Overview of Self-Assessment Questionnaires (SAQs)

The first thing to keep in mind while attempting to scope PCI DSS requirements is that the entity is required to comply with all PCI DSS requirements that are applicable always. Regardless of the SAQ used, compliance with applicable requirements not listed on a specific SAQ document is required to maintain compliance.

Quoted from a SAQ document:

"This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements to be PCI DSS compliant."

SAQs are presented to provide a typical list that would be applicable in certain circumstances. This comes into play with SAQ B-IP, C, and C-VT as they have a prerequisite for isolation from other systems. The strict interpretation can be, and would likely be in the event of a breach, that there is no connection between these systems and other business systems to the point of connection to the Internet. This implies separate firewalls and switches, in addition to systems. However, most organizations using environments that appear to fit into one of these SAQs will have some overlap. For instance, using an optional port off the firewall to provide an isolated network or a separate vlan on a switch to provide isolated connectivity. In this case, the requirements listed in the SAQ as well as some requirements not listed could be applicable. Below is a breakdown at a high level of the SAQ requirements and the environments that they apply to:

SAQ A

Outsourced e-commerce transactions

Prerequisites

In order to use this SAQ, the merchant needs to have e-commerce transactions completely outsourced to a validated PCI DSS compliant service provider. Outsourcing requires that no part of the payment form is presented to the customer by the merchant's webserver. The customer's system must either redirect the web browser to a site hosted by the service provider or use an iframe to present the form. The most common mistake in selecting this SAQ is using it when connected to the service provider's API for transaction processing.

Requirements

SAQ A may be the easiest set of requirements, as it only requires that the merchant validate that the service provider is compliant with PCI DSS on regular basis.

SAQ A-EP

Partially outsourced e-commerce transactions

Prerequisites

SAQ A-EP is like A, however should be used when the merchant's website does have direct interaction with cardholder data. Since compromise of the merchant controlled web server can lead to breach of cardholder data, many technical requirements of PCI DSS become applicable. If the merchant's webserver has a form or script presented from their server to the customers web browser, even if the script is created by the service provider and the customer's browser sends cardholder data directly to the service provider, SAQ A-EP is the appropriate set of requirements. However, the merchant is ineligible to use SAQ A-EP if their server stores or transmits cardholder data.

Requirements

SAQ A-EP requirements are significantly more difficult to adhere to that SAQ A. SAQ A-EP brings firewall, system hardening, vulnerability management, change control, secure software development, code review or web-application firewall, physical security, log management/SIEM, vulnerability scanning, penetration testing, file integrity monitoring, security policy, and incident response requirements into scope for compliance. Many organizations will find that it takes a significant ongoing investment in both staff and technical solutions to adhere to SAQ A-EP.

SAQ B

Dial-out Payment Terminals

Prerequisites

SAQ B applies to payment terminals connected to a telephone line. It should be noted that the entity cannot use this SAQ if they store or transmit cardholder data electronically in any way. For instance, if the entity receives order forms via e-mail or fax software they would be ineligible for SAQ B.

Requirements

SAQ B, from the compliance perspective, provides a short and relatively easy set of requirements to meet. For the most part, handling of hard-copy cardholder data and physical review for tamper of devices are the only items that need to be addressed.

SAQ B-IP

Network connected Payment Terminals

Prerequisites

Many newer payment terminals use Ethernet or wireless networks for connection to the processor. SAQ B-IP was released to provide an option for reporting compliance when using these network connected payment terminals. Use of SAQ B-IP requires that the payment terminals are connected to an isolated network with a firewall in place. Keep in mind, if the isolation is created by device(s) used for other networks more requirement may become applicable (e.g. systems used to manage a shared firewall may come into scope).

Requirements

The network connected payment terminals must setup behind a firewall, with strict rule sets applied. Additionally, the merchant must have process in place to patch the terminals and keep them up to date if any vulnerabilities present themselves. Finally, the same requirements apply as SAQ B for hard-copy data and physical review for tampering.

SAQ C

Payment Applications/Systems connected to the Internet

Prerequisites

This SAQ typically applies to companies purchasing a POS system. Payment applications can be validated as PA-DSS applications to aid in PCI DSS compliance. There are a few things to note when looking at SAQ C and PA-DSS validation. First, validation to PA-DSS only assures that the application will not interfere PCI DSS, it does not guarantee compliance. Second, PA-DSS use is not required by PCI DSS. However, MasterCard does require any purchased payment application by a merchant to be PA-DSS validated (excluding custom developed applications). Finally, the use of SAQ C is limited to smaller merchants because of the requirement that the POS environment is limited to a single store or physical location. A wide area network or multiple locations makes the merchant ineligible for SAQ C.

Requirements

SAQ C contains a long list of requirements as compared to the other SAQs. However, if a PA-DSS validated application is used and deployed as described in its implementation guide, compliance with PCI DSS can be straightforward. In any case, the merchant will be responsible for some items that are not addressed by the payment application alone. Specifically, SAQ C includes firewall, system hardening, vulnerability management, change control, physical security, log management/SIEM, vulnerability scanning, penetration testing, file integrity monitoring, security policy, and incident response requirements.

SAQ C-VT

Web-based Virtual Terminals

Prerequisites

Web-based virtual terminals are web pages hosted by validated service providers that allow processing transactions through manual entry on a computer keyboard. On the merchant's side, they would have a computer with Internet access, all other functions are done by the service provider. Two key items are required for a merchant to use SAQ C-VT. First, the system(s) should be dedicated and isolated for use with only the payment processing website. Second, no magnetic card readers should be used to enter the credit card data.

Requirements

SAQ C-VT requirements are not difficult to meet, most merchants have the most difficulty meeting the eligibility requirements as single purpose workstations are rare in existing networks. After setting up a dedicated network and workstations the requirements that apply include antivirus software, regular patching, and restrictive firewall rules.

SAQ D

Everything else

Prerequisites

SAQ D applies to all service providers. SAQ D also applies to any merchants that do not fit the requirements for the other SAQs.

Requirements

Includes all of the requirements from PCI DSS.