loads or delivers a script(s) that runs in the consumer browser (for example, JavaScript).		
All other e-commerce methods and implementations.	SAQ D for Merchants	All PCI DSS Requirements

Criteria for SAQ A mail/telephone order (MOTO) channels are not included in this table.

** Applicable requirements are identified via explanatory notes in SAQ A.*

Importance of new requirements added to SAQ A for PCI DSS v4.0

SAQ A for PCI DSS v4.0 includes additional security controls needed to address common breaches that are targeting SAQ A merchants, specifically to secure websites that 1) redirect payment transactions to a PCI DSS compliant TPSP or 2) include a PCI DSS compliant TPSP's embedded payment page/form. To mitigate these common breaches, the following new requirements are included in SAQ A (***Note**: This list highlights requirements added to specifically address recent e-commerce breaches; this is not a list of all new requirements included in SAQ A*):

- **PCI DSS Requirement 6.4.3** to manage payment page scripts. The intent is for a merchant to manage any payment page scripts present on the merchant's website.
- **PCI DSS Requirement 11.3.2** for external vulnerability scans at least once every 90 days and Requirement 11.3.2.1 for external vulnerability scans after significant changes. The intent is for a merchant to scan for and resolve any vulnerabilities on the merchant's website.
- **PCI DSS Requirement 11.6.1** for a change and tamper-detection mechanism deployed to detect and provide alerts for unauthorized modifications to HTTP headers and the contents of payment pages. The intent is for merchants to deploy this mechanism on the merchant's website and respond to alerts.

How does SAQ A compare to SAQ A-EP?

The following table provides a high-level overview of some of the key similarities and differences between SAQ A and SAQ A-EP.

	SAQ A	SAQ A-EP
	All Account Data Functions Completely Outsourced	**Partially Outsourced E-commerce Payment Channel**
Applies to:	**Card-not-present** merchants (e-commerce or mail/telephone-order)*	**E-commerce** merchants
Functions Outsourced	**All processing** of account data is entirely outsourced to PCI DSS compliant third-party service provider (TPSP)/payment processor	All processing of account data**, with the exception of the payment page,** is entirely outsourced to a PCI DSS compliant TPSP/payment processor
Payment Pages	All elements of all payment page(s)/form(s) delivered to the customer's browser **originate only and directly** from a PCI DSS compliant TPSP/payment processor	Each element of the payment page(s) delivered to the customer's browser **originates from either** the merchant's website or a PCI DSS compliant TPSP
Third-Party Compliance	Merchant confirmed that all TPSPs are PCI DSS compliant for the services being used by the merchant	
Merchant Systems	Merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions	
Data Retention	Any account data retained by merchant is on paper (for example, printed reports or receipts), and these documents are not received electronically	

** Criteria for SAQ A mail/telephone order (MOTO) channels are not included in this comparison.*

This table is intended to provide a comparison between SAQ A and SAQ A-EP and does not supersede or replace the eligibility criteria for either SAQ.

Overview: SAQ B and SAQ B-IP

SAQ B is intended for merchants that process account data via imprint machines or standalone, dial-out terminals. SAQ B merchants may be either brick-and-mortar (card-present) or mail/telephone order merchants. To be eligible for this SAQ, the standalone, dial-out terminals do not connect to other systems in the merchant environment, and they do not connect to the Internet. SAQ B merchants do not store account data in electronic format. This SAQ is not applicable to e-commerce channels.

SAQ B-IP is intended for merchants using only standalone payment terminals that connect to their payment processors via an IP-based connection. To be eligible for SAQ B-IP, merchants must be using payment terminals that are PCI-listed approved PIN Transaction Security (PTS) point-of-interaction (POI) devices. Note that merchants using the PTS POI devices classified as Secure Card Readers (SCR) or Secure Card Readers for PIN (SCRP) are NOT eligible for SAQ B-IP.

Other eligibility criteria for SAQ B-IP include that the approved PTS POI devices are not connected to any other types of systems in the merchant environment. This can be achieved via segmentation that isolates the PTS POI devices from other systems within the environment. Connections to other types of systems that would not meet SAQ B-IP eligibility criteria include, but are not limited to, connections to cash register systems, and if the PTO POI devices rely on any other device (for example, a computer, mobile phone, tablet, etc.) to connect to the payment processor. Additionally, to be eligible for SAQ B-IP, the only permitted transmission of account data is from the PTS POI device to the payment processor, and the merchant must not store account data in electronic format. SAQ B-IP, like SAQ B, is not applicable to e-commerce channels.

How does SAQ B-IP compare to SAQ B?

The following table provides a high-level overview of some of the key similarities and differences between SAQ B and SAQ B-IP.

	SAQ B	SAQ B-IP
	Imprint machines or standalone, dial-out terminals	**Standalone, PTS-approved payment terminals with an IP connection**
Applies to:	Brick-and-mortar (card-present) or mail/telephone order (card-not-present) merchants	
Payment Terminals	**Standalone, dial-out** terminal	**Standalone, PTS-approved point-of-interaction (POI) devices** (excludes secure card readers (SCRs and secure card readers PIN (SCRPs))
Connections	**Connected via phone line** to the processor **No connections** to other merchant systems or to the Internet	**Connected via IP** to the processor **Other IP-connected PTS-approved POI devices can be in the same network zone** but must be **isolated** from all other types of systems.
Account Data Transmissions	Only via **phone line** to the processor	Only via **IP** from the PTS-approved POI devices to the processor
Merchant Systems	Merchant does not store account data in electronic format	
Data Retention	Merchant retains only paper reports or receipts with account data, and these documents are not received electronically	

This table is intended to provide a comparison between SAQ B and SAQ B-IP and does not supersede or replace the eligibility criteria for either SAQ.

Overview: SAQ C-VT and SAQ C

SAQ C-VT is intended for merchants that process account data only via third-party virtual payment terminal solutions on an isolated computing device connected to the Internet. The merchant manually enters account data into the virtual payment terminal solution from an isolated computing device via a securely connected web browser, and the payment card transactions are submitted for authorization by the PCI DSS compliant third-party service provider that is hosting the virtual payment terminal solution. SAQ C-VT merchants may be either brick-and-mortar (card-present) or mail/telephone order merchants. To be eligible for this SAQ, the merchant only accesses the PCI DSS compliant virtual payment terminal solution via a computing device that is isolated in a single location, and that is not connected to other locations or systems.

SAQ C is intended for merchants with payment application systems (for example, point-of-sale systems) connected to the Internet. SAQ C merchants may be either brick-and-mortar (card-present) or mail/telephone order merchants. To be eligible for this SAQ, the merchant's payment application systems do not connect to other systems in the merchant environment, and the physical location of the environment is not connected to other premises or locations (single store only).

How does SAQ C-VT compare to SAQ C?

The following table provides a high-level overview of some of the key similarities and differences between SAQ C-VT and SAQ C.

	SAQ C-VT	SAQ C
	Web-Based Third-Party Virtual Payment Terminal Solution	**Payment Application System Connected to the Internet**
Applies to:	Brick-and-mortar (**card-present**) or mail/telephone order (**card-not-present**) merchants	
Payment Method	Account data is **manually entered** into a **third-party virtual payment terminal solution** Isolated computing device and securely connected web browser	**Point-of-sale (POS)** or **other payment application system**
Connections	Connected to the **Internet** **No connections to other locations or systems**	Connected to the **Internet** **No connections to other merchant systems** No connections to other premises or locations (**single store only**)
Account Data Transmissions	Only via the Internet to a **PCI DSS compliant Third-Party Virtual Payment Terminal System provider**	Only via the Internet to the processor
Merchant Systems	Merchant does not store account data in electronic format	
Data Retention	Merchant retains only paper reports or receipts with account data, and these documents are not received electronically	

This table is intended to provide a comparison between SAQ C-VT and SAQ C and does not supersede or replace the eligibility criteria for either SAQ.

SAQ Eligibility Criteria

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

SAQ A includes only those PCI DSS requirements applicable to merchants with account data functions completely outsourced to PCI DSS validated and compliant third parties, where the merchant retains only paper reports or receipts with account data.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on pages 23 and 24.

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

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

This SAQ is not applicable to service providers.

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

- The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of account data is entirely outsourced to PCI DSS compliant third-party service provider (TPSP)/payment processor;
- The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;
- The merchant has reviewed the PCI DSS Attestation of Compliance form(s) for its TPSP(s) and confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.

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

SAQ A-EP includes only those PCI DSS requirements applicable to e-commerce merchants with a website(s) that does not itself receive account data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the customer's account data.

SAQ A-EP merchants are e-commerce merchants that partially outsource their e-commerce payment channel to PCI DSS validated and compliant third parties and do not electronically store, process, or transmit any account 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 pages 23 and 24.

This SAQ is applicable only to e-commerce channels.

This SAQ is not applicable to service providers

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

- The merchant accepts only e-commerce transactions;
- All processing of account data, with the exception of the payment page, is entirely outsourced to a PCI DSS compliant third-party service provider (TPSP)/payment processor;
- The merchant's e-commerce website does not receive account data but controls how customers, or their account data, are redirected to a PCI DSS compliant TPSP/payment processor;
- If the merchant website is hosted by a TPSP, the TPSP is compliant with all applicable PCI DSS requirements (including PCI DSS Appendix A if the TPSP is a multi-tenant hosting provider);
- Each element of the payment page(s) delivered to the customer's browser originates from either the merchant's website or a PCI DSS compliant TPSP;
- The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;
- The merchant has reviewed the PCI DSS Attestation of Compliance form(s) for its TPSP(s) and has confirmed that the TPSP(s) are PCI DSS compliant for the services being used by the merchant; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

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 account data is transmitted, even though the website itself does not receive account data.*

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

SAQ B includes only those PCI DSS requirements applicable to merchants that process account 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 account data on any computer system.

This SAQ is not applicable to e-commerce channels.

This SAQ is not applicable to service providers.

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

- The merchant uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line to the merchant processor) to take customers' payment card information;
- The standalone, dial-out terminals are not connected to any other systems within the merchant environment;
- The standalone, dial-out terminals are not connected to the Internet;
- The merchant does not store account data in electronic format; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on pages 23 and 24.

SAQ B-IP – Merchants with Standalone, PCI-listed Approved PTS POI devices, No Electronic Account Data Storage

SAQ B-IP includes only those PCI DSS requirements applicable to merchants that process account data only via standalone, PCI-listed approved[1] PIN Transaction Security (PTS) point-of-interaction (POI) devices with an IP connection to the payment processor.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on pages 23 and 24.

An exception applies for PTS POI devices classified as Secure Card Readers (SCR) and Secure Card Readers for PIN (SCRPs); merchants using SCRs or SCRPs are not eligible for this SAQ.

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

This SAQ is not applicable to e-commerce channels.

This SAQ is not applicable to service providers.

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

- The merchant uses only standalone, PCI-listed approved[1] PTS POI devices (excludes SCRs and SCRPs) connected via IP to merchant's payment processor to take 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 and SCRPs);
- The standalone, IP-connected PTS POI devices are not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate PTS POI devices from other systems)[2];
- The only transmission of account data is from the approved PTS POI devices to the payment processor;
- The PTS POI device does not rely on any other device—e.g., computer, mobile phone, tablet, etc.—to connect to the payment processor;
- The merchant does not store account data in electronic format; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

[1] A merchant using an expired PTS POI device should check with its acquirer or individual payment brands about acceptability of this SAQ. Refer to the PCI list of PIN Transaction Security Devices with Expired Approvals.

[2] This criterion is not intended to prohibit more than one of the permitted system types (that is, IP-connected POI devices) being on the same network zone, as long as the permitted systems are isolated from other types of systems—e.g., by implementing network segmentation. Additionally, this criterion is not intended to prevent the defined system type from being able to transmit transaction information to a third party for processing, such as an acquirer or payment processor, over a network.

SAQ C-VT – Merchants with Web-Based Third-Party Virtual Payment Terminal Solutions, No Electronic Account Data Storage

SAQ C-VT includes only those PCI DSS requirements applicable to merchants that process account data only via third-party virtual payment terminal solutions on an isolated computing device connected to the Internet.

A virtual payment terminal is a third-party solution used to submit payment card transactions for authorization to a PCI DSS compliant third-party service provider (TPSP) website. Using this solution, the merchant manually enters account data from an isolated computing device via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment" on pages 23 and 24.

This SAQ option is intended to apply only to merchants that manually enter a single transaction at a time via a keyboard into an Internet-based virtual payment terminal solution. SAQ C-VT merchants may be brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants, and do not store account data on any computer system.

This SAQ is not applicable to e-commerce channels.

This SAQ is not applicable to service providers.

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

- The only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser;
- The virtual payment terminal solution is provided and hosted by a PCI DSS compliant third-party service provider;
- The PCI DSS compliant virtual payment terminal solution is only accessed via a computing device that is isolated in a single location, and is not connected to other locations or systems;
- The computing device does not have software installed that causes account data to be stored (for example, there is no software for batch processing or store-and-forward);
- The computing device does not have any attached hardware devices that are used to capture or store account data (for example, there are no card readers attached);
- The merchant does not otherwise receive, transmit, or store account data electronically through any channels (for example, via an internal network or the Internet); and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

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

SAQ C includes only those PCI DSS requirements applicable to merchants with payment application systems (for example, point-of-sale systems) connected to the Internet, and that do not store electronic account data.

SAQ C merchants process account data via a point-of-sale (POS) system or other payment application systems connected to the Internet, do not store account data on any computer system, and may be either brick-and-mortar (card-present) 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 pages 23 and 24.

This SAQ is not applicable to e-commerce channels.

This SAQ is not applicable to service providers.

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

- The merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN);
- The payment application system is not connected to any other systems within the merchant 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;
- The merchant does not store account data in electronic format; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically**.**

SAQ P2PE – Merchants Using only Payment Terminals in a PCI-listed P2PE Solution, No Electronic Account Data Storage

SAQ P2PE includes only those PCI DSS requirements applicable to merchants that process account data only via a validated[3] PCI-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 payment terminals from a validated[3] PCI-listed 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 account data on paper or over a telephone, and key it directly and only into payment terminal from a validated[3] PCI-listed P2PE solution.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on pages 23 and 24.

This SAQ is not applicable to e-commerce channels.

This SAQ is not applicable to service providers.

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

- All payment processing is via a validated[3] PCI-listed P2PE solution;
- The only systems in the merchant environment that store, process, or transmit account data are the payment terminals from a validated[3] PCI-listed P2PE solution;
- The merchant does not otherwise receive, transmit, or store account data electronically;
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- The merchant has implemented all controls in the *P2PE Instruction Manual (PIM)* provided by the P2PE Solution Provider.

[3] P2PE solutions on the PCI list of Point-to-Point Solutions with Expired Validations are no longer considered "validated" per the P2PE Program Guide. A merchant using an expired P2PE solution should check with its acquirer or individual payment brands about acceptability of this SAQ.

SAQ SPoC – Merchants Using only PCI-listed Approved PTS SCRP Device and COTS Device as Part of a Validated PCI-Listed SPoC Solution

SAQ SPoC includes only those PCI DSS requirements applicable to merchants that process account data only via a PCI-listed approved PTS Secure Card Reader-PIN (SCRP) device and accompanying commercial off-the-shelf (COTS) mobile device (for example, phone or tablet) as part of a validated PCI-listed Software-based PIN Entry on COTS (SPoC) solution.

SAQ SPoC merchants do not have access to clear-text account data on any computer system and only enter account data via an SCRP as part of a PCI-listed SPoC solution, using a merchant COTS mobile device. These COTS mobile devices are general-purpose mobile devices – this means that the mobile device does not have to be used only for payment or dedicated to a payment channel.

SAQ SPoC merchants process card-present transactions (contact chip transactions, contactless transactions, and SCRP-based magnetic stripe transactions).

An exception applies for merchants using non-PTS listed magnetic stripe readers (MSRs); these merchants are not eligible for this SAQ. This SAQ may be used for PTS-listed SCRPs that include MSR functionality.

This SAQ is not applicable to unattended card-present—for example, kiosks, self-checkout—mail-order/telephone order (MOTO), or e-commerce channels.

This SAQ is not applicable to service providers.

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

- All payment processing is only via a card-present payment channel;
- All cardholder data entry is via an SCRP that is part of a validated SPoC solution approved and listed by PCI SSC;
- The only systems in the merchant's SPoC environment that store, process, or transmit account data are those used as part of the validated[4] SPoC solution approved and listed by PCI SSC;
- The merchant does not otherwise receive, transmit or store account data electronically;
- This payment channel is not connected to any other systems/networks within the merchant environment;
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- The merchant has implemented all controls in the SPoC user guide provided by the SPoC Solution Provider.

[4] SPoC solutions on the PCI list of SPoC Solutions with an Expired Validation are no longer considered "validated" per the SPoC Program Guide. Merchants using an expired SPoC solution should check with their acquirer or individual payment brands about acceptability of this SAQ.

SAQ D for Merchants – All Other SAQ-Eligible Merchants

SAQ D for Merchants applies to merchants that are eligible to complete a self-assessment questionnaire but do not meet the criteria for any other SAQ type. Examples of merchant environments to which SAQ D may apply include, but are not limited to:

- E-commerce merchants that accept account data on their website;
- Merchants with electronic storage of account data;
- Merchants that do not store account 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.

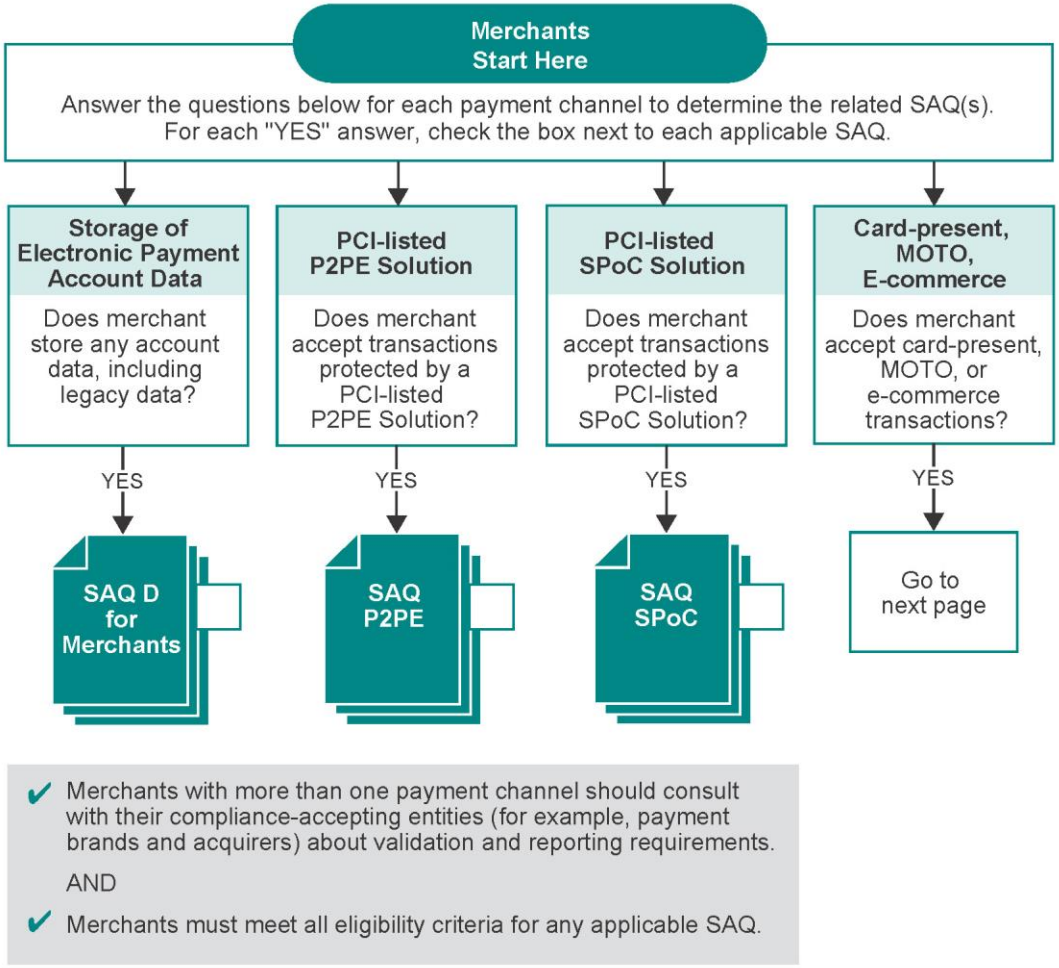
SAQ D for Service Providers – SAQ-Eligible Service Providers

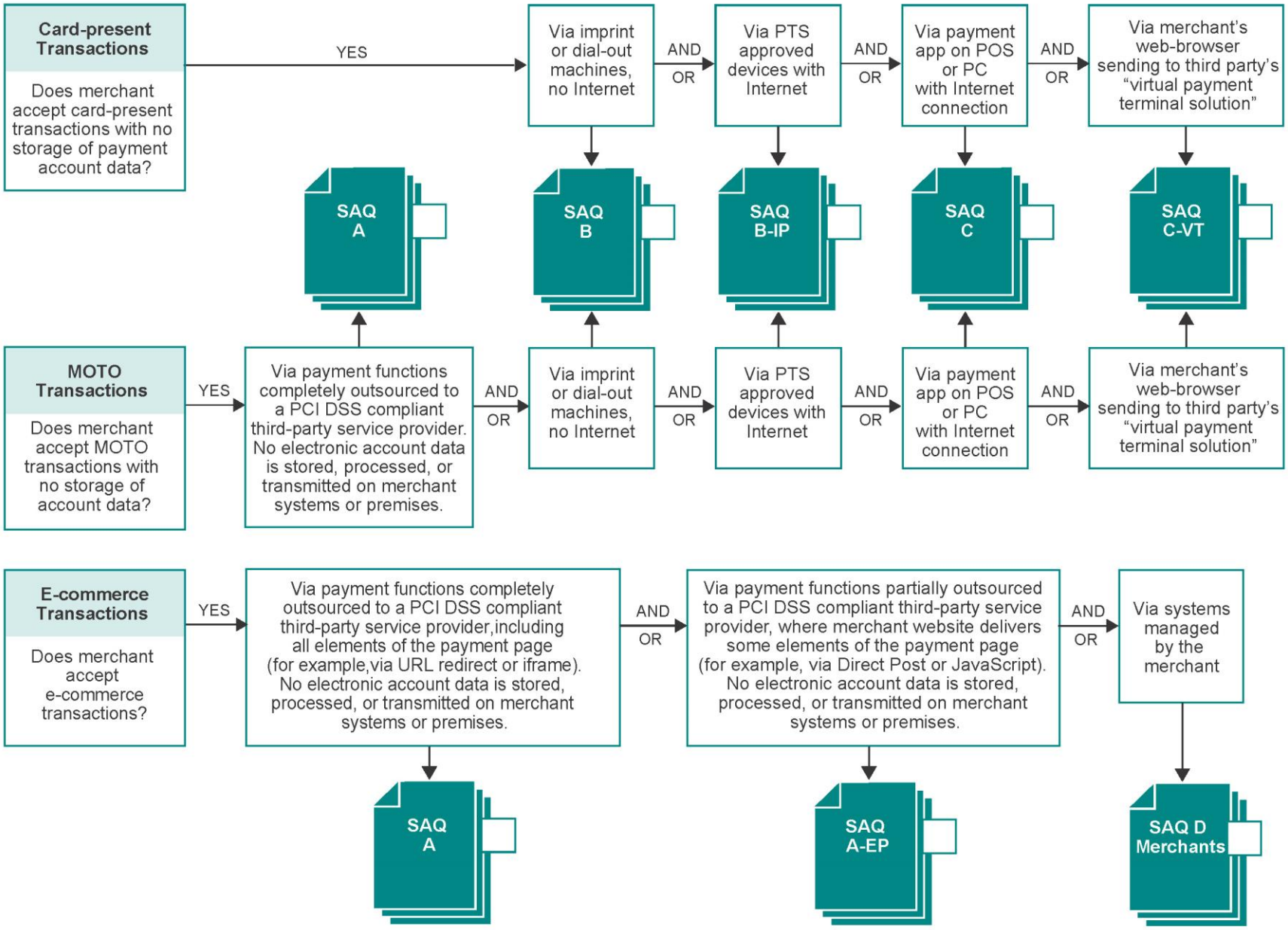
SAQ D for Service Providers applies to all service providers defined by a payment brand as being eligible to complete a self-assessment questionnaire.

Note that, for PCI DSS v4.0, SAQ D for Service Providers now requires additional documentation in Section 2a and specifies that service providers "Describe Results" for each PCI DSS requirement.

For a graphical guide to choosing your SAQ type, please see "Which SAQ Best Applies to My Environment?" on pages 23 and 24.

Which SAQ Best Applies to My Environment?





Appendix A: How SAQs Changed for PCI DSS v4.0

The following is a summary of general changes made to all SAQs in the transition from v3.2.1 to v4.0.

- A "Defining Account Data, Cardholder Data, and Sensitive Authentication Data" table was added from PCI DSS v4.0 to define the various terms used in PCI DSS.
- A "Reporting Responses" table was added to describe the meaning of each reporting response that entities select for each PCI DSS requirement when completing a SAQ.
- The requirements in each SAQ have been updated to reflect changes made to PCI DSS v4.0, and to align more closely with other PCI DSS v4.0 documents. For example:
  - The wording for each PCI DSS requirement now mirrors the wording in PCI DSS v4.0, rather than being stated in the form of questions.
  - Some complex requirements were broken into sub-requirements, and other requirements were clarified.
  - The reporting responses for each PCI DSS requirement were updated to align with the language in the PCI DSS v4.0 Report on Compliance (ROC) Template – for example, "Yes" is now "In Place."
  - The Attestation of Compliance (AOC) sections were updated to align with the wording and content of the ROC AOCs.
- For some of the more complicated requirements, explanations were added[5] to help merchants understand how to evaluate that requirement in the context of a given SAQ.
- New appendices were added for completion of additional information about specific reporting responses.

In addition to the changes described above, SAQ D for Service Providers now requires additional documentation in Section 2a and specifies that service providers "Describe Results" for each PCI DSS requirement.

[5] Except for SAQ D for Merchants and SAQ D for Service Providers.