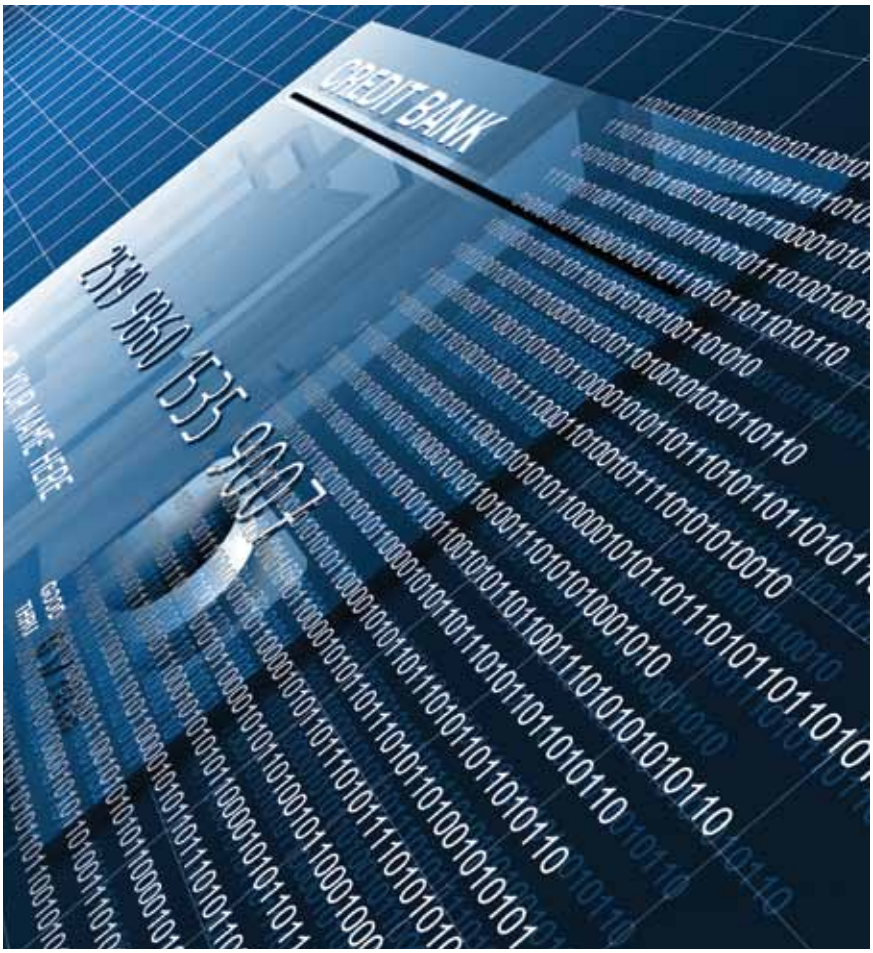
FIVE WAYS TO REDUCE SAQ SCOPE

By Gary Glover, CISSP, CISA, QSA, PA-QSA

Reducing the scope for the PCI DSS Self Assessment Questionnaire (SAQ) ultimately boils down to reducing the areas in which payment card data touches



The Payment Card Industry (PCI) Data Security Standard (DSS) Self Assessment Questionnaire (SAQ) is a crucial yet difficult part of any PCI journey. Typically, SAQ questions are very technical, involved and leave little room for guesswork.

As a PCI QSA (Qualified Security Assessor), my ultimate goal in helping a customer successfully and truthfully complete their SAQ is to reduce PCI scope. Being 'in scope' indicates any system component included in or connected to the card data environment, comprised of people, process and technology that stores, processes or transmits cardholder data. Reducing PCI scope ultimately boils down to reducing the areas in which payment card data touches.

For example, if a merchant was originally required to complete an SAQ D, my goal (and the goal of all businesses in the payment card industry) should be to help them transition to the less technical SAQ C. Not only does scope reduction relieve merchant frustration with technical PCI requirements, but also decreases cost, resources and the risk of payment data theft. Here are the five best ways to reduce your PCI scope.

1. Segment Your Network

The quickest and easiest way to limit the scope of PCI requirements is to segment your network so that cardholder data and the systems that process, transmit and store it are isolated from all other network processes.

Most card data environments aren't created with PCI compliance in mind.

Gary Glover CISSP, CISA, QSA, PA-QSA is QSA director for SecurityMetrics and has completed over 100 PCI DSS, PABP and PA-DSS security audits. He is a speaker at the 2013 HFTP Annual Convention & Tradeshow. He can be reached at gglover@securitymetrics.com.

The Five Best Ways To Reduce Your PCI Scope

1. Segment Your Network
Segment your network so that cardholder data and the systems that process, transmit and store it are isolated from all other network processes.

2. Stop Storing Payment Data
It doesn't matter if an organization stores one payment card number. Electronically storing any payment data automatically indicates a merchant must complete SAQ D, the most complex SAQ required by the PCI SSC.

3. Make the Switch to P2PE
Point-to-point encryption ensures payment data is secure by encrypting card information inside the POS hardware and sending it over a network to a service provider for decryption outside of the merchant network.

4. Tokenize Card Data
Tokenization occurs when sensitive card numbers are replaced by a non-sensitive surrogate value, also known as a token. Tokenization can reduce the components of a merchant system that need to be protected by PCI requirements, thereby reducing the amount of SAQ questions required.

5. Outsource Your Processing
Outsourced IT companies can actually help remove the burden of compliance. Although, companies should note that outsourcing doesn't absolve them from the responsibility to process payments securely.

In smaller merchant environments, it is common to see a *flat* network where cardholder data is unsegmented and unsecured from the rest of the network. The reason? Flat networks are extremely simple to understand and build. Organizations are often unaware that processing card data on their unsegmented network brings their entire network under PCI scope.

At a minimum, network segmentation entails logical separation between networks, usually provided by an industry-standard firewall. Though a firewall sits between network zones to limit network traffic, its presence between network segments doesn't necessarily mean secure and effective segmentation. Physical segregation between networks would provide an even more segmented and secure processing environment.

Segmenting a network can be quite difficult based on the complexity of the processing environment, but QSAs and other security professionals are available to assist. By partitioning the places card data travels into dedicated card zones from all other aspects of your business network, you reduce potential card data exposure.

A word of caution. Too many segments can lead to environment bottlenecks and complex firewall rules. Keep segmentation simple, and it will lead to better security.

2. Stop Storing Payment Data

Do you have unprotected card data on your point-of-sale or back office systems waiting to be harvested and sold for fraudulent purposes? Many merchants answer this question with a vehement no; but in reality, 71 percent of businesses store payment card data, often unknowingly (*2012 Payment Card Threat Report, SecurityMetrics*). While conducting onsite security assessments, I often see problems that result in insecure data storage — even on very sophisticated merchant systems.

It doesn't matter if an organization stores one payment card number, or a million. Electronically storing any payment data automatically indicates a merchant must complete SAQ D, the most complex SAQ required by the PCI Security Standards Council (SSC).

The first step is to discover where card data is used and if it's being stored. Just like flotsam in a river gets caught in eddies, card data can be deposited on systems that may or may not be directly involved in POS transactions. Knowing where to look for potential data eddies is half the battle.

The other half is finding, implementing and using a good data discovery tool that identifies card data in its various forms and alerts you to its location. Tools including CardRecon (GroundLabs), Spider (Cornell University) and PANscan (SecurityMetrics), can be used to search computer systems for data. The PCI SSC recommends data discovery methodologies to be used at least annually.

Don't forget to run these search tools on your e-commerce web servers, old systems historically dealing with card data and in departments such as accounting, sales and marketing.

Once unsecured card data is found, you must securely remove it using a secure removal or wipe process. (Hint, don't just use the delete key — it's not really gone after that.)

Now that your process and systems are clean, you need a program to keep them that way. Clear text credit card data has a way of creeping up again where you don't expect it to be. Define and follow a process of periodic data discovery cycles at least annually to recheck systems and ensure they remain free of unprotected card information.

3. Make the Switch to P2PE

Point-to-point encryption (P2PE) ensures payment data is secure by encrypting card information inside the POS hardware and sending it over a network to a service provider for decryption outside of the merchant network.

Troy Leach, CISSP, CISA, chief technology officer for the PCI SSC said of P2PE, "The PCI Council has never made this statement before — that through this effort you might be able to simplify your [PCI DSS] validation requirements." Using P2PE, merchant scope is reduced to the POS device and the delivery and installation procedures.

The best practice for a P2PE solution is to work with a service provider or acquirer that offers a validated P2PE solution with which to replace your current POS terminal.

4. Tokenize Card Data

Tokenization occurs when sensitive card numbers are replaced by a non-sensitive surrogate value, also known as a token. Properly implemented, tokenization can reduce the components of a merchant system that need to be protected by PCI requirements, thereby reducing the amount of SAQ questions required of a merchant.

As stated in the PCI SSC's informational supplement on tokenization, "storing tokens instead of PANs is one alternative that can help to reduce the amount of cardholder data in the environment, potentially reducing the merchant's effort to implement PCI DSS requirements" *(PCI SSC, 2012)*.

Implementing tokenization could simplify the requirements of PCI because cardholder data storage is centralized and sensitive data environment minimized. Businesses can work with QSAs, acquiring banks, processors or service providers to securely implement tokenization services.

5. Outsource Your Processing

While its admirable to have a DIY process surrounding business operations, small to midsize companies should seriously consider outsourcing payment processing. Outsourced IT companies can actually help remove the burden of compliance.

To illustrate, let me tell you how to become an SAQ A merchant. In order to be privileged enough to fill out the easiest, 13-question SAQ, all processes involving payment cards must go through a third party, no electronic storage of cardholder data is allowed, and you may only have card-not-present transactions.

Companies should note that outsourcing doesn't absolve them from the responsibility to process payments securely. The merchant still owns and is responsible for verifying PCI requirements are met, even if the process is outsourced.

Use caution when selecting IT vendors who use host information in the public cloud. Public cloud computing PCI compliance can be extremely difficult because of potential co-hosted customers existing on the same host server. Another problem with public cloud computing is lack of network segmentation. It's difficult to know where a business' virtual hosting servers are physically located and if they are properly segmented from other customers. Consequently, there are very few PCI-validated public cloud offerings worldwide.

Go and Do

Whether through recent and rapidly evolving technologies or age-old methods, reducing scope has recently become more and more attractive to businesses. As a QSA, I highly recommend scope reduction to all varieties of merchant. Not only does it reduce the time and resources required to become PCI compliant, but it also provides significantly more security. Remember that PCI DSS compliance and validation is not a quick or easy process, but reducing scope is one of the best ways to lighten the PCI load and reduce risk of payment data theft. ■