sysnet global solutions

PCI DSS v3.2 revision 1.1 SAQs

What's changed?

Natasja Bolton, Senior Acquirer Support QSA

What are the key dates for the updated SAQs?

Since the publication of revision 1.1 of the SAQs, there are two active versions of the SAQs. Currently both versions may be used to assess compliance: v3.2 revision 1.0 or v3.2 revision 1.1. The v3.2 revision 1.0 SAQs, published back in April 2016, may continue to be used for compliance assessment until 30th September 2017. From 1st October 2017 assessment must be undertaken using the updated revision 1.1 SAQs.

Are there any new SAQs?

No, the changes are to the existing v3.2 SAQs; no new SAQs have been published. The nine v3.2 revision 1.1 SAQs address the same payment processing scenarios as before:

SAQ Type	Description
A	Card Not Present (Ecommerce or MOTO) Outsource all cardholder data (CHD) functions to validated third parties
A-EP	Card Not Present (Ecommerce) Partially outsource CHD functions to validated third parties.
B	Imprint-only, or standalone, dial-out terminal No electronic cardholder data storage
B-IP	Standalone, point-of-interaction (POI) device connected via IP. No electronic cardholder data storage
C-VT	Virtual terminal only merchants, no electronic cardholder data storage
C	Internet connected payment application systems, no electronic cardholder data storage
P2PE	Hardware payment terminals included in a P2PE validated payment solution, no electronic cardholder data storage
D – Merchant D – Service Provider	All other merchants not eligible for SAQ types above, and all service providers defined by a payment brand as eligible to complete an SAQ

As the PCI SSC outline in their blog, revision 1.1 makes only minor changes to the v3.2 SAQs to "clarify points of confusion", to incorporate explanations from recent PCI SSC FAQs, to better align some of the SAQs with the changes brought in with PCI DSS v3.2 and, lastly, to amend some typographical and grammatical errors (such as missing checkboxes).

Revision 1.1 amendments to the SAQs

Four of the SAQs have not been changed and, for those SAQs that have been amended, the changes are either the inclusion of additional PCI DSS requirements and/or clarifications.

SAQs with no changes

Firstly, the SAQs A-EP, B, P2PE and D (both merchant and service provider versions) have not had any changes made to them. These SAQs have been updated to revision 1.1 purely to align their version numbering to that of the amended SAQs.

Clarification Changes

Clarification in the SAQ A:

The SAQ A revisions 1.1 amendments are a clarification of intent only; the actual SAQ questions themselves are the same as in the original v3.2 SAQ A release.

As we explained in our SAQ A: Changes for e-Commerce article, new requirements introduced to the SAQ A on the publication of PCI DSS v3.2, are applicable to a merchant's e-commerce web server if they have implemented a redirect or iFrame approach for their e-commerce payment processing.

> The SAQ A requirements applicable when using a redirect to a hosted payment page (or iFrame of same) provided by a validated PCI DSS compliant service provider:
> - Vendor defaults have been changed and unnecessary default accounts removed (reqt 2.1);
> - All users are uniquely identified and authenticated (reqt 8.1.1, 8.1.3, 8.2, 8.5);
> - Strong passwords are being used (reqt 8.2.3);
> - Terminated user accounts are de-activated or removed (reqt 8.1.3).

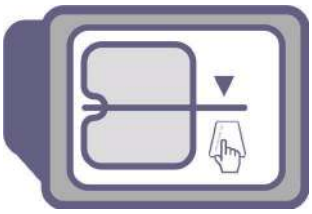
The PCI SSC initially clarified the intent of these new SAQ A requirements in a September 2016 FAQ, confirming the questions from requirements 2 and 8 were included in SAQ A to make sure that merchants implement some basic security measures to address the ongoing threats and reduce the risk of compromise of e-commerce web servers that redirect customers to a third party for payment processing.

That FAQ explanation has now been added to the SAQ A revision 1.1 as a note in the 'Before You Begin' section (page iii). The note explains when the requirements must be included in the merchant's assessment and when they can be marked as 'Not Applicable'.

Clarifications in the SAQ B-IP:

The SAQ B-IP revision 1.1 includes one clarification relating to its use of the term 'SCR'. SCR is used in the 'Before You Begin' applicability section of the SAQ B-IP (page iii). Merchants using Secure Card Readers (SCRs) are not eligible for the SAQ B-IP.

SCRs are a particular category of approved PTS device, listed by the PCI SSC, and include devices such as the card readers implemented with separate PIN Pads in unattended payment kiosks:



As well as contactless card readers:

Or card readers used by many mPOS (mobile payments) solutions:

The SAQ B-IP is intended to be used by merchants using standalone PTS-approved IP-based payment terminals; these SCRs do not fulfil this definition as they have dependencies on other components in order to be able to take and submit the customer's cardholder data to the payment processor.

Clarifications in the SAQ C-VT and SAQ C:

In November, the PCI SSC published an FAQ 'What is the intent of the SAQ eligibility criteria?'. This FAQ was issued to help merchants and assessors understand how to interpret the SAQ eligibility criteria set out in the 'Before You Begin' section of each SAQ.

The FAQ confirmed that *"In order for a merchant environment to meet SAQ eligibility criteria, only system types defined in the eligibility criteria may be used in that environment. Additionally, these SAQs explicitly state that the defined system type must not be connected to any other systems, and that segmentation may be used to isolate the permitted system type from all other systems*".*

*"*This criteria 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".*

This FAQ also stated that *"The SAQ criteria is not intended to prohibit more than one of the permitted system types being on the same network zone, as long as the permitted systems are all isolated from other types of systems (e.g. by implementing network segmentation)".*

These PCI SSC SAQ eligibility clarifications have now been included as a footnote in both the SAQ C-VT and SAQ C revision 1.1.

SAQ C-VT eligible merchants are those using isolated virtual payment terminals (web-browser based access from a personal computer connected to the Internet) to authorise transactions by manually entering payment card data into a website provided by an PCI DSS validated acquirer, processor, or third-party service provider. The footnote confirms that a merchant's SAQ C-VT eligible environment may have more than one of these 'permitted system types' on the same network zone. The merchants do need to ensure that these permitted systems are isolated from other types of systems, for example by implementing network segmentation.

For example, that could be a merchant environment like this:

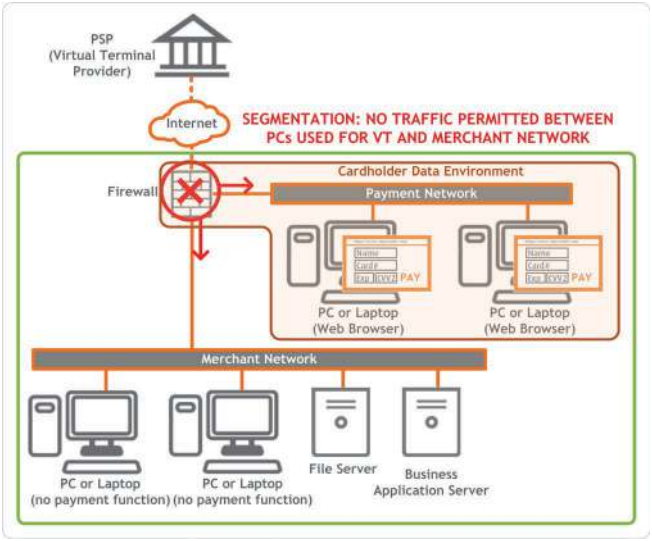


Figure 1: SAQ C-VT eligible environment

SAQ C eligible merchants are those using a point-of-sale (POS) system or other payment application system connected to the Internet to process cardholder data. The footnote in SAQ C confirms that a merchant's SAQ C eligible environment may have more than one payment application system on the same network zone. Merchants will still need to ensure that these payment application systems are isolated from other types of systems, for example:

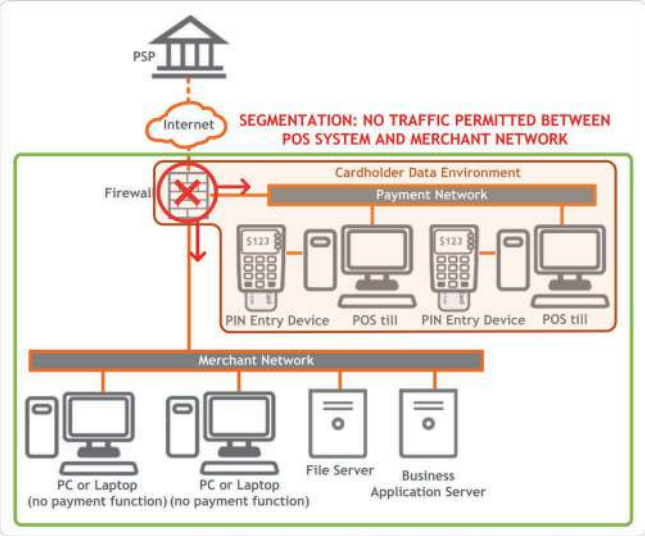


Figure 2: SAQ C eligible environment

New requirements

Two additional PCI DSS requirements have been added to the SAQs B-IP and C-VT.

8.3.1: Is multi-factor authentication incorporated for all non-console access into the CDE for personnel with administrative access? ***Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.***

11.3.4: If segmentation is used to isolate the CDE from other networks:

(a) Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE?

(b) Does penetration testing to verify segmentation controls meet the following?

- Performed at least annually and after any changes to segmentation controls/ methods
- Covers all segmentation controls/methods in use
- Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

(c) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organisational independence of the tester exist (not required to be a QSA or ASV)

As we discussed in our PCI DSS v3.2 what's changed article, requirement 8.3.1 was introduced to make sure that users with the ability to make changes to CDE systems, and hence to potentially weaken security controls or introduce vulnerabilities, are more strongly authenticated. This multi-factor authentication requirement has been included in the SAQs B-IP and C-VT to align with the intent of the existing requirement 2.3 (which requires strong encryption for all methods of non-console administrative access).

The requirement for multi-factor authentication for all non-console administrative access, would mean an SAQ B-IP eligible merchant, like that shown below, will not only need strongly encrypted methods for administrative access to their network devices such as the Switch and Firewall shown but which also incorporate multi-factor authentication of the administrative user:

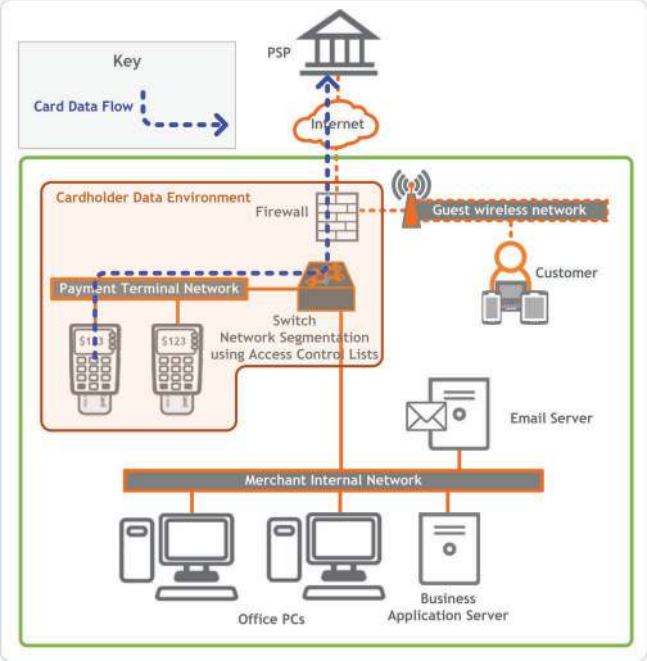


Figure 3: SAQ B-IP eligible environment

The segmentation penetration testing requirements (11.3.4. a, b. and c.) are applicable, if the merchant is making use of segmentation controls to confirm eligibility for the selected SAQ. The penetration testing is necessary to confirm the segmentation methods used are operational and effective, and isolate all out of scope systems (e.g. the Merchant Network shown in the diagram above) from systems in the CDE (e.g. the Payment Terminal Network).

Summary Table of v3.2 rev 1.1 SAQ Questions and Requirements

The table below shows how the v3.2 SAQ question count has changed and highlights (in red text) which PCI DSS requirements the new questions appear in:

SAQ Type	Number of Assessment Questions*	
	PCI DSS V3.2 rev 1.0	PCI DSS V3.2 rev 1.1
A	22 questions: Requirements 2, 8, 9 & 12	No changes
A-EP	193 questions: Requirements 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, Appendix A2	No changes
B	41 questions: Requirements 3, 4, 7, 9 & 12	No changes
B-IP	84 questions: Requirements 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, Appendix A2	88 questions: Requirements 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, Appendix A2
C-VT	81 questions: Requirements 1, 2, 3, 4, 5, 6, 7, 8, 9 & 12, Appendix A2	85 questions: Requirements 1, 2, 3, 4, 5, 6, 7, 8, 9, 11 & 12, Appendix A2
C	162 questions: Requirements 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 & 12, Appendix A2	No changes
P2PE	33 questions: Requirements 3, 9 & 12 PLUS PIM validation	No changes
D – Merchant D – Service Provider	331 questions - merchant 359 questions – service provider	No changes

*note: the count shown is of the number of questions the business is required to answer, for example one requirement may consist of many sub-requirements: a, b, c, etc. The count also includes the two questions in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS, if included the SAQ.