Understanding the SAQs for PCI DSS version 3

The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI DSS self-assessment. The different SAQ types are shown in the table below to help you identify which SAQ best applies to your organization. Detailed descriptions for each SAQ are provided within the applicable SAQ.

Note: *Entities should ensure they meet all the requirements for a particular SAQ before using the SAQ. Merchants are encouraged to contact their merchant bank (acquirer) or the applicable payment brand(s) to identify the appropriate SAQ based on their eligibility.*

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated 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 electronic storage, processing, or transmission of any cardholder data on the 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 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.*
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
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 a SAQ.

** New for PCI DSS v3.0*

What's new in version 3 of the SAQs?

The format of the self-assessment questionnaire (SAQs) has been updated in version 3 to provide more guidance and reporting information for each PCI DSS requirement.

A new column titled "Expected Testing" describes the testing activities to be performed during the self-assessment, to help the entity determine whether a requirement has been met. The "Special" column from version 2 has been replaced with two separate columns in version 3: "Yes with CCW" (compensating control worksheet) and "N/A." These updated response options help entities to more clearly identify which response to use for each requirement. The orientation of the SAQs has changed from portrait to landscape to accommodate these additional columns.

There is also additional guidance provided at the beginning of the SAQs to assist with understanding how to complete the SAQ. The sections within the SAQ documents have been reorganized, such that Parts 3 and 4 of the AOC now follow the questionnaire portion of the SAQ. This is to ensure that an entity's attestation encompasses all elements of the SAQ and AOC.

Additional guidance and information about SAQ format is provided in the "Before you Begin" section of each SAQ.

How will the SAQ updates impact my organization?

With PCI DSS version 3, there are new SAQs as well as updated eligibility criteria for existing SAQs, and organizations will need to review the eligibility criteria to understand which SAQ may now be right for them. For example, one of the new SAQs 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 criteria for that particular SAQ to determine whether it is still appropriate for their environment.

The SAQ updates for version 3 may also mean that a merchant may need to validate additional requirements, which could impact how the merchant approaches their self-assessment.

Even where the eligibility criteria have not changed for a particular SAQ, the SAQ may include different PCI DSS requirements in version 3 than in version 2. The questions in each SAQ have been updated to reflect changes made to PCI DSS version 3. For example, some complex requirements have been broken down into sub-requirements, and other requirements may have been clarified or extended, resulting in updated questions in the SAQs.

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).

What are the new SAQs for PCI DSS version 3?

SAQ A-EP is a new SAQ for e-commerce merchants who outsource their transaction-processing functions to PCI DSS compliant third-party service providers, where the merchant website controls how the cardholder data is redirected to the third-party service provider. To be eligible for this SAQ, the merchant must not store, process, or transmit cardholder data on any of their systems or premises.

SAQ B-IP is a new SAQ for merchants who process cardholder data only via standalone, PTS-approved point-of-interaction (POI) devices that have an IP connection to their payment processor, and do not electronically store cardholder data. To be eligible for this SAQ, the merchant must be using payment terminals that are currently listed on the *PTS List of Approved POI Devices* (https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php). Note that the Secure Card Reader (SCR) class of POI devices does not meet the criteria for SAQ B-IP, and thus merchant using SCRs are not eligible for this SAQ. SAQ B-IP is not applicable to e-commerce channels.

What is the intent of SAQ A-EP?

SAQ A-EP has been developed to differentiate between merchants that have partially outsourced management of their e-commerce transactions, and merchants that have completely outsourced all management of their e-commerce environment (SAQ A merchants).

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

Prior to the release of SAQ A-EP, many e-commerce merchants with web sites that impacted the security of payment transactions may have felt they were eligible for SAQ A because their web server does not store, process, or transmit cardholder data. As a result, these web servers did not have sufficient security controls applied to them and have become common targets for attackers as a means to compromise cardholder data.

SAQ A-EP is intended to identify the controls needed to secure merchant web sites that control or manage the payment transaction, and reduce the likelihood a breach of the web site can be used to compromise cardholder data.

How does SAQ A-EP compare to SAQ A?

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 All Cardholder Data Functions Completely Outsourced	SAQ A-EP 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 cardholder data is entirely outsourced to PCI DSS validated third-party service providers	All processing of cardholder data**, with the exception of the payment page,** is entirely outsourced to a PCI DSS validated third-party payment processor
Payment Pages	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)	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)
Third-Party Compliance	Merchant confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant	
Merchant Systems	Merchant does not electronically store, process, or transmit any cardholder data on their systems or premises, but relies entirely on a third party(s) to handle all these functions	
Data Retention	Merchant retains only paper reports or receipts with cardholder data, 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.

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

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 third-party payment processor
- Merchant website provides an inline frame (iFrame) to a PCI DSS compliant third-party processor facilitating the payment process.
- Merchant website contains a URL link redirecting users from merchant website to a PCI DSS compliant third-party 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 script 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.

What is the intent of SAQ B-IP?

SAQ B-IP has been developed to differentiate between merchants using only standalone payment terminals that connect to their payment processors via an IP-based connection, from merchants who connect to their payment processor using only dial-out connections (which may meet the criteria of SAQ B). To be eligible for SAQ B-IP, merchants must be using payment terminals that have been approved under the PCI PTS program and are listed on the PCI SSC website as approved devices. Note that merchants using the Secure Card Reader (SCR) category of devices are NOT eligible for SAQ B-IP.

Other eligibility criteria for SAQ B-IP include that the approved devices are segmented from other systems within the environment, and the devices do not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor. Additionally, to be eligible for SAQ B-IP, the only permitted transmission of cardholder data is from the PTS-approved device to the payment processor, and the merchant must not store cardholder data in electronic format. SAQ B-IP, like SAQ B, is not applicable to e-commerce channels.

Prior to the release of SAQ B-IP, merchants with this type of environment may have needed to complete SAQ C or SAQ D. These merchants may now be eligible to use SAQ B-IP, which may be better suited for their particular environment and provides a simpler validation than SAQ C.

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 **Imprint machines or standalone, dial-out terminals**	**SAQ B-IP** **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 (connected via a phone line to the processor)**	Standalone, **PTS-approved point-of-interaction (POI) devices (excludes SCRs) connected via IP to the payment processor**
CHD Transmissions	**CHD is not transmitted over a network** (either an internal network or the Internet)	**Only CHD transmission is via IP from the PTS-approved POI devices to the payment processor**
Merchant Systems	Merchant does not does not store cardholder data in electronic format	
Data Retention	Merchant retains only paper reports or receipts with cardholder 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.